

June 30, 2007

Privacy and Security Solutions for Interoperable Health Information Exchange

Assessment of Variation and Analysis of Solutions

Prepared for

Jonathan White, MD, Director of Health IT
Agency for Healthcare Research and Quality
540 Gaither Road
Rockville, MD 20850

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Program Analyst
Office of Policy and Research
Office of the National Coordinator
330 C Street SW
Switzer Building, Room 4090
Washington, DC 20201

Prepared by

Linda L. Dimitropoulos, PhD
RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Contract Number 290-05-0015
RTI Project Number 0209825.000.007

Contract Number 290-05-0015
RTI Project Number 0209825.000.007

Privacy and Security Solutions for Interoperable Health Information Exchange

Assessment of Variation and Analysis of Solutions

June 30, 2007

Prepared for

Jonathan White, MD, Director of Health IT
Agency for Healthcare Research and Quality
540 Gaither Road
Rockville, MD 20850

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Program Analyst
Office of Policy and Research
Office of the National Coordinator
330 C Street SW
Switzer Building, Room 4090
Washington, DC 20201

Prepared by

Linda L. Dimitropoulos, PhD
RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Identifiable information in this report or presentation is protected by federal law, section 924(c) of the Public Health Service Act, 42 U.S.C. § 299c-3(c). Any confidential identifiable information in this report or presentation that is knowingly disclosed is disclosed solely for the purpose for which it was provided.

Contents

Section	Page
Executive Summary	ES-1
1. Background and Purpose	1-1
1.1 Description of the Purpose and Scope of This Report	1-1
1.2 Level of HIT Development in States	1-1
1.3 Description of Report Limitations	1-2
2. Assessment of Variation	2-1
2.1 Methodology	2-1
2.1.1 Steering Committee Composition	2-3
2.1.2 VWG and LWG Membership	2-5
2.1.3 Outreach to Stakeholders to Gather Variations	2-5
2.1.4 Outreach Methods	2-7
2.1.5 List of Stakeholders	2-8
2.1.6 Approaches to Conducting the Work	2-8
2.2 Treatment (Scenarios 1–4)	2-14
2.2.1 Stakeholders	2-16
2.2.2 Domains	2-17
2.2.3 Critical Observations	2-17
2.3 Payment (Scenario 5)	2-20
2.3.1 Stakeholders	2-20
2.3.2 Domains	2-21
2.3.3 Critical Observations	2-22
2.4 Regional Health Information Organization (RHIO; Scenario 6)	2-25
2.4.1 Stakeholders	2-25
2.4.2 Domains	2-27
2.4.3 Critical Observations	2-27
2.5 Research Data Use Scenario (Scenario 7)	2-30
2.5.1 Stakeholders	2-30
2.5.2 Domains	2-30
2.5.3 Critical Observations	2-31
2.6 Law Enforcement (Scenario 8)	2-33
2.6.1 Stakeholders	2-33

2.6.2	Domains	2-34
2.6.3	Critical Observations	2-36
2.7	Prescription Drug Use (Scenarios 9 and 10)	2-36
2.7.1	Stakeholders	2-37
2.7.2	Domains	2-37
2.7.3	Critical Observations	2-40
2.8	Health Care Operations and Marketing (Scenarios 11 and 12)	2-40
2.8.1	Stakeholders	2-41
2.8.2	Domains	2-42
2.8.3	Critical Observations	2-43
2.9	Bioterrorism Event (Scenario 13)	2-45
2.9.1	Stakeholders	2-45
2.9.2	Domains	2-46
2.9.3	Critical Observations	2-48
2.10	Employee Health Information (Scenario 14)	2-48
2.10.1	Stakeholders	2-49
2.10.2	Domains	2-51
2.10.3	Critical Observations	2-51
2.11	Public Health (Scenarios 15–17)	2-54
2.11.1	Stakeholders	2-55
2.11.2	Domains	2-55
2.11.3	Critical Observations	2-61
2.12	State Government Oversight (Scenario 18)	2-64
2.12.1	Stakeholders	2-64
2.12.2	Domains	2-64
2.12.3	Critical Observations	2-67
3.	Summary of Key Issues Raised by the State Teams in the Assessment of Variation	3-1
3.1	Variation in the Interpretation and Application of Consent	3-1
3.1.1	Consent for Treatment, Payment, and Health Care Operations	3-1
3.1.2	Specially Protected Information	3-3
3.1.3	Challenges Ahead	3-3
3.2	Misunderstandings and Differing Applications of HIPAA Privacy Rule Requirements	3-5
3.2.1	Minimum Necessary	3-5
3.2.2	Re-release or Redisclosure of PHI Obtained from Another Provider	3-7
3.2.3	Importance of Human Judgment Factor in Disclosures	3-7
3.2.4	Accounting of Disclosures	3-7

3.2.5	General Issues	3-8
3.3	Misunderstandings and Differing Applications of the HIPAA Security Rule.....	3-9
3.4	Security	3-9
3.4.1	Authentication and Authorization	3-9
3.4.2	Inadequate Application-Level Data Access or Screening Controls	3-10
3.4.3	Audit Programs	3-10
3.4.4	Secure Transmission of Personal Health Information.....	3-11
3.4.5	Lack of a Sound Security Infrastructure	3-11
3.4.6	Variability in Administrative and Physical Safeguards	3-12
3.5	Trust in Security	3-13
3.6	State Laws	3-14
3.7	Networking Issues.....	3-15
3.8	Linking Data from Multiple Sources to an Individual	3-16
3.8.1	Types of Patient Identification Used	3-17
3.8.2	Different Identification Systems: Common Challenges	3-18
3.8.3	Patient Identification: Consumer Communication and Education.....	3-19
3.9	Interstate Issues.....	3-19
3.10	Disclosure of Personal Health Information	3-20
3.10.1	Interpretation of Requirements for the Re-release or Redisclosure of Health Information.....	3-20
3.10.2	Differences in How Specially Protected Health Information Must Be Treated.....	3-20
3.10.3	Issues of Ownership of Health Information	3-21
3.10.4	Need for Fast, Easy, and Secure HIE Under Medical or Health Emergency Circumstances	3-22
3.10.5	Variations in Interpretation of Reporting Requirements for Public Health Purposes	3-22
3.10.6	Handling of Disclosures Related to Judicial Proceedings and Law Enforcement.....	3-23
3.11	Cultural and Business Issues.....	3-23
4.	Review of State Solution Identification and Selection Process	4-1
4.1	Solutions Work Group Formation	4-1
4.2	Process Used to Identify and Propose Solutions	4-3
4.3	Process Used to Vet, Evaluate, and Prioritize Solutions	4-3
4.4	Determination of Feasibility	4-5

5.	Analysis of State Proposed Solutions	5-1
5.1	Reducing Variation: Practice or Policy Solutions	5-1
5.1.1	Interpreting and Applying the HIPAA Privacy Rule	5-1
5.1.2	Uniform Consent	5-5
5.1.3	Policies to Govern Interstate Exchange	5-6
5.2	Legal or Regulatory Issues	5-6
5.2.1	State Laws: Finding and Interpreting Them	5-6
5.2.2	State Law Governing Secure Exchange of Health Information	5-7
5.2.3	Intersection of State and Federal Regulations (HIPAA Rules, 42 C.F.R. pt. 2, CLIA Rules)	5-9
5.3	Technology and Standards.....	5-11
5.3.1	Data Security and Transmission.....	5-12
5.3.2	Patient Identity Management	5-18
5.3.3	Segmenting Data	5-19
5.3.4	Standards That Affect Technology	5-20
5.4	Education.....	5-22
5.4.1	Consumer Education	5-23
5.4.2	Provider Education.....	5-25
5.4.3	Integrated Education	5-27
5.4.4	Education Targeted to Specific Groups.....	5-28
5.5	Implementation and Governance of Privacy and Security Solutions.....	5-28
5.5.1	General Implementation and Governance Issues.....	5-28
5.5.2	Governance and Implementation of HIEs	5-30
5.6	Ancillary Issues and Solutions	5-31
5.6.1	Funding	5-31
5.6.2	Incentives/EHR Adoption Issues	5-31
5.6.3	Stakeholder Engagement.....	5-32
6.	National-Level Recommendations	6-1
6.1	National Standards.....	6-1
6.1.1	National Standards for Transferring Health Information Among States.....	6-1
6.1.2	National Standard for Health Information Exchange-Related Business Associate Agreements	6-3
6.1.3	Standardized Model National Consent Form.....	6-3
6.1.4	Centralized Model Regulation Process	6-4
6.1.5	National Oversight Body	6-4
6.2	Clarifications/Revisions to Federal Regulations.....	6-4
6.2.1	HIPAA Privacy Rule Revisions/Clarifications	6-4

6.2.2	Clarify Legal Status Under HIPAA of Entities Participating in a Health Information Exchange	6-7
6.2.3	Confidentiality of Alcohol and Drug Abuse Patient Records (42 C.F.R. pt. 2)	6-7
6.2.4	Revision or Amendment to CLIA Regulations	6-8
6.2.5	Clarification of Medicaid Data Disclosure	6-8
6.3	Funding	6-9
6.3.1	Funding for More Widespread Adoption of Technology.....	6-9
6.3.2	Funding for Educating Patients and Consumers	6-10
7.	Moving States Forward Collectively	7-1
7.1	Coordinating Standards and Policy	7-1
7.2	Coordinating HIEs Between States.....	7-2
7.3	Coordinating Legislation	7-2
8.	Conclusions and Next Steps	8-1
Appendixes		
A	State Summaries	A-1
B	Descriptions of Health Information Exchange Development and Health Information Technology Adoption by State.....	B-1
C	List of Stakeholders	C-1
D	Glossary of Acronyms	D-1

Tables

Number	Page
2-1. Number of States Including Members from Major Stakeholder Groups on Steering Committee.....	2-4
2-2. Number of States Including Members from Major Stakeholder Groups on Variations Work Group and Legal Work Group	2-6
2-3. Number of Stakeholders Engaged in Assessment of Variation Process (All States Combined).....	2-9
2-4. Stakeholder Groups Engaged in Scenario 1–4 Reviews.....	2-16
2-5. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenarios 1–4 (N = 34).....	2-18
2-6. Stakeholder Groups Engaged in Scenario 5 Reviews	2-21
2-7. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 5 (N = 34).....	2-23
2-8. Stakeholder Groups Engaged in Scenario 6 Reviews	2-26
2-9. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 6 (N = 26)*	2-28
2-10. Stakeholder Groups Engaged in Scenario 7 Reviews	2-31
2-11. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 7 (N = 34).....	2-32
2-12. Stakeholder Groups Engaged in Scenario 8 Reviews	2-34
2-13. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 8 (N = 34).....	2-35
2-14. Stakeholder Groups Engaged in Scenario 9 and 10 Reviews.....	2-38
2-15. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenarios 9 and 10 (N = 34).....	2-39
2-16. Stakeholder Groups Engaged in Scenario 11 and 12 Review	2-42
2-17. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenarios 11 and 12 (N = 34)	2-44
2-18. Stakeholder Groups Engaged in Scenario 13 Reviews	2-46
2-19. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 13 (N = 34)	2-47
2-20. Stakeholder Groups Engaged in Scenario 14 Reviews	2-50
2-21. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 14 (N = 34)	2-52
2-22. Stakeholder Groups Engaged in Scenario 15–17 Reviews	2-56
2-23. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenarios 15–17 (N = 34)	2-57

2-24.	Stakeholder Groups Engaged in Scenario 18 Reviews	2-65
2-25.	Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 18 (N = 32)	2-66
4-1.	Stakeholder Group Representation of Solutions Work Group Members.....	4-2
4-2.	Stakeholder Group Engagement in Solutions Development and Evaluation.....	4-4

EXECUTIVE SUMMARY

This report is the fourth in a series to be produced under RTI International's contract with the Agency for Healthcare Research and Quality (AHRQ). The contract, entitled Privacy and Security Solutions for Interoperable Health Information Exchange, is managed by AHRQ and the Office of the National Coordinator for Health Information Technology (ONC). The following report is a summary of 34 separate final reports submitted by 33 states and one territory as subcontractors to RTI; these subcontractors form the Health Information Security and Privacy Collaboration (HISPC).¹ The Assessment of Variation and Analysis of Solutions (AVAS) report comprises the final reports submitted by the 34 subcontracted state teams and represents a "final look" at the major areas states have identified as presenting challenges to the privacy and security of electronic health information exchange and potential solutions to those issues raised. This summary report captures the highlights from the 34 reports and presents some of the major crosscutting themes that have been raised during the state teams' discussions.

This summary report consists of 8 major sections:

- Background and Purpose
- Assessment of Variation
- Summary of Key Issues Raised by the State Teams in the Assessment of Variation
- Review of State Solution Identification and Selection Process
- Analysis of State Proposed Solutions
- National-Level Recommendations
- Moving States Forward Collectively
- Conclusions and Next Steps

Background and Purpose

The purpose of the AVAS is to illustrate, in a descriptive report, the variations among the organization-level business practices, policies, and laws, related to privacy and security, as identified by each state team. The term *law* as used here refers to regulatory, statutory, or case law that serves as the primary driver behind a business practice. The AVAS reports also describe the process for identifying and proposing potential solutions, including an explanation of how state teams are evaluating and prioritizing the solutions and their feasibility. The information summarized in this report was provided by each of the state teams as a result of the work conducted by the Variations Work Groups (VWGs), Legal Work Groups (LWGs), and Solutions Work Groups (SWGs) of each participating state team. The

¹ Throughout this report the 33 states and 1 territory are referred to as the state project teams or as the state teams.

information also forms the basis for the work being conducted by the Implementation Planning Work Groups (IPWGs) as the state teams finalize their implementation reports. Although the AVAS reports are final, the work continues as the state teams work with stakeholders toward developing privacy policy and security standards to address the needs of their local communities.

Although each state team followed a core methodology, ample opportunity remained to tailor the process to meet the needs of each participating state and territory. The reports include a section that documents the process used to generate the set of organization-level business practices for each scenario, including outreach to the broader stakeholder groups, and a description of the membership and stakeholder representation of the VWGs, LWGs, and SWGs. Each state team followed an outline that provided an *a priori* categorization for potential solutions based on whether the potential solution effected a change in organization-level practice or policy, state law or regulations, federal law or regulations, or specifically impacted interstate electronic health information exchange. Although this categorization was recommended, state teams were given the opportunity to tailor the categorization to meet the needs of their specific participating state or territory. The reports also included a section in which state teams could discuss potential solutions that would require implementation at the national level. The outline and content of the AVAS reports are described in Table ES-1.

Summary of Assessment of Variation

The descriptions of business practices in each of the HISPC reports are organized by 11 purposes for health information exchange (HIE), as shown in Table ES-2. These purposes represent clusters of the 18 scenarios used to drive the discussions of business practices. Within each of the 11 sections, each state team was asked to provide a description of (1) the stakeholders who provided input to the collection of business practices; (2) the major domains addressed by the business practices (based on the 9 domains of privacy and security) including a discussion of the relevant policy, legal drivers, or rationale behind the practices; and (3) critical observations not offered elsewhere in the report. Finally, each state report provided a summary of the critical observations and key issues that the SWGs and the IPWGs further explored.

Summary of Key Issues in the Assessment of Variation

The AVAS report describes 10 major issues that state project teams raised as having broad implications for private and secure nationwide electronic health information exchange. This section provides a brief overview of these topics, which is not intended to be a thorough analysis of the issues or their implications, but rather a descriptive treatment of the issues.

Table ES-1. Outline of Assessment of Variations and Analysis of Solutions Report

Section Title	Content
Section 1—Background and Purpose	Purpose and scope of this report Description of level of health information technology (HIT) development in the state/territory Description of report limitations
Section 2—Assessment of Variation	Brief description of the methodology Description of variation identified, organized by scenario including stakeholders, domains, and critical observations
Section 3—Summary of Key Issues Raised by the State Teams in Assessment of Variation	Discussion of the key areas of variation as identified by the state teams
Section 4—Review of State Solution Identification and Selection Process	Description of the state Solutions Work Group, its charge, membership and stakeholder representation Description of the process the state used to identify and propose solutions Description of the process the state used to vet, evaluate, and prioritize solutions Description of how state determined the level of feasibility of identified solutions
Section 5—Analysis of State Proposed Solutions	Solutions to issues driven by variation in organizational business practices and policies (but not state laws) Solutions to issues driven by state laws/regulations Solutions to issues related to technology and standards Solutions to issues related to education Solutions to issues related to implementation and governance Solutions to collateral issues
Section 6—National-Level Recommendations	National standards related to draft model legislation, business agreements, uniform patient consent/authorization forms, national oversight body Clarification/revisions to federal regulations Funding
Section 7—Moving States Forward Collectively	Coordinating standards and policy Coordinating legislation
Section 8—Conclusions and Next Steps	Discussion of the implementation plans

Table ES-2. Purposes of Health Information Exchange (HIE) and Relevant Scenarios

Purposes of HIE	Relevant Scenarios
Treatment	Scenarios 1–4
Payment	Scenario 5
Regional health information organizations (RHIOs)	Scenario 6
Research data use	Scenario 7
Law enforcement	Scenario 8
Prescription drug use/benefit	Scenarios 9 and 10
Health care operations/marketing	Scenarios 11 and 12
Bioterrorism	Scenario 13
Employee health	Scenario 14
Public health	Scenarios 15–17
State government oversight	Scenario 18

Variation in the Interpretation and Application of Consent versus Authorization²

The state teams have identified broad variation in the use and implementation of patient consent and authorization. The terms are often used interchangeably although they have two distinct definitions and separate uses under various federal and state laws. For example, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires patient authorization for any uses and disclosures of protected health information (PHI) not otherwise permitted or required by the Privacy Rule. In contrast, the Privacy Rule permits, but does not require, the obtaining of consent for uses and disclosures of PHI for treatment, payment, and health care operations purposes. Further, the term *consent* has a specific meaning pursuant to the provisions of 42 C.F.R. pt. 2 (alcohol and chemical dependency). Despite the specific legal definitions, the terms *patient consent* and *patient authorization* have been used *interchangeably* by some state teams to refer to the *need for* (perceived or otherwise) and the actual *process of* obtaining appropriate approval from a patient (who is the subject of the information) or a corresponding legal guardian or representative before use or disclosure of the patient’s health information. Included are specific discussions regarding consent for treatment, payment, and health care operations;

² The terms *consent* and *authorization* have specific meanings in the context of various state and federal laws. Although context must be considered when examining a specific statute, here the terms are used to generally mean a signed permission to release or disclose protected health information.

special rules for disclosure of sensitive information; and challenges ahead for devising an approach to managing permissions necessary to permit electronic exchange.

Differing Interpretations and Applications of HIPAA Privacy Rule Requirements

State teams reported many business practice variations based on different interpretations and applications of the requirements of the Privacy Rule. This variation was not unexpected and is the result of the intentional flexibility and scalability of some of the Privacy Rule's requirements (e.g., *minimum necessary* and reasonable safeguards). The most commonly mentioned issues were variability in application of the *minimum necessary* standard and the use and implementation of patient consent, which the Privacy Rule permits but does not require, or authorization, across organizations.

Misunderstandings and Differing Applications of the HIPAA Security Rule

The state teams indicated that stakeholders misunderstood and were confused about appropriate security practices; moreover, they also misunderstood what was currently technically available and scalable to the health care industry and consumers. This lack of knowledge, understanding, and trust among organizations and stakeholders was more evident in the business practices than in state laws. For the most part, state laws did not pose challenges to sound security, nor did the HIPAA Security Rule.

Security

Authentication and Authorization. A number of state teams identified the need for standard authentication and authorization protocols to permit electronic health information exchange. State teams noted that the lack of a common method for authenticating individuals created mistrust between organizations. Currently, some organizations will accept a phone call or a fax from a known staff member at the requesting organization to authenticate the request and disclose the information. This is typical if the organizations have a previously established relationship. However, the same organization may impose a stricter requirement on other organizations including the requirement that the patient or individual sign a consent form (although not necessarily required by law) before the personal health information is exchanged. It becomes a cumbersome process that does not lend itself well to electronic health information exchange.

Inadequate Application-Level Data Access or Screening Controls. The state reports clearly indicate that many stakeholders are not using or are not familiar with currently available technologies. A critical issue identified by stakeholders that are either current users or exploring available technologies are the inadequacies in existing applications used to manage personal health information and for HIE, including electronic health records (EHRs) and data repositories. For example, some stakeholders indicated that they were required to print out copies of records from EHRs and redact especially sensitive

information, or information that should not otherwise be disclosed, because the EHRs did not accommodate segregation of certain types of data. The current business practice is to print a paper copy, redact the information, and fax the redacted copy of the record to the intended recipient.

Audit Programs. Several state teams indicated that the poor auditing capability of current software applications is a challenge to electronic health information exchange and that it is particularly problematic when the management of community health records or HIEs was discussed. Adequate audit processes mean more than activating the appropriate audit logs; they include the development and regularly scheduled use of an appropriate audit program that addresses potential privacy and security risks and is based on an established set of audit criteria that match the organization's needs.

Secure Transmission of Personal Health Information. Several state teams identified the secure transmission of personal health information between health care organizations, and between health care organizations and consumers, as a significant issue. Reports cited the lack of interoperable solutions and the high cost of implementing appropriate forms of secure transmission that protect the data in transit and protect against inappropriate interception and potential modification.

Lack of a Sound Security Infrastructure. A number of the state reports addressed interorganizational security issues but did not examine barriers related to these issues (administrative, physical, and technical). The lack of appropriate security program investment by health care and related organizations stems generally from 3 areas that should be reviewed and addressed at the organizational, state, and federal levels, including lack of knowledge about appropriate security practices and HIPAA Security Rule requirements; lack of investment in security on the part of the industry; and the method by which the HIPAA Security Rule is enforced by the US Department of Health and Human Services.

Variability in Administrative and Physical Safeguards. State teams noted that the lack of adoption of consistent and appropriate administrative and physical safeguards within health care organizations has resulted in mistrust between organizations and increased concerns related to liability (where an organization with a sound security program transmits personal health information to an organization that lacks a sound security infrastructure). This issue is not related to technology; rather, it involves lack of understanding about, or insufficient emphasis on, appropriate security for any size organization. State teams noted that reducing the variability in the application of administrative and physical security would do much to reduce certain challenges to electronic health information exchange, improve trust among organizations, and reduce liability concerns.

Trust in Security

Providers were principally concerned about potential liabilities from the activities of other participants in electronic health information exchange and about consumers' lawsuits for errant or inappropriate disclosures of their information. One state identified the concern about trust as the single most significant issue, one which had been repeatedly raised by stakeholders and the reason providers were not willing to participate in HIEs.

The second most commonly reported trust issue was consumer lack of trust in electronic health information exchange. The primary concern consumers raised was related to payer and employer access to health data and, secondarily, distrust of new technologies.

State Laws

Organizations vary widely in how they identify, locate, and apply existing state law. Some organizations use the HIPAA Privacy Rule as a ceiling rather than as the federal floor. In many states, the relevant state law is fragmented and scattered throughout many chapters of state law, making it difficult to find. In addition, the laws frequently conflict, are antiquated, and do not apply to electronic health information exchange.

Networking Issues

Most state teams were concerned about the lack of well-defined, operational, and deployable models for regional networking, which created a gap between policy development and practical application; in some states, this gap made it difficult to engage stakeholders in the policy work.

Linking Data from Multiple Sources to an Individual

The ability for a health care provider to identify the correct records for a patient is critical to clinical medicine and to electronic health information exchange. The lack of a standard, reliable way of accurately matching records to patients introduces the potential for inappropriate use and disclosure of personal health information, and inappropriate clinical decision-making issues that are both a clinical and a privacy risk.

Interstate Exchange Issues

Although the identification of interstate issues was not a primary focus of the interim assessment of variation, more than half the state teams reported that interstate issues should be considered and that agreements among states must be made to facilitate the exchange. States typically raised interstate issues because health care facilities draw patients from across state lines or because states experience very large seasonal inflows of both out-of-state workers and tourists.

Disclosure of Personal Health Information

The state teams reported multiple sources of variation in business practices related to the disclosure of health information:

- multiple interpretations of the requirements for patient consent or authorization in connection with the release of health information;
- issues related to the re-release or redisclosure of health information received by one entity from another;
- differences in how sensitive health information is treated;
- multiple interpretations and applications of the HIPAA Privacy Rule *minimum necessary* requirement;
- issues about rights and responsibilities regarding control of health information;
- varying degrees of reporting requirements for public health purposes;
- issues of ownership of health information;
- need for fast, easy, and secure electronic health information exchange under medical or health emergency circumstances;
- handling of disclosures related to judicial proceedings and law enforcement; and
- burden imposed by the need to document certain disclosures of health information.

Cultural and Business Issues

State teams referenced cultural and business issues that pose challenges to electronic health information exchange.

- Stakeholders are concerned about liability for incidental or inappropriate disclosures, which causes many organizations to take a conservative approach to developing practice and policy.
- A general resistance to change is evident; organizations and individuals are comfortable with existing paper-based or manual systems believed to be timely and effective.
- Clear definitions of terms within state and federal laws are needed. For example, terms like *medical emergency*, *current treatment*, *related entity*, and *minimum necessary* do not have agreed-upon definitions and, therefore, serve to increase variation.
- Tension exists among health care providers, hospitals, and patients concerning who controls or owns the data.

Review of the Solution Identification and Selection Process

A number of factors affected the approach that each state team took to developing solutions to the challenges and barriers to private and secure electronic health information exchange. Teams that represented states with existing HIEs or states that have done significant work toward implementing electronic health information exchange provided some very detailed

and specific analyses of the technical issues related to data security and standards. Teams representing states in the early stages of planning for electronic health information exchange tended to focus more on understanding the sources of variation that were identified; making decisions about the role of human judgment and how to build trust into the system; and developing governance structures and the need for oversight bodies and funding. Other factors also contributed to the variation in the reports, including the level of fragmentation of state laws. States with highly fragmented state privacy law focused on resolving that source of variation while states with relatively little or no state law governing privacy and security of electronic health information exchange discussed the possible need for legislation. On the other hand, some state teams with fairly stringent state privacy laws discussed the potential need to make changes to permit electronic health information exchange. Their struggle is the balance between ensuring the privacy and security requirements of their communities and maximizing the benefits of electronic health information exchange to the community.

Summary of Solutions

While many of the identified solutions were specific to a state, a number of common themes, issues, and solutions clearly surfaced. Generally, states' solutions fell into one or more of the following broad common areas that serve as a source of variation.

Reducing Variation: Practice or Policy Solutions

State teams identified the greatest amount of variation in organizations' interpretation and application of the HIPAA Privacy and Security Rules, including its *minimum necessary* standard. The Privacy Rule is frequently cited as limiting exchange, even though it generally allows the use or disclosure of protected health information, without *authorization*, for treatment, payment, and health care operations. All state teams agree that to reduce the current existing variation that poses challenges to interoperable electronic health information exchange, organizations and states must agree on some common interpretations and applications of the HIPAA Rules and develop some uniform policy. In addition to broad agreement on the need for policy development, the state teams also advanced many specific recommendations for detailed policy development. The state teams agreed on the need to define parameters for standard use and disclosure, including specifying the purpose and use of the data, consent and authorization policies and procedures, data use limitations, data collection limitations, and requests for restrictions on data use and disclosure, patient notification (including accounting and audit of prospective and retrospective data uses and disclosures), and patient education (including information about patient rights, granting of consent, and others). State teams also agreed about the need to establish a standardized or uniform patient consent form and process to be adopted by the entire health care industry. A number of states indicated that the uniform consent form and policy should clearly reflect patients' rights to information in their medical records

and provider confidentiality principles. Another state team added that state law should determine general consent requirements, consent principles relative to condition-specific consent requirements, interstate information exchange, information exchange with payers and employers, use of information for marketing, and waivers of consent when the patient's life is at risk and in public health emergencies.

Legal or Regulatory Solutions

Four state teams identified another source of variation driven, in part, by difficulties identifying and interpreting state law that is frequently fragmented and scattered. In addition, once found, the laws sometimes conflict with one another. This situation is further complicated by misunderstanding of how the state law intersects with federal laws and regulations. A number of state teams have proposed plans to consolidate statutes related to HIE to facilitate review to identify conflicting or outdated state laws.

State teams were also concerned about restrictive or outdated state laws that currently do or may in the future govern private and secure electronic health information exchange. Many states have no clear comprehensive privacy approach or any current body of state law governing electronic health information exchange. A number of state teams noted the need to update state laws and regulations to address provisions that inadequately address interoperability of electronic health information exchange and to reconcile the differences between state laws and the Privacy Rule. Some specific recommendations that should be included in a comprehensive approach include exploring the creation of new laws/policies to protect health care information held by third-party custodians. State teams also recommended amending existing laws/policies to ensure patients have access to their health information in electronic format, where available. One state specifically proposed making modifications to state statutes to resolve differences regarding *when* and *how* patient consent is required to exchange patients' health information. The team also identified the need to define undefined terms and ambiguous concepts in state patient consent requirements (such as *health record*); add language to clarify application of the state's patient consent requirements to new concepts in electronic health information exchange; and update the state's patient consent requirements to allow mechanisms that facilitate the electronic exchange of patients' information while respecting patients' ability and wishes to control their information.

Additional recommendations include the following:

- Draft sample language for uniform medical records statutes and regulations.
- Develop/promulgate rules detailing electronic health information exchange during a bioterrorism response and action, including public/private electronic health information exchange.
- Examine the federal and state provisions governing responsibilities to maintain and control patient data and records.

- Draft new legislation that provides specific protection for genetic data and that would standardize the age of consent regarding the release of medical information for treatment, payment, and operations to permit interstate exchange.
- Revise statutes to address electronic health information exchanges in emergency situations where the patient is unable to provide written or verbal consent.
- Request state regulatory change to include state versions of an exception to patient consent for treatment, payment, and health care operations.
- Evaluate the feasibility and applicability of a model state law or model state contract for the privacy and security of health information and, if appropriate, work with other states to develop and recommend such models.
- Require state government to recognize the Healthcare Information Technology Standards Panel (HITSP) and the Certification Commission for Healthcare Information Technology (CCHIT) standards criteria for privacy and security in all relevant contracting, policies, and programs.

Recommendations were also offered to address differences between state and federal laws dealing with inconsistent and sometimes conflicting requirements for patient consent; disclosure of sensitive health information; security requirements such as data protection, including business agreements, authentication, authorization of all individuals and their delegates; protection of data at rest in each party of an exchange; and protection of data in transit.

Similarly, a number of state teams identified the need to address inconsistencies between federal and state laws and regulations in areas such as sharing of specially protected health information (e.g., mental health and substance abuse data); Medicaid data sharing; interstate data sharing; state-to-local data sharing; data sharing for research; and data sharing in an HIE.

Technology/Data Standard Solutions

A number of state teams proposed the development of a standard national data format to document consent that recognizes the differing state-based consent policies, laws, and regulations but also promotes normalization and common application. In addition, a number of state teams, citing the need for patients to have more control over access to their health records, recommended that higher access standards/restricted access standards be developed for select information. These teams also indicated a need to educate patients on how, when, and why to control access to their information. Another recommendation was that states develop mechanisms and standards under which patient notification and a full audit trail is provided when specially protected information is requested and accessed.

A number of states proposed solutions for managing patient identity. The ability of a health care provider to identify the correct records for a patient is critical to clinical medicine and to electronic health information exchange. The lack of a standard, reliable way to accurately match records to patients introduces the potential for inappropriate use or disclosure of

health information about the wrong patient, both a clinical and a privacy risk. This problem is particularly acute when information is shared across institutions that have different methods of patient and record identification. All state teams noted the need for the ability to correctly identify patients, and most states recommended potential ways to accomplish this goal. Some recommendations include:

- Develop national guidelines and standards for a master patient index or record locator service.
- Establish a patient identity management service.
- Adopt a universal standard for patient identification, with official, verifiable means of both primary and secondary identification defined.
- Identify and adopt standards on patient identification (including unique patient ID, record locator capabilities, access to personal information, and ability to amend portions of the record).
- Identify and use a unique identifier for patient identification, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier.
- Identify patients accurately through biometrics.
- Coordinate a statewide approach to identify, authenticate, and authorize patients.

A number of state teams reported the need for systems that can segregate data to allow for controlled access to specially protected data and to allow patients to control access to portions of their records.

Education

All states recognize the need for varying levels of education to reduce variation in how policies are applied and also to increase stakeholder awareness and trust in the systems. The most common recommendations were for educational campaigns directed at patients and consumers and training programs for providers and organizations. Some examples include:

- Educate patients and consumers concerning federal and state privacy laws at both the national and state level. Include an explanation of the conditions in which their individually identifiable health information can be disclosed without their permission.
- Conduct a consumer needs assessment to see what consumers most want from an electronic health record (EHR)/HIE environment; focus on providing these functionalities to encourage public acceptance.
- Establish core education competencies for staff who manage personal health information, to include not only privacy and security training, but also awareness of the technical issues relevant to their job responsibilities and electronic health information exchange.

Implementation and Governance of Solutions

One goal of this project is to establish a state infrastructure that will allow the work to continue beyond the conclusion of this contract. To that end, a number of state teams have proposed an administrative or governance body to oversee the state's electronic health information exchange activities. Some recommendations are overarching to include all activities related to electronic health information exchange advancement and define the source of authority, operational structure, rules of the governing body, rules of participation in an electronic health information exchange network, and service offerings of the oversight entity. Other state teams propose forming entities to govern specific areas. For example, some state teams have proposed the establishment of an HIE Privacy and Security Advisory Board to oversee key aspects of privacy and security for statewide HIE. States also proposed establishing an information technology privacy and security committee to recommend standard privacy and security policies, procedures, and technology controls. Some states also suggested the formation of legal committees to recommend legal solutions to privacy and security issues.

Ancillary Issues and Solutions

Funding. A few states recommended investigating the possibility of providing public and private financial incentives for organizations to implement best security and privacy practices. Many more states explored ways to fund electronic health information exchange activity in the broader context, including providing incentives for adoption of technology. Although not directly related to the development of privacy policy and security standards, the funding and adoption issues are closely related to maintaining momentum among stakeholders working on the policy issues. A few examples are included below:

- Utilize tax incentives and other state-supported financing mechanisms for providers to invest in technology that will advance the utilization of private and secure HIE methodologies and systems.
- Research opportunities to make the HIEs reimbursable by Medicaid and under the state employee group health plan.
- Provide financial support for electronic health information exchange activities through grants, fundraising, and government appropriations.

Incentives/EHR Adoption. Financial incentives are an obvious solution to EHR adoption issues. Small providers, those located in rural or low-income areas, or providers with a large percentage of underinsured or uninsured patients, may face financial difficulty in purchasing and implementing EHR systems. The state teams proposed several types of incentives including tax incentives for providers, combinations of private and public incentives, and incentives for organizations that implement best practices in privacy and security. State teams also considered nonfinancial incentives, including a proposed mentoring program for providers who are implementing EHR systems.

Stakeholder Engagement. Although each state team is composed of representatives from a broad array stakeholders, all teams recognized the need for the continual engagement of stakeholders in discovery and solution development. Clearly, all state teams understood the need for ongoing consumer participation. A few examples of plans for engaging consumers are as follows:

- Hold a community forum.
- Assess consumer needs.
- Determine consumer perceptions and understanding of specially protected clinical data to see if it aligns with state and federal law.
- Strengthen the communication channels between the state, Indian Health Service, and sovereign Native American tribes.

In the majority of cases, stakeholder engagement included some form of educational programs.

Summary of National-Level Recommendations

The final section of the report summarizes the state teams' recommendations for solutions that would be most effectively implemented at the national level. The state project teams focused primarily on generating potential solutions that could be implemented at the local or state level. However, state teams also recommended solutions at the federal level that would be highly valuable to states as they develop privacy policy and security standards. Many ideas summarized in this section were also raised by other state teams as potential solutions to be implemented at the state level. The state teams that offered these preliminary thoughts about national level recommendations generally indicated that privacy policy and security standards for electronic health information exchange could achieve faster uptake if adopted at the national level rather than trying to come to agreement nationwide at the state level.

National Standards

Many state teams called for national standards to form a framework for nationwide electronic health information exchange. The teams recommended standardizing both a basic set of data elements and the accompanying technical standards for the interstate transfer of personal health information. All state teams expressed an interest in sharing data across state lines; however, some state teams felt strongly that the federal government would need to impose a national framework as a starting point that would include national standards that the states could use as a common basis for exchange. These state teams argued that without a national framework, the states will develop silos that will not be able to exchange data with one another, leading to a fragmented and disjointed system. Some state teams also noted that, while technical solutions can be designed and implemented at a regional level, they can lead to multiple and disparate approaches that would inhibit

exchange among regions. National standards and guidelines could provide a platform to begin exchange discussions; states could alter it if necessary, but a similar core framework would be maintained from state to state. Similar arguments were proposed for the development and publication of a national standard for data sharing agreements.

National Standards for Transferring Health Information Among States. State teams most frequently called for national standards that would collectively guide the transfer of health information among states. Without a centralized effort, states could go in disparate directions or the effort will take far longer to coordinate.

National Standard for Health Information Exchange-Related Business Associate Agreements.³ Similar arguments were proposed for the development and publication of a national standard for data sharing agreements, such as a business associate agreement (BAA).⁴ Eight state teams proposed that a standard BAA be established at the national level even though there is a national standard for BAAs and data use agreements in the HIPAA Privacy Rule.

Standardized Model National Consent Form. The state teams indicated that a model consent form is one of the essential components to encourage data sharing among organizations and across states. Many state teams have proposed solutions about the development of statewide uniform consent models. State teams recommending a model national consent form recognize that each state must be concerned with the unique state laws that affect their consent process, but they also recognize that using a common template to build upon will decrease variation.

Centralized Model Regulation Process. To develop a centralized model regulation development process, state teams suggested a range of options: a national effort to provide structured guidance to the current national standard setting bodies, a centralized national process to examine the role of emerging standard setting organizations, and working with the National Conference of Commissioners on Uniform State Laws (NCCUSL) to broker a set of model legislation. All states proposing this recommendation felt that some national-level oversight was needed in the production of model standards or model legislation.

³ Five of the 8 states making this recommendation referred specifically to a national standardized business associate agreement, and 3 state teams referred to contractual or participant agreements. None of the states used the more specific term *business associate contract*. HIPAA requires covered entities to document they have obtained satisfactory assurance that their business associate will safeguard health information through a written contract or other written agreement or arrangement. The Privacy Rule has specific provisions for business associate contracts and other arrangements. The other arrangements category includes, for example, memorandums of understanding between agencies. Thus, the term *business associate agreement* encompasses both contracts and other arrangements, so this term is used in the summary above.

⁴ These types of agreements are common and required by both the HIPAA Privacy and Security Rules. BAAs are executed whenever a third party performs certain services for a covered entity that includes access to PHI. For example, organizations receiving PHI and serving as a platform for many regional or local data exchange systems on behalf of covered entities would be a business associate of all covered entities that use the organization's services.

National Oversight Body. Three state teams proposed that an organized authority or oversight body guide the standardization of privacy and security implementation among states. Although all 3 states provided different alternatives, the sentiment was that this oversight could accelerate the adoption of recognized model laws, contracts, policies, and procedures among participating entities in an HIE. The state teams also recommended that the national oversight body oversee a consistent national educational campaign to consumers that will lead to greater public understanding and electronic health information exchange participation.

Clarifications/Revisions to Federal Regulations

The second most frequent set of issues raised by the state teams that offered national-level recommendations included recommended revisions and clarifications to federal regulations, including HIPAA Privacy Rule, 42 C.F.R. pt. 2, Clinical Laboratory Improvement Amendments (CLIA) regulations and Medicaid data disclosure regulations.

HIPAA Privacy Rule Revisions/Clarifications. Only 6 state teams recommended clarifications or revisions to the HIPAA Privacy Rule. One state team stated that clarification and perhaps revision of the Privacy Rule is necessary to reduce the variation in interpretation and application of Privacy Rule provisions across organizations and states.

Two states recommended that the Privacy Rule requirements for *minimum necessary*, de-identification, limited data set, and designated record set be reviewed for possible technical adjustments. Neither state elaborated on what types of technical adjustments were recommended, nor did they describe in the interim report what was problematic. Both state teams also recommended that the Department of Health and Human Services (HHS), Office for Civil Rights, develop new and more nuanced guidance.

One state pointed out the need to clarify appropriate electronic exchange guidelines to provide specific guidance concerning federal law restrictions about information types and classes, and also to provide solutions by which electronic personal health information can be viewed and exchanged outside established HIPAA standard transactions (e.g., via EHR, electronic clinical notes, electronic health information exchange, and so forth).

One state team identified 3 potential changes to the Privacy Rule to reduce both administrative burden and variation. First, the state team noted that although the Privacy Rule introduced requirements intended to protect patient privacy, in some situations, the requirements provide nominal improvements in patient privacy protections over existing state law but increase administrative burdens in ways that may impede electronic health information exchange. The team's first proposed solution was to remove the requirement for BAAs and modify the statute to hold business associates directly accountable and liable for adhering to the Privacy Rule requirements. Second, the state team explained that interpretations and applications of the *minimum necessary* standard vary widely. The team

proposed that states work to develop model policies and procedures to promote more consistent application of the *minimum necessary* standard. Finally, the team noted that prior to the HIPAA Privacy Rule, access to research information without patient consent was controlled by 45 C.F.R. pt. 46, the Common Rule, which applies to all research on Human Subjects. The Privacy Rule's requirements governing access for research purposes are deemed more protective of patient information than state laws; therefore, the Privacy Rule requirements control access without consent for research purposes. Under the Privacy Rule, generally, if researchers request access to identifiable health information as part of a research study, they must either obtain a waiver of *authorization* from the institutional review board (IRB) as part of the IRB approval process, or obtain *authorization* from all patients in the study.⁵ Because of the additional waiver criteria required by the Privacy Rule, many facilities have created privacy boards in addition to the IRB to evaluate and grant waivers. In evaluating a research proposal, an IRB is required to weigh the proposal's risks and benefits, including its impact on the confidentiality of patient health information. The state team agreed that IRB approval under the Common Rule is sufficient to protect patient confidentiality, and the team proposed that the federal government eliminate the Privacy Rule's additional waiver criteria.

Clarify Legal Status under HIPAA of Entities Participating in an HIE. Two state teams noted a need to clarify the legal status of certain entities participating in HIEs, including regional health information organizations (RHIOs), and to clarify whether they could be considered covered entities, business associates, or another as yet undefined category. The state teams noted a need to adopt a nationally accepted common definition of terms when referring to these organizations, their organizational and structural models and core components, their operational frameworks, and their legal standing in terms of liability.

Confidentiality of Alcohol and Drug Abuse Patient Records (42 C.F.R. pt. 2). Seven state teams raised issues related to 42 C.F.R. pt. 2, and 3 state teams proposed ways to manage the special protections governing the exchange of information that is protected by the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (42 C.F.R. pt. 2).⁶ Two state teams proposed adopting technological solutions (such as using the continuity of care record to restrict transmission of specially protected data). Three other state teams proposed legislative or regulatory changes that may not be feasible but, nevertheless, highlight areas with which the state teams are struggling, including:

- Amend 42 C.F.R. pt. 2 to state that patient consent is not required to exchange the data for treatment purposes and impose strict monetary penalties for misuse or inappropriate disclosure of identifiable alcohol or chemical dependency data (that would require appropriate and consistent enforcement activity). Currently, the criminal penalty under 42 U.S.C. §§ 290ee-3(f), 290dd-3(f), is that any person who

⁵ 45 C.F.R. § 164.512(i)(2)(ii).

⁶ 42 C.F.R. pt. 2 uses the term *alcohol and drug abuse*. Most of the states used the term *substance abuse*. This summary has adopted the terminology from the federal regulation for consistency.

violates any provision of the statutes or regulations can be fined not more than \$500 in the case of a first offense, and not more than \$5,000 in the case of each subsequent offense.

- Explore HHS's authority to define the contours of the consent without the need for legislative action, recognizing that it may not be permitted without Congressional action. That is, the consent provisions should be clarified so that a single consent allows for unlimited downstream releases for certain purposes (e.g., treatment), clarify that consent can describe generally the entities to which pt. 2 records may be disclosed (e.g., health care providers), and also allow consent to be effective indefinitely—at least until explicitly revoked.

Revision or Amendment to CLIA Regulations. One state suggested a revision to the federal CLIA regulations. The federal CLIA regulations, 42 C.F.R. § 493.1291(f), currently provide as follows: "Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test." The term *authorized person* is defined in 42 C.F.R. § 493.2 as "an individual authorized under State law to order tests or receive test results, or both." The term "individual responsible for using the test results" is not defined in the CLIA regulations, and its meaning is uncertain. The state team proposed that the CLIA regulations may pose a barrier to laboratories' exchange of health care information directly with the patient, with RHIOs, or with other similar organizations who may participate in electronic health information exchange.

Funding

Funding for More Widespread Adoption of Technology. Although this project focuses on issues related to private and secure electronic health information exchange, nearly all states raised the issue of low levels of technology adoption and the absence of a technical infrastructure as key barriers to their progress with the privacy and security work. Two state teams reported that national-level incentives could help sustain the momentum and prevent discussions from stagnating.

Funding for Educating Patients and Consumers. Two state teams called for education campaigns at the national level to reduce variation in practice. One state called for a national HHS public relations effort to provide a consistent, centralized, and visible source of education to the public.

Moving States Forward Collectively

The primary goal of each state team was to work toward solutions that would enable secure and private transfer of electronic health information between entities. However, the importance of collaboration in this project should not be ignored. Perhaps the greatest long-term effect of these activities will be the concurrent momentum built within each of the subcontracting states, the enthusiasm of which was not confined to state lines.

Conclusions and Next Steps

While the national-level recommendations summarized in Section 7 are an important outcome of the project, the final effort will focus on developing implementation plans for the state/territory-level solutions summarized in Section 5. These have been classified into 6 types of solutions:

- reducing variation: practice or policy solutions;
- legal and regulatory issues;
- technology and data standards;
- education;
- implementation and governance of privacy and security solutions; and
- ancillary issues and solutions.

The implementation plans for each of the state teams have been emphasized from the project's initiation. The project teams in each state and territory have been reminded that the government's purpose in funding this project has been not only to identify barriers to electronic health information exchange but also to solve them in a way that protects the privacy and security of health care consumers. The project has generated much discussion over the course of the past 10 months in steering committees and work group sessions, in stakeholder meetings, and in the regional meetings—as well as at the national meeting that was held in March 2007. These discussions have, in turn, resulted in stakeholders' commitments to fulfill the promises of improved health information exchange and to protect this information. In addition to a better understanding of barriers and proposed solutions, the perpetuation of this commitment is a major goal of the collaboration.

In developing their implementation plans, the state teams have been encouraged to focus on the practical and efficacious. As noted previously, conditions relevant to electronic health information exchange vary both within and between states. What works in one state may not work in another. The project teams have been encouraged to vet implementation plans with stakeholder groups in the same iterative process used to identify the variation in business practices, policies, and state laws to develop solutions that reduce variation and permit widespread electronic health information exchange in a private and secure way.

Based on the draft implementation plans provided by the teams in each state/territory, we anticipate the final implementation plans will include detailed plans to move forward in the following areas:

- governance and leadership;
- business practices and policies;

- legal and regulatory solutions;
- technological and data standards solutions; and
- education and outreach.

In addition to these concrete objectives, the project teams in each state/territory have provided practical considerations for accountability, funding, and specific timelines.

1. BACKGROUND AND PURPOSE

1.1 Description of the Purpose and Scope of This Report

Under the aegis of the Privacy and Security Solutions for Interoperable Health Information Exchange contract, RTI International has contracted with entities in 33 states and 1 territory to conduct an assessment of variations in business practices related to health information exchange, identify practices, policies, and laws that might be perceived as barriers to electronic exchange of health information, suggest possible solutions to these barriers, and prepare plans to implement these solutions.

This report documents and summarizes the Assessment of Variations and Analysis of Solutions (AVAS) reports submitted by the state and territory project teams. The Executive Summary from each of the individual state team reports is provided in Appendix A. Each state project team has prepared interim reports: the Interim Assessment of Variation report describes variation in business practices related to privacy and security in health information exchange and identifies those sources of variation that might inhibit electronic health information exchange; the Interim Analysis of Solutions report details solutions to reduce the variation and enable electronic health information exchange while preserving essential privacy and security protections. This report represents the integration and culmination of the project work in these areas.

This AVAS report describes and discusses variations among the organization-level business practices, policies, and laws—as related to privacy and security—that each state project team identified. The term *law* as used here refers to regulatory, statutory, or case law that serves as the primary driver for a business practice. This AVAS report also describes the process for identifying and proposing potential solutions, including an explanation of how state project teams are evaluating and prioritizing the solutions and their feasibility.

1.2 Level of HIT Development in States

The state teams participating in this project represent several levels of health information technology (HIT) adoption and use. In their AVAS reports, state teams were asked to describe the status of HIT implementation within their state in order to provide context for proposed solutions. Appendix B provides a table that summarizes each state's level of HIE development and the level of adoption of HIT (when known). The references to low or high HIT development in this table are based on the state team's assessment; they are not the result of applying a consistent set of criteria across the reports. Even in states described as having sophisticated HIT, some regions do not have access to systems.

1.3 Description of Report Limitations

Thirty-one of the 34 reports discussed limitations, and the constraint of the project schedule was a common theme. States uniformly indicated time constraints meant that proposed solutions were preliminary and that further work would be required to operationalize the solutions. Specific constraints included difficulties in scheduling meetings with busy stakeholders, overcoming project learning curves for stakeholders, engaging consumers, and the amount of out-of-meeting time individuals and groups needed to produce multiple solutions for review and analysis. States concluded that their solutions reports are works in progress as further work developing implementation plans often points to additional solutions worthy of pursuit.

A smaller set of state teams specifically described the lengthy process necessary for their stakeholders to reach consensus on prioritizing solutions for the report. For another state this set of limitations included the need for additional legal analysis of solutions to determine their legal feasibility.

A handful of states noted that their state stakeholders and participants were not familiar with electronic health record-related privacy and security environments in their workplaces. In such cases, lack of familiarity limited the project team's scope of analysis.

Most state teams reported no problems engaging stakeholders, with the exception of a number of states reporting difficulty engaging consumer or patient groups in a meaningful way. As they proceed with implementation plans, additional efforts are under way to ensure participation by consumers/patients and consumer advocacy groups.

2. ASSESSMENT OF VARIATION

2.1 Methodology

In June 2005 the US Department of Health and Human Services published the *Summary of Nationwide Health Information Network Request for Information Responses*, which contained the responses from 512 organizations and individuals. In this report, privacy and security considerations were crosscutting, and nearly every response cited the importance of “patient privacy and reiterated that the American public must feel confident that their health information is secure, protected, portable, and under their control” (p. 21). The report also noted major concerns among respondents about the varying interpretations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules being implemented by organizations and the challenges this variation would pose to nationwide electronic health information exchange. Respondents noted that the Privacy and Security Rules allow for 2 hospitals to develop 2 different business practices, both compliant, for protecting privacy and security of health care records and that this variation must be addressed if interoperable electronic health information exchange is to be achieved nationwide. Furthermore, the respondents noted that complications would exist both within and across states because of differences between state privacy laws and federal laws.

The purpose of this Privacy and Security Solutions for Interoperable Health Information Exchange project is to assess variations in organization-level business practices, policies, and state laws that affect electronic health information exchange and to identify and propose practical ways to reduce the variation to those “good” practices that will permit interoperability while preserving the necessary privacy and security requirements set by the local community. Because business practices are typically derived from business policies and law, uncovering the policy or legal driver on which the business practices are based is crucial to understanding how a current practice might be impacted by electronic health information exchange. Current laws or policies may prevent or impede electronic health information exchange, or perhaps may actually support and encourage electronic transfer, which would presumably make the exchange more efficient. By developing a complete understanding of the rationale for a business practice, whether paper-based or electronic, one can determine what elements should be retained as requirements for an electronic system of exchange and what, if any, policy or legal changes are needed to enable private and secure exchange. This report discusses the variations uncovered through this project as well as the proposed solutions. The final phase of the project will focus on outlining detailed implementation plans in a separate report.

The project methodology is based on three key assumptions. First, for stakeholders to trust electronic health information exchange, decisions about how to protect the privacy and security of health information should be made at the local community level. Second, to

accomplish this goal, discussions must take place to develop an understanding of the current landscape and the variation that exists among organizations within each state and, ultimately, across states. Finally, stakeholders at the state and community levels, including patients and consumers, must be involved in identifying the current variation that exists, understanding the rationale that underlies the current business practices, deciding what the privacy and security requirements are, and developing solutions to achieve broad-based acceptance.

The 9 Domains of Privacy and Security

- User and Entity Authentication
- Authorization and Access Control
- Patient and Provider Identification
- Transmission Security
- Information Protection
- Information Audits
- Administrative and Physical Safeguards
- State Law
- Use and Disclosure Policy

State project teams followed a modified community-based research model that provided limited flexibility to each team to organize its leadership, steering committee, and work groups in ways appropriate to the needs of their current industry organization and market structure. Project teams followed a core methodology that framed discussions for the exchange of specific types of health information within 9 domains of privacy and security by using 18 scenarios as the starting point for work group discussions.

The Health Information Security and Privacy Collaboration (HISPC) comprises 33 states and one territory, Puerto Rico. Only one subcontracted organization, designated by the governor, is used per state. Each state and territory identified a steering committee that was a private-public partnership of leaders from state government and stakeholder organizations, and all work was conducted through a series of coordinated work groups with specific charges. Each state or territory was expected to reach out to a broad range of stakeholders to include, at a minimum:

- providers,
- payers,
- federal health facilities,
- state government,
- pharmacies,
- long-term care facilities and nursing homes,
- professional associations and societies,
- medical and public health schools that undertake research,
- hospitals,
- public health agencies,
- community clinics and health centers,
- laboratories,
- homecare and hospices,
- correctional facilities,
- quality improvement organizations, and
- consumers or consumer organizations.

The following sections summarize the various methods state project teams used to organize their respective leadership teams and work groups, the methods used to engage stakeholders in the process, and the methods each state and territory followed to conduct the interim assessment of variation. Further, the state project teams' findings are summarized by major domains of privacy and security. Finally, 10 crosscutting issues are summarized; (these issues were raised by the state teams in the interim assessment of variation).

The methodology sections of the 34 interim reports focused primarily on narrating the activities in which their work groups engaged to obtain a comprehensive set of business practices from the stakeholder community. State teams provided varying degrees of detail when they described the composition and subject matter expertise of their Variations Work Groups (VWGs) and Legal Work Groups (LWGs).

This report, by virtue of its subject matter, has certain limitations. This report summarizes the work conducted by project teams in 34 of the 56 states and US territories and, therefore, presents a "snapshot" of the current landscape in the 33 states and 1 territory that form HISPC, although many of the issues will be relevant to the entire nation.

2.1.1 Steering Committee Composition

All state teams were required to form a steering committee composed of state leaders and public and private stakeholders to provide leadership throughout the process and to sustain the effort beyond the end of the contract. Steering committee membership varied in accordance with the unique landscape and environment of each state and territory, but all committees were asked to include one member that represented the governor's office—either a senior policy advisor, cabinet member, or, in the case of one state, the lieutenant governor. The other members of the committees include high-level health care officials, such as directors of health insurance companies, health care, hospitals, and public health care systems. The number of states including a member from these and other stakeholder groups on their steering committee is provided in Table 2-1. Most states that provided details about their steering committee membership notably included members from private or public task forces focused on improving electronic health information exchange; also included were directors of information technology services across the spectrum of state and private health care systems, including many chief information and security officers.

The breadth of stakeholder representation on the steering committee varied across the 34 state project teams. Although only a few states provided the specific number of people on their steering committees in their reports, where numbers were provided, steering committees were generally smaller than other work groups and less representative of the broader stakeholder community from which they drew. Some states with large Native American populations included tribal representatives in both their steering committees and in their work groups. The state teams were required to engage consumers as individuals and as members of advocacy groups on their steering committees and in their work groups.

Table 2-1. Number of States Including Members from Major Stakeholder Groups on Steering Committee

Stakeholder Group	States Including Stakeholder Group in Steering Committee Membership (N = X)	States Including Stakeholder Group in Steering Committee Membership (%)
Providers	33	(97)
Physicians and physicians groups	28	(82)
Hospitals/health systems	28	(82)
Professional associations and societies	23	(68)
Clinicians	22	(65)
Community clinics and health centers	15	(44)
Mental health and behavioral health	13	(38)
Pharmacies/pharmacy benefit managers	13	(38)
Federal health facilities	10	(29)
Long-term care facilities and nursing homes	8	(24)
Safety net providers	8	(24)
Homecare and hospice	7	(21)
Other health care providers	6	(18)
Emergency medicine	4	(12)
Laboratories	4	(12)
Technology and health information experts	33	(97)
Quality improvement organizations	18	(53)
Health IT consultants	17	(50)
Electronic health records experts	14	(41)
Regional health information organizations	13	(38)
Privacy and security experts/compliance officers	13	(38)
Health information management organizations	9	(26)
Technology organizations/vendors	8	(24)
Other health data and technology experts	5	(15)
Other government	31	(91)
Medicaid/state government except public health	30	(88)
County government	4	(12)
Payers	28	(82)
Medical and public health schools/research	25	(74)
Public health agencies or departments	25	(74)
Legal counsel/attorneys	25	(74)
Consumers	22	(65)
Consumer organizations and advocates	17	(50)
Individual consumers	12	(35)
Employers	17	(50)
Foundations/other policy consultants	2	(6)
Other	1	(3)
Law enforcement and correctional facilities	0	(0)

2.1.2 VWG and LWG Membership

Most state teams included details about the size and general composition of their VWGs and LWGs; see Table 2-2 for a list of states including members of certain major stakeholder groups in these two work groups. As a whole, states attended to the need for breadth of stakeholder representation on the VWG. Some states decided to increase the size of their VWG to provide sufficient breadth in the group itself, while other states preferred to have a smaller VWG that gathered required information from the broader stakeholder community to achieve appropriate representation across that community.

Although the states' work groups did not always fully represent the entire stakeholder community, states explicitly described the processes they used to engage those stakeholder groups not represented. All but a few of the state teams provided information about their VWG and LWG subject matter expertise as related to their particular stakeholder community. The few state teams that did not provide these details did describe the processes their work groups undertook to engage a wide variety of stakeholders to gather business practices. A few state teams explained in detail activities their VWG members engaged in to ensure a broader range of stakeholder involvement in gathering business practices. LWGs were smaller across the board, ranging from 8 members to as many as 22. All but 9 state teams included some information about their LWG members' subject area expertise; most of their expertise was in private or public health care-sector legal affairs.

2.1.3 Outreach to Stakeholders to Gather Variations

A leading researcher in the concept of the stakeholder, R. Edward Freeman, defines the *stakeholder* as an individual or group that has some share or interest in the functioning of the business system (1984).⁷ Freeman explains that the term *stakeholder* is preferred over terms such as *constituents* or *influencers* because it connotes a level of accountability to the stakeholder by the business entity or initiative. The stakeholder can be as dynamic as the business system: depending on the issue, the stakeholder's level of interest, influence, and perspective may change. Each state team was, therefore, asked to identify the appropriate stakeholders for its project. RTI provided state teams minimal direction for identifying the stakeholders, except to request that the greatest effort be made to identify and include as many stakeholders as possible (for the list of recommended stakeholders to include in state work groups, see Appendix C).

⁷ Freeman, RE. *Strategic Management: A Stakeholder Approach*. Boston, Mass: Pitman Publishing Company; 1984.

Table 2-2. Number of States Including Members from Major Stakeholder Groups on Variations Work Group and Legal Work Group

Stakeholder Group	States Including Stakeholder Group in Variations Work Group Membership (N = 34)	States Including Stakeholder Group in Variations Work Group Membership (%)	States Including Stakeholder Group in Legal Work Group Membership (N = 34)	States Including Stakeholder Group in Legal Work Group Membership (%)
Technology and health information experts	33	(97)	34	(100)
Privacy and security experts/compliance officers	24	(71)	31	(91)
Health IT consultants	22	(65)	27	(79)
Electronic health records experts	22	(65)	21	(62)
Quality improvement organizations	21	(62)	14	(41)
Regional health information organizations	17	(50)	10	(29)
Health information management organizations	16	(47)	10	(29)
Technology organizations/vendors	11	(32)	8	(24)
Other health data and technology experts	6	(18)	6	(18)
Providers	32	(94)	5	(15)
Hospitals/health systems	32	(94)	4	(12)
Physicians and physicians groups	30	(88)	4	(12)
Clinicians	29	(85)	4	(12)
Community clinics and health centers	27	(79)	3	(9)
Professional associations and societies	27	(79)	2	(6)
Pharmacies/pharmacy benefit managers	24	(71)	1	(3)
Long-term care facilities and nursing homes	21	(62)	30	(88)
Mental health and behavioral health	20	(59)	21	(62)
Homecare and hospice	17	(50)	14	(41)
Federal health facilities	16	(47)	12	(35)
Emergency medicine	16	(47)	10	(29)
Laboratories	15	(44)	8	(24)
Safety net providers	12	(35)	8	(24)
Other health care providers	3	(9)	6	(18)
Public health agencies or departments	31	(91)	2	(6)
Other government	29	(85)	24	(71)
Medicaid/state government except public health	27	(79)	23	(68)
County government	11	(32)	22	(65)
Payers	27	(79)	4	(12)
Medical and public health schools/research	23	(68)	21	(62)
Legal counsel/attorneys	22	(65)	20	(59)
Consumers	22	(65)	17	(50)
Individual consumers	16	(47)	12	(35)
Consumer organizations and advocates	17	(50)	7	(21)
Employers	17	(50)	8	(24)
Law enforcement and correctional facilities	15	(44)	4	(12)
Foundations/other policy consultants	3	(9)	1	(3)
Other	3	(9)	0	(0)

The first step in developing an effective outreach strategy for stakeholders was for the state teams to create as comprehensive a list of stakeholders as possible on the basis of the privacy and security domains. By developing an initial list, the states were able to “piggyback” on that list and add more stakeholders as needed. Another phenomenon of the stakeholder concept is that various program levels spur various stakeholders. For example, at the administrative or management level, stakeholders may be different from those who will interface with the project on the operations level. Most state teams addressed these nuances as they worked with their stakeholder groups by soliciting information from the appropriate participant level within them.

All of the state teams relied on a top-down approach in their outreach strategies. Once they agreed on a stakeholder, the initial contact was at the highest level to solicit participation and input from the organization or entity. The thought was that, for the type of detail required, participants needed to understand that their leadership supported their participation. Information was then sent either to the initial contact person or an in-person contact was made to introduce the project. During the initial contact the state teams also detailed the expectations for participating in the work groups.

Once the states were provided the scenarios, the state teams revisited the lists of stakeholders and began placing the stakeholders into work groups. The stakeholder work groups reviewed and analyzed scenarios relevant to their roles and concerns. Although the state teams differed in how the work groups were formed or how data were collected, the level of effort expended to identify and reach stakeholders did not differ at all.

2.1.4 Outreach Methods

To enhance outreach, the state teams

- circulated documents to all active members of health organizations, most of whom work in medical records or a related area;
- reached out to stakeholder and professional associations, government agencies at all levels, and consumer groups;
- held regional meetings and broke work groups into sublevel work groups;
- highlighted the project on websites and in newsletters;
- identified individuals to participate in focus groups or on Listservs;
- capitalized on existing health information technology collaborations and partnerships;
- sought stakeholder involvement through word-of-mouth invitations;
- through VWG members, recommended additional stakeholders who were invited to participate; and
- provided a public e-mail address so that interested persons could participate in the project.

2.1.5 List of Stakeholders

An integral part of this methodology included gathering information from individuals that were part of the wider stakeholder community to determine how widespread the variation was from organization to organization. Anecdotal information indicated not only that the variation between privacy policy and security practices between similar entities posed a problem to engaging in electronic exchange, but also that different stakeholder groups had potentially competing interests. A common example given indicated that while consumers felt that their information should be subject to very stringent privacy guidelines even for purposes of treatment, physicians felt strongly that they would not be able to provide quality care if their access was too tightly regulated.

Table 2-3 provides the raw numbers of stakeholders engaged during the assessment of variation process, as reported by all 34 state teams. This table gives an idea of the scope of stakeholder input that is included in the variation information provided below.

2.1.6 Approaches to Conducting the Work

Plan

In June and July 2006, RTI conducted a series of web-based conference calls and in-person trainings to introduce the state project teams to the project tools that had been developed, including the 18 scenarios and the Agency for Healthcare Research and Quality (AHRQ) National Resource Center portal, and, on the basis of these tools, to suggest an approach to the work. This approach consisted of 4 main steps through the submission of the Interim Assessment of Variation (IAV) report. Although this process is delineated here as a sequence of separate steps, it is actually a dynamic and interactive iterative process; most state teams managed the process by having considerable overlap in the composition of their work groups.

Step 1. The VWG members reviewed as many of the 18 health information exchange (HIE) scenarios as their knowledge and experience allowed in order to generate a core set of business practices and policies consistent with the stakeholder roles represented in the scenarios. VWG members could also at this stage begin to identify business practices for which policy decisions may be needed to transition from a paper-based system to electronic health information exchange. As part of this initial step, project teams were asked to categorize business practices as potential barriers to electronic health information exchange; as potential enablers of or aids to electronic health information exchange; or as having no impact on the flow of information, whether on paper or electronically.

Table 2-3. Number of Stakeholders Engaged in Assessment of Variation Process (All States Combined)

Stakeholder Group	Stakeholders Engaged in Variations Assessment through Community Outreach (Raw Numbers) (N = 34)	Stakeholders Engaged in Variations Assessment through Community Outreach (Raw Numbers) (Average)
Providers	1,630	(48)
Hospitals/health systems	341	(10)
Clinicians	240	(7)
Physicians and physicians groups	220	(6)
Community clinics and health centers	185	(5)
Professional associations and societies	157	(5)
Pharmacies/pharmacy benefit managers	85	(3)
Mental health and behavioral health	82	(2)
Long-term care facilities and nursing homes	74	(2)
Safety net providers	61	(2)
Homecare and hospice	44	(1)
Laboratories	43	(1)
Emergency medicine	42	(1)
Federal health facilities	37	(1)
Other health care providers	19	(1)
Technology and health information experts	582	(17)
Privacy and security experts/compliance officers	141	(4)
Electronic health records experts	94	(3)
Health IT consultants	84	(2)
Quality improvement organizations	67	(2)
Technology organizations/vendors	58	(2)
Health information management organizations	56	(2)
Regional health information organizations	47	(1)
Other health data and technology experts	35	(1)
Consumers	458	(13)
Individual consumers	318	(9)
Consumer organizations and advocates	140	(4)
Other government	243	(7)
Medicaid/other state government	193	(6)
County government	50	(1)
Public health agencies or departments	213	(6)
Employers	198	(6)
Legal counsel/attorneys	181	(5)
Medical and public health schools/research	140	(4)
Payers	122	(4)
Law enforcement and correctional facilities	37	(1)
Foundations/other policy consultants	4	(<1)
Other	3	(<1)
Total	3,811	(112)

In this scheme, the term *barrier* was initially defined as any business practice that impeded or blocked the electronic flow of information; it was intended to flag any business practice for which an understanding of the underlying rationale (i.e., the policy or legal driver) would be required to guide decisions about whether the practice was necessary. If the practice was deemed necessary, this understanding would also guide reconciliation of the practice with the need to exchange the information electronically. Similarly, the category of *aid to electronic health information exchange* was to flag practices for review as potentially good practices that could be shared with other organizations and states.

The RTI project team including the RTI Technical Advisory Panel (TAP), and the state teams wrestled with the term *barrier* as applied to individual practices because of its negative connotations. The project focus is on the *variation* in practice, policy, and law that poses a barrier to interoperable electronic health information exchange, not on individual practices that may or may not be barriers to interoperable electronic health information exchange. The definition was refined in an attempt to remove the value judgment and was then presented as “a practice, policy, or law that impedes, prohibits, or imposes conditions on health information exchange.” States were asked not to make a decision at this point in the process about whether a practice categorized as a barrier was “an appropriate protection” or an overly restrictive practice that could be modified; instead, they were asked to flag practices for further scrutiny.

Although many state teams followed this approach, a number of state teams took the position that, under this definition, informed consent would be a barrier and, even though it could be called an appropriate protection or a good barrier, the label *barrier* would, nonetheless, be a bad fit in this context. The RTI project team ultimately decided that states could use their own method of flagging the business practices for further evaluation and consideration by their work groups. This report contains many references to *barriers*; they are derived from the text provided by the state reports and the definition provided here.

Step 2. The scenarios and core set of business practices generated by the VWG were circulated to a broad group of stakeholders to develop additional business practices based on their experience. This step served to involve the community, build consensus, fill gaps in the VWG membership, and check the accuracy of the practices generated by the VWG.

On the basis of the American Health Information Management Association’s (AHIMA) experience during development and pilot testing of the scenarios, the RTI project team suggested that this step might be most effectively accomplished through a series of facilitated meetings, but recognized that such meetings would not be feasible for all state teams. AHIMA and the RTI project team prepared a guide to facilitating these meetings, which was included in the *Manual of Operations*. To ensure efficiency during use of the facilitated-meeting model, meetings were organized around subsets of the 18 scenarios,

and the relevant stakeholders were invited to attend each meeting. State teams submitted plans describing their preferred methods for organizing the stakeholder groups.

Step 3. The VWG reviewed the full set of collected business practices to ensure that the data were complete and sufficiently detailed for use by the LWG; in addition, the VWG was charged with identifying those business practices for which policy decisions might be needed.

Step 4. To identify and capture any legal drivers that might be relevant, the LWG reviewed the collected business practices that the VWG flagged.

Each state team was granted considerable latitude to determine, given its own circumstances, the specific approach that would work best for it. In particular, state teams determined the best methods for engaging a broad group of stakeholders in the review of scenarios.

Outcomes

The VWGs' task was to review the scenarios, generate a core set of business practices, and begin to identify challenges to interoperable electronic health information exchange. VWGs achieved broad coverage of stakeholder groups and state regions. To increase coverage of stakeholder perspectives, some states expanded the VWG to include additional individuals from participating organizations.

The function of the VWG varied across teams. Most collected a core set of business practices as suggested. Others generated the initial set of business practices in meetings that combined the VWG with the broader group of stakeholders. A few asked stakeholders to generate the initial set of business practices, which the VWG then reviewed and completed. Before collecting business practices, some VWGs identified interoperability challenges based on their perceptions of the scenarios. Shortly after receiving the scenarios, one state team generated a core set of questions or topic areas for each scenario to guide stakeholder discussion. These questions were shared with RTI, AHRQ, the Office of the National Coordinator for Health Information Technology (ONC), and selected TAP members for review and comment. It was then distributed to all project teams as a scenario guide.

The practices collected were shared with a broader group of stakeholders to validate that, as a set, they were reasonably complete and to fill gaps as necessary. All teams engaged the broader stakeholder community; 30 to approximately 300 stakeholders participated. Most teams used facilitated meetings, but also employed additional techniques to collect supplementary data from stakeholders. Additional stakeholder input was collected by telephone and in-person interviews, conference calls, e-mail, submissions to websites, and submittal of completed worksheets.

Stakeholders were usually asked to review and vet the core set of business practices generated by the VWG. A number of reports noted that they also sent background materials, scenarios, and the core set of business practices to stakeholders in advance of the meeting.

A few teams noted that they added scenarios or modified the provided scenarios to adapt them to particular circumstances in their respective states or territory.

Most project teams arranged meetings organized by subsets of scenarios that required input from a common set of stakeholder groups. Usually 2 to 5 scenarios were reviewed per meeting. This approach also allowed teams to limit participation to a manageable size to encourage active participation. Most teams reported that 2 to 3 members of the core team attended the stakeholder meetings to provide background, facilitate, and take notes.

Six state teams reported that they encountered concerns from stakeholders about confidentiality and anonymity in the discussions. Three teams reported that they developed a confidentiality agreement to address these concerns. One state team reported that stakeholder participation was limited because some recruits were prohibited from sharing their practices, citing proprietary business practice information. A few states reported participants who were unwilling to share business practices despite assurances of confidentiality and anonymous reporting.

Some teams noted an inability to engage particular stakeholder groups, such as consumers, law enforcement, and federal health facilities, in this phase of the work. These project teams reported continuing efforts to engage these stakeholder groups so they would be able to include their input in the final Assessment of Variation and Analysis of Solutions reports.

All teams made a conscious effort to assess the completeness of the coverage they had achieved between their VWG membership and the stakeholders they were able to engage. They solicited additional input through targeted recruitment as necessary to fill gaps. Many state teams reported that they cycled back to collect additional information as necessary to ensure that their information was sufficiently specific and complete. State teams also reported that they had distributed the larger, final set of business practices to the entire group of participants as a final quality control check on the accuracy of note-taking and data entry.

All state teams mapped legal drivers to business practices, although in some instances the work was not finished at the time of report submission. Rather than wait to receive business practice data, at least 12 LWGs chose, on the basis of their review of each scenario, to compile compendiums of relevant law. This method proved efficient, allowing LWGs to map legal drivers to business practices as soon as business practices became available.

Representativeness of Business Practices

In designing the process for assessing variation in business practices related to the privacy and security of health information exchange, the project team faced the major challenge of ensuring that the business practices identified by the states were comprehensive and represented the broad range of entities that might participate in HIEs. Stakeholder groups are numerous and often have many constituents within each group (e.g., providers). Seventeen groups were named in the request for proposals sent to each of the states and territories, with the option of identifying additional stakeholders (for a complete list of stakeholders, see Appendix C). Statistical sampling methods would have provided a quantitative approach to the information collection, but the process of engaging stakeholders and building relationships among organizations at the community level would have been compromised. Instead we opted for a microiterative approach.

First, the scenarios were developed to represent a wide range of stakeholders, as well as an array of contexts for HIE. Second, each participating state and territory was specifically required to demonstrate the capability to ensure participation by a wide range of stakeholders collectively representing the state's current environmental landscape, both within the stakeholder communities and geographically across each state. Third, the importance of engaging a broad coalition of stakeholder organizations was also covered during the training of each of the state teams to ensure that, as a practical matter, appropriate groups would participate in each state. Fourth, the design of the assessment process relies on a recursive approach, one in which practices identified by the VWG are vetted with larger groups of stakeholders at several points in the assessment process to identify and fill gaps.

2.2 Treatment (Scenarios 1–4)

1. Patient Care Scenario A

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89-year-old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. The patient may be impaired because of medications; that possibility is being investigated as well. Her adult daughter informed the ER staff that her mother was recently treated at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines the need to obtain information about patient X's prior diagnosis and treatment during the previous inpatient stay.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Determining status of the patient and chain of responsibility.
2. Practice and policy for obtaining information sufficient for treatment.
3. Practice and policy for handling mental health information.
4. Practice and policy for securing the data exchange mechanism.
5. Practice and policy related to authentication of requesting facility by the releasing facility.
6. Practice and policy related to patient authorization for the release of information.

2. Patient Care Scenario B

An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The 2 organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol that is relevant for medical diagnosis. The primary care provider has requested that the substance abuse information be sent by the treatment facility. The primary care provider intends to refer the patient to a specialist and plans to send all of the patient's medical information, including the substance abuse information that was received from the substance abuse treatment facility, to the specialist.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. How does the releasing organization obtain authorization from the patient to allow release of medical records?
2. What is the process for handling substance abuse medical records data?
3. How does the releasing organization authenticate the health care provider requesting the information?
4. How is the data exchange secured?

3. Patient Care Scenario C

At 5:30 p.m., Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psychiatric unit to the skilled nursing facility. The hospital and skilled nursing facility are separate entities and do not share electronic record systems. At the time of the patient's transfer, the discharge summary and other pertinent records and forms were electronically transmitted to the skilled nursing home.

When Dr. X enters the facility, he seeks assistance locating his patient, gaining entrance to the locked psychiatric unit, and accessing the patient's electronic health record to review the discharge summary, I&O, MAR, and progress notes. Dr. X was able to enter the unit by showing a picture identification badge, but was not able to access the electronic health record (EHR). As it is Dr. X's first visit, he has no log-in or password to use their system.

Dr. X completes his visit and prepares to complete his documentation for the nursing home. Unable to access the skilled nursing facility EHR, Dr. X dictates his initial assessment via telephone to his outsourced, offshore transcription service. The assessment is transcribed and posted to a secure Web portal.

The next morning, from his home computer, Dr. X checks his e-mail and receives notification that the assessment is available. Dr. X logs into his office Web portal, reviews the assessment, and applies his electronic signature.

Later that day, Dr. X's office manager downloads this assessment from the Web portal, saves the document in the patient's record in his office, and forwards the now encrypted document to the long-term care facility via e-mail.

The skilled nursing facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Agreements for data sharing—business associate agreements.
2. Setting out access and role management policies and practices for temporary or new access.
3. Determining appropriate access to mental health records.
4. Securing unstructured, possibly nonelectronic patient data.
5. Reliability of other entity security and privacy infrastructure.

4. Patient Care Scenario D

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the *BrCa* gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Authenticating entities and individuals.
2. Determining processes and laws for release of genetic and HIV information.

2.2.1 Stakeholders

For Scenarios 1 through 4, RTI suggested that hospitals, substance abuse treatment facilities, physicians, public health agencies, patient-consumers, and community clinics and health centers be included as the stakeholder groups engaged in the review of the scenarios and asked to describe business practices.

All stakeholder groups were engaged in the review of Scenarios 1 through 4, although participation among the groups was not uniform across the states. The frequency with which each of the stakeholder groups was engaged in the review and discussion is shown in Table 2-4. The most frequently engaged stakeholder groups were hospitals, engaged by all the state teams; physician groups (91%); clinicians (88%); long-term care facilities (59%); community clinics (53%); and consumers and consumer groups (50%).

Table 2-4. Stakeholder Groups Engaged in Scenario 1–4 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenarios 1–4 (N = 34)	Percentage of State Teams Engaging Stakeholder Group in Review of Scenarios 1–4 (%)
Hospital personnel/emergency room staff	34	(100)
Physician groups	31	(91)
Clinicians	30	(88)
Long-term care facilities	20	(59)
Public health agencies	19	(56)
Community clinics	18	(53)
Consumers/consumer groups	17	(50)
Behavioral health	13	(38)
State government	11	(32)
Nursing homes	10	(29)
Payers	9	(26)
Federal health facilities	8	(24)
Correctional facilities personnel	7	(21)
Homecare and hospice	6	(18)
Laboratories	6	(18)
Pharmaceutical companies	6	(18)
Professional associations	6	(18)
Schools	6	(18)
Health information management/transcription	5	(15)
Quality improvement organizations	5	(15)
Attorneys	5	(15)
Law enforcement	3	(9)

2.2.2 Domains

Table 2-5 shows the domains of privacy and security affected by business practices reported for each state team. Domains examined across the state teams showed little variation, with more than half of the state teams addressing 8 or 9 of the domains. The top 4 domain areas were

- Domain 2—Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information (97%);
- Domain 9—Information use and disclosure policies that arise as health care entities share clinical health information electronically (97%);
- Domain 1—User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be (91%); and
- Domain 4—Information transmission security or exchange protocols (i.e., encryption) for information that is being exchanged over an electronic communications network (91%).

2.2.3 Critical Observations

Critical observations related to the treatment scenarios were fairly uniform, although numerous variations were described in the management and transmission of health information. In many states, paper-based records are still the norm, and patient information is exchanged informally, most often verbally and by fax. In many circumstances, voice recognition, caller-ID, or requests received on letterhead were cited as the means for authenticating the individuals receiving the personal health information. In this context, privacy and security policies were unevenly implemented in practice. Stakeholders tended to rely heavily on already established relationships when they exchanged information, with voice recognition alone serving to authenticate the person receiving the information. For organizations that used an electronic health record (EHR), significantly more procedures were in place to protect patient information, including training, signed confidentiality statements, and access controls. Stakeholders experienced in electronic health information exchange indicated that most EHR systems did not include functionality for segregating specially protected health information. While most stakeholders respected the need for policies and procedures to protect personal health information, they also expressed a tension between having access to appropriate health information available to providers at the time it is needed, and having security policies and practices that make that access useable while respecting the patient's privacy. Many stakeholders who were private-practice physicians or part of a small group practice felt that the prohibitive cost of EHR systems that provided adequate levels of security was a significant barrier to electronic health information exchange.

Table 2-5. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenarios 1–4 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X	X	X	X	X	X	X
Arizona	X	X	X	X	—	X	X	X	X
Arkansas	X	X	X	X	—	—	X	X	X
California	X	X	—	—	—	X	—	X	X
Colorado	X	X	X	X	X	X	X	—	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida	X	X	X	X	—	—	X	X	X
Illinois	X	X	X	X	X	X	X	—	X
Indiana	—	X	—	X	X	X	—	—	X
Iowa	X	X	X	X	X	X	X	X	X
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	X	X	—	X	—	X	X	X	X
Louisiana	X	X	—	X	X	X	X	X	X
Maine	X	X	X	X	X	X	X	X	X
Massachusetts	X	X	X	X	X	—	X	X	X
Michigan	X	X	X	X	X	X	X	X	X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi	X	X	X	X	—	—	—	—	X
New Hampshire	—	—	—	—	—	—	—	—	X
New Jersey	X	X	—	X	—	—	X	X	X
New Mexico	X	X	X	X	X	X	X	X	X
New York	X	X	X	X	X	—	X	X	X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio	X	X	—	—	—	—	—	—	—
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	X	X	X	X	—	—	X	X	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	X	—	X	X	—	—	X	X
Utah	X	X	—	X	X	—	X	X	X
Vermont	X	X	X	X	X	X	X	—	X
Washington	X	X	X	X	X	X	X	X	X
West Virginia	X	X	X	X	X	X	X	X	X
Wisconsin	X	X	X	X	X	X	X	X	X
Wyoming	X	X	X	X	—	—	—	—	X
Total	31 (91%)	33 (97%)	25 (74%)	31 (91%)	22 (65%)	22 (65%)	26 (76%)	27 (79%)	33 (97%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

In nearly all states, additional protections and restrictions were placed on special categories of specially protected information, including drug and alcohol diagnoses and treatment, mental health information, HIV/AIDS diagnoses, and genetic information. Some states mentioned business practices they used that provided a work-around to sharing such information when necessary (such as dictating the information into the patient record). Many states indicated that while sexual health information is not part of the legally protected category, with the exception of HIV/AIDS status, most providers attach additional protections to sharing such information in light of protecting their patients' privacy. A few states indicated that 42 C.F.R. pt. 2 provides a higher degree of protection for behavioral health information than the HIPAA Privacy Rule.

The Privacy Rule requires that covered entities make reasonable efforts to use and release only the *minimum necessary* protected health information to achieve the intended purpose. The state teams reported widespread variation, however, in how the *minimum necessary* standard is interpreted and applied. The state teams reported no clear definition of *minimum necessary* in any given situation. The level of information provided to satisfy this standard varies not only from organization to organization, but also among people within the same organization. Many states suggested that, because the standard is a reasonableness standard and is variable and flexible, it lends itself to multiple interpretations that create variability, which, in turn, poses a challenge to electronic health information exchange. In addition, there is misunderstanding of when and how to apply the standard that also adds to the variable application.

Analysis of Scenario 2 also illustrated that many providers are reluctant to share health information and will request consent even in routine treatment circumstances. With respect to the Privacy Rule, "consent" for the release of health information (which is permitted, but not required, for treatment payment and health care operations) is often confused by stakeholders with *authorization*, which is often required to exchange health information for other purposes.⁸ More frequently, it is state law or organizational policy that requires consent for treatment.

Even though obtaining patient consent is a widespread practice across providers in most states, the policies and procedures for obtaining consent vary considerably, as do working definitions of the term *consent*.

Many stakeholders do not fully understand the interstate exchange of health information and the request for health information for out-of-state patients. The state teams identified broad variation in practices followed to exchange health information, including variation in data definitions, transmission protocols, and authentication protocols. Definitions of key

⁸ The terms *consent* and *authorization* have specific legal meanings in the context of various state and federal laws, including the HIPAA Privacy Rule. Although context must be considered when determining the proper term to use under a specific law, here the term consent is used to generally mean a signed permission to release or disclose PHI, unless otherwise noted.

data elements describing procedures, treatments, and patient characteristics are inconsistent across entities, compromising the comparability of health information maintained by different providers. In addition, both paper-based and electronic information systems employ a wide range of incompatible practices that can lead to misinterpretation by users outside of the originating systems. Differing legal definitions used in licensing health professionals provide an additional degree of complication when examining interstate health information sharing.

Lack of a consistent, accurate method for tracking individuals and linking their multiple disparate patient records presents a challenge whenever health information is shared across organizational boundaries. Various algorithms provide a relatively high level of matching given a few pieces of personal information, although no algorithm-based system can assure 100% accurate matching. The reverse situation, where more than one individual's health information is contained in one record, is commonplace in states with large numbers of uninsured and possibly illegal aliens.

2.3 Payment (Scenario 5)

5. Payment Scenario

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the health care provider serves. As part of the insurance coverage, the health plan case managers must approve/authorize all inpatient encounters. This requires access to patient health information (e.g., emergency department records, clinic notes).

The health care provider has recently implemented an EHR system. All patient information is now maintained in the EHR and is accessible to users who have been granted access through an approval process. Access to the EHR has been restricted to the health care provider's workforce members and medical staff members and their office staff.

X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Get patient authorization to allow payer access.
2. Facility needs to determine the minimum necessary and limit to pertinent time frame.
3. If allowed, access and role management are issues.
4. Determine method for enabling secure remote access if allowed.

2.3.1 Stakeholders

Overall, the state teams included a wide variety of stakeholders in discussions for Scenario 5. While some states were able to draw from a large pool of stakeholders, other states were able to include only a few stakeholders for this scenario. Although stakeholder variation among states was great, 2 of the stakeholder groups that would be most directly affected by this scenario were well represented: 31 of the 34 state teams included a payer stakeholder in discussions, and 28 of the 34 included hospital personnel (Table 2-6). In contrast, consumers, another stakeholder group highly likely to be affected by this scenario,

Table 2-6. Stakeholder Groups Engaged in Scenario 5 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 5 (N = 34)	Percentage of State Teams Engaging Stakeholder Group in Review of Scenario 5 (%)
Payers/insurance	31	(91)
Hospital personnel/emergency room staff	28	(82)
Consumers/consumer organizations	14	(41)
State government	12	(35)
Clinicians	11	(32)
Physician groups	11	(32)
Homecare and hospice	11	(32)
Community clinics and health centers	9	(26)
Federal health facilities	9	(26)
Long-term care facilities/nursing homes	7	(21)
Public health agencies	7	(18)
Professional associations	7	(18)
Pharmacies	5	(15)
Information security	3	(9)
Quality improvement organizations	3	(9)
Medical and public health schools that undertake research	3	(9)
Laboratories	2	(6)
Correctional facilities personnel	2	(6)
Health IT personnel	2	(6)
Regional health information organization (RHIO) representatives	1	(3)
County government	1	(3)
Substance abuse centers	1	(3)

were represented in only 14 states. Other common stakeholder groups were state government, clinicians, physician groups, and homecare/hospice, each represented in 11 to 12 states.

2.3.2 Domains

The state teams varied widely in their views about Scenario 5: some thought that all 9 domains were relevant to this scenario and others felt that this scenario involved only 1 or 2 domains. Despite this variation, 29 of the 34 of the state teams reported that Domain 2—Information authorization and access control to allow access only to people or software programs that have been granted access rights to electronic personal health information—was related to this scenario.

To ensure that users have access only to appropriate information, state teams use procedures such as log-in names and passwords to help identify the user and role-based access. Some state teams found that nonexistent access control procedures in partner organizations were a barrier to electronic health information exchange. Additionally, some state teams found that hospital systems and payers do not use a standardized protocol for role-based access beyond their own facility and, therefore, cannot distinguish whether users from other facilities have permission to access treatment data, specially protected data, or more general data. A related issue was the lack of access to organizations' electronic systems by third-party administrators. Most organizations do not allow any kind of remote access to their systems by outside parties.

Twenty-six of the 34 state teams listed Domain 9—"Information use and disclosure policies that arise as health care entities share clinical information electronically"—as valid for this scenario (Table 2-7). State teams found that many health care providers have no written policies to address this issue. They agreed that patients authorize release for payment purposes (not for access to medical records), that patient consent is required by the payer before any disclosure, and that payers should have access to only *minimum necessary* patient information.

Domain 1—"User and entity authentication is used to verify that a person or entity seeking access to electronic personal health information is who they claim to be" was the third most common domain cited by the state teams for the payer scenario. Of the 34 states, 21 felt this domain was relevant to Scenario 5. Currently, most providers ask for a written request from the insurance company or use a call-back procedure to authenticate the identity of the requestor if they are not in regular contact with the person calling.

2.3.3 Critical Observations

A common theme among the states was the issue of access to electronic data by outside entities, specifically payers. The state teams reported that hospitals currently do not allow third-party payers access to their EHR, and access by nonhospital personnel is generally restricted and often limited to hard copies of medical records. Payer stakeholders agreed that if they did not already have the information they were seeking through their own claims data, they would request the additional information using a paper-based procedure for release of information.

While the states agree that disclosures relating to payments do not require consent or *authorization* under the HIPAA Privacy Rule, states and providers express confusion about the amount of patient information required to meet the *minimum necessary* requirement of the Privacy Rule. States reported that what constitutes the *minimum necessary* information seemed to vary among organizations, as well as within the same organization. They were also concerned about the ability to segregate information in an EHR to meet the *minimum necessary* requirements. States that are unable to segregate the data feel that they would

Table 2-7. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 5 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X	X	X	X	X	X	X
Arizona	X	X	X	X	—	X	X	X	X
Arkansas	X	X	X	X	X	—	—	—	X
California	—	X	—	—	—	X	X	—	X
Colorado	—	X	—	—	—	—	X	—	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida	—	X	—	—	—	—	—	X	X
Illinois	X	X	—	—	—	—	—	X	—
Indiana	—	X	—	—	X	—	—	—	—
Iowa	—	X	X	X	X	X	X	—	X
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	X	X	—	X	X	X	X	X	X
Louisiana	X	X	X	—	—	X	X	—	—
Maine	X	X	—	—	—	X	—	—	—
Massachusetts	—	—	—	—	—	—	—	X	X
Michigan	X	X	X	X	X	X	—	—	X
Minnesota	X	X	—	—	X	X	X	X	X
Mississippi	—	X	—	X	—	X	—	—	X
New Hampshire	—	—	—	—	—	—	—	—	X
New Jersey	X	X	—	X	—	—	—	X	—
New Mexico	—	X	—	—	—	—	—	X	—
New York	X	X	—	—	—	—	X	—	—
North Carolina	X	X	X	X	—	X	—	—	X
Ohio	—	X	—	—	—	—	—	—	X
Oklahoma	X	X	X	X	X	—	X	X	X
Oregon	X	—	—	—	—	X	X	—	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	X	—	—	—	—	—	—	X
Utah	—	X	—	—	—	—	—	—	X
Vermont	—	X	—	X	—	X	—	—	X
Washington	X	X	X	X	X	X	X	—	X
West Virginia	X	—	X	X	—	—	—	X	—
Wisconsin	X	X	—	X	X	—	—	X	X
Wyoming	X	—	—	—	—	—	—	—	X
Total	21 (62%)	29 (85%)	13 (38%)	17 (50%)	13 (38%)	17 (50%)	15 (44%)	15 (44%)	26 (76%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

be stuck in an “all or nothing” situation when sharing data and would not share any data electronically for fear of improperly disclosing information. The issue of granting access in a HIPAA-compliant manner was a concern commonly reported by the state teams.

Patient consent was another issue discussed in many state team reports. Most states agreed that when a patient signs a release form, it is for permission to release only that information necessary for payment purposes and not for the payer’s access to his or her entire medical record. The state team reports indicate wide variation among organizations in deciding when patient consent is required; how the consent is obtained and documented; and how patient consent is communicated to health care organizations, payers, and other outside entities.

In their discussions of the domains of authorization and access controls, the state teams reported that providers use means such as log-in names and passwords to limit access to electronic information. Most stakeholders agreed that only approved users with current business associate agreements (BAAs), contracts, or some other type of legal agreement with the provider would be allowed access to the EHR. Access to the EHR would be time-sensitive, with information specific to the current admission. Additionally, role-based access helps ensure users have access only to the information that they need, not the entire EHR. However, many hospitals have role-based access criteria only for their own facility, which is often not compatible with other facilities. Common criteria must be established for this security measure to be effective in controlling access by outside parties. Time and effort must be spent in developing an electronic system that will restrict access where necessary instead of allowing complete EHR access to all users. Additionally, a database of approved users and executed agreements would need to be maintained and constantly updated to reflect changes in the status of users. State teams that addressed this issue found that providers were currently unwilling to spend the time and money necessary to make these provisions.

Another common theme is the issue of trust. While consumers would like to have their health records available electronically, they have also expressed a general concern about who can access their health information and for what purposes. In essence, they would like for their information to be easily accessible, but at the same time be completely private and secure. Many consumers would also like control over who has access to their medical records. Patients do not trust payers and employers to refrain from using their EHR in an improper way if they have access to it. In addition, some patients are concerned that the release of records containing information related to drug abuse, mental health, alcoholism, or HIV/AIDS may cause substantive harm to individuals and families.

Providers also distrust EHRs; they are concerned the information will be used against them in setting rates. Providers do not trust that others who participate in electronic health information exchange will protect health information to the same degree that they

themselves do, thereby exposing them to potential liability. Additionally, providers have a certain level of discomfort in allowing payers to have broad access to EHRs; they are concerned that payers might access EHRs that are not relevant to the patient being treated.

Technology-based solutions, such as restricting access to relevant records only, maintaining a log of payer activities, and providing read-only access to combat the possibility of a payer improperly modifying a record, will help to alleviate concerns. Otherwise, this lack of trust might lead to organizations' and individuals' refusals to participate in an HIE if it becomes available. Substantively addressing these concerns, as well as educating both the public and providers about security policies and measures, will be crucial to achieving widespread participation in electronic health information exchange.

Related to the issue of distrust of EHRs is the cultural issue of comfort with paper systems. Many providers reported that they have used the paper system, including the use of phone and fax, for years and were uncomfortable using new and unfamiliar technologies. However, the providers do recognize that an EHR would be more efficient, allow for a more complete patient history from a variety of sources, and can be more secure than paper records if security is correctly applied. Payers and providers both admitted to a sense of uncertainty about who actually sees a record when it is faxed.

2.4 Regional Health Information Organization (RHIO; Scenario 6)

6. RHIO Scenario

The RHIO in your region wants to access patient-identifiable data from all participating organizations (and their patients) to monitor the incidence and management of diabetic patients. The RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Decision to utilize medical record data to monitor disease management.
2. Authorization from patients to allow RHIO to monitor their PHI for disease management.
3. Determine mode of transferring information and type of information, i.e., identifiable or de-identified information to the RHIO.

2.4.1 Stakeholders

Scenario 6 was included to provide a context for discussions in states that currently have HIE activity. The generic term *RHIO*, or *regional health information organization*, was used in this scenario to describe an HIE. However, no definition of the term *RHIO* was provided, leaving it open to the state teams to define as needed. While some states have one or more RHIOs, other states have organizations that only participate in HIE at a local level. During the discussions that follow, an HIE of any kind is referred to as a RHIO.

A total of 6 state teams offered no responses for this scenario because their states currently have no RHIOs in operation. As shown in Table 2-8, the 28 state teams that responded to this scenario included a wide variety of stakeholders in discussions. Because of this diversity, the most common stakeholder, hospitals, appeared in only 17 of the 28 responding states. Other common stakeholders, represented in between 10 to 12 states, were payers, public health agencies, physicians groups, clinicians, professional associations, and community clinics and health centers.

Table 2-8. Stakeholder Groups Engaged in Scenario 6 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 6 ^(a) (N = 28)	Percentage of State Teams Engaging Stakeholder Group in Review of Scenario 6 ^(a) (%)
Hospitals	17	(61)
Payers	12	(43)
Public health agencies	12	(43)
Physician groups	11	(39)
Clinicians	11	(39)
Professional associations	11	(39)
Community clinics and health centers	10	(36)
Consumers/consumer organizations	9	(32)
Pharmacies	9	(32)
Homecare and hospice	8	(29)
Long-term care facilities/nursing homes	8	(29)
Federal health facilities	8	(29)
RHIO representatives	7	(25)
Laboratories	6	(21)
State government	6	(21)
Correctional facilities personnel	5	(18)
Medical and public health schools that undertake research	5	(18)
Quality improvement organizations	3	(11)
Information security	2	(7)
Health information management	2	(7)
Data vendors	2	(7)
Law enforcement	1	(4)
Mental health	1	(4)
Attorneys	1	(4)
County government	1	(4)
Advocacy groups	1	(4)

^a Six of the 34 states did not respond to the RHIO scenario.

2.4.2 Domains

Two state teams responded to this scenario but did not list any domains related to it, leaving a total of 26 states that selected domains. As with other scenarios, opinions varied widely among the states as to which domains were relevant to this scenario. Limited stakeholder response to this scenario in some states may have had an effect on the domains selected.

Of the 26 states that selected domains for this scenario, 22 listed Domain 9—“Information use and disclosure policies that arise as health care entities share clinical information electronically”—as relevant to this scenario (Table 2-9). States agreed that sharing de-identified data with the RHIO for disease surveillance would not necessarily be a problem, but patient or institutional review board (IRB) approval would be necessary to send identifiable data to the RHIO for research or surveillance purposes. Additionally, hospitals would require a BAA or confidentiality agreement with the RHIO before they send data.

Seventeen states selected Domain 2—“Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information”—as relevant to this scenario; 17 states also selected as relevant Domain 4—“Information transmission security or exchange protocols for information that is being exchanged over an electronic communications network.” States indicated that proper encryption methods, or use of a secure file transfer protocol (FTP), were needed to transmit data to the RHIO. Additionally, access to personal health information transmitted through a RHIO is usually role-based, with permissions set according to an individual’s affiliation with one of the connecting institutions.

2.4.3 Critical Observations

Some states were uncertain about the functions of a RHIO, specifically as they relate to data collection, analysis, and disease management. Several state teams were unsure of a RHIO’s legal status in their state, and opinions differed as to whether a RHIO was a HIPAA-covered entity. One state team mentioned the lack of a uniform definition for a RHIO; in addition, a RHIO was not recognized as a specific legal entity in that particular state. The general consensus among provider and hospital stakeholders in states where a RHIO has uncertain status was that they were reluctant to input information into the RHIO if it was not subject to the HIPAA Rules or state regulations.

Although the scenario indicated that the RHIO wanted to “access patient-identifiable data,” most states responded that they would share only de-identified data with the RHIO. Patient consent would be required for the RHIO to receive patient-identifiable data. Several state teams mentioned that no current state laws prohibited the use of medical information to monitor disease management if the data are de-identified and the patients are not contacted.

Table 2-9. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 6 (N = 26)*

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	—	X	X	—	—	—	—	X
Arizona	—	—	—	—	—	—	—	—	—
Arkansas	—	—	—	—	—	—	—	—	—
California	—	X	—	—	—	—	—	—	X
Colorado	—	X	X	X	—	—	—	X	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida	—	—	—	—	—	—	—	X	X
Illinois	X	X	—	—	—	—	—	X	—
Indiana	—	—	—	X	—	—	—	—	X
Iowa	—	X	X	X	—	—	X	X	—
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	X	X	—	X	X	X	X	X	X
Louisiana	X	X	—	X	—	—	X	—	X
Maine	—	—	—	X	—	—	—	—	X
Massachusetts	—	—	—	X	—	—	—	X	X
Michigan	X	X	—	—	—	—	—	—	X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi	—	—	—	X	—	—	—	—	X
New Hampshire	—	—	—	—	—	—	—	—	—
New Jersey	—	—	—	—	—	—	—	—	—
New Mexico	—	X	—	—	—	—	—	X	—
New York	—	X	—	—	—	—	—	—	X
North Carolina	—	X	X	X	X	X	X	—	X
Ohio	—	—	—	—	—	—	—	—	X
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	—	—	—	—	—	—	—	—	—
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	—	—	—	—	—	—	—	—
Utah	—	—	—	—	—	—	—	—	—
Vermont	—	—	—	—	—	—	—	—	—
Washington	—	—	—	X	—	—	X	—	X
West Virginia	—	—	X	—	—	—	—	X	X
Wisconsin	X	X	—	X	—	—	—	X	X
Wyoming	—	X	—	—	—	—	—	—	—
Total	11 (42%)	17 (65%)	10 (38%)	17 (65%)	7 (27%)	7 (27%)	10 (38%)	14 (54%)	22 (85%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

*In addition to the 6 state teams that did not respond to this scenario, 2 state teams out of the 34 did not list any domains associated with this scenario.

According to states, verification of patient identification across different systems can be an issue. One organization may have more up-to-date or complete demographic information than another organization and, therefore, be able to better identify the correct patient. Currently, each organization—hospital, clinic, physician office, or RHIO—employs its own algorithm and patient-matching methods, resulting in inconsistent patient matching. Compounding the problem is the prohibition of using Social Security numbers in medical records in certain states, making patient matching even more difficult. One state has indicated that its statewide RHIO will host a master patient and provider index, as well as provide a variety of functions and rules for matching records across all providers and locations. These functions will allow the RHIO to support identification of particular populations of individuals as required for disease management, to provide clinical decision supports to providers, and to identify and aggregate data as required for performance monitoring.

State teams agreed that, if information is to be exchanged, whether it is patient-identifying or de-identified, security is very important. To remain compliant with the HIPAA Rules, state teams indicated that they would need a BAA or, in the case of one state, a data subscription agreement (DSA) with the RHIO before sending identifiable data. Data files would have to be sent encrypted or be uploaded to a secure website. The RHIO itself would need to have security measures such as password-protected computers, credentialing and authentication of users, and role-based access in place to keep any data it received secure. Additionally, all partner organizations in the RHIO must have adequate and comparable levels of critical factors such as credentialing and authentication of system users and system security. State teams are concerned that if a minimum standard for system security is not met, a participant with weak security measures could compromise the security of all participants.

Some state teams did not want RHIOs to rank participating providers. Some specific concerns included the following: the ranking of providers would likely jeopardize the neutrality of a RHIO; a RHIO must have broad participation, and providers might not want to participate if they know they are being ranked; providers who participate may be unfairly compensated because of referrals associated with their ranking; and consumers may mistakenly assume that a nonparticipating provider is somehow better than a ranked, participating provider.

Another common theme among the state teams regarding RHIOs was the different level of technical capabilities of organizations (large versus small, urban versus rural), a difference that amounts to a capacity gap for some entities that may participate in those RHIOs. Some providers are not currently participating in RHIOs because they still operate a paper-based medical records system, or they cannot bear the cost of connectivity with the RHIO.

2.5 Research Data Use Scenario (Scenario 7)

7. Research Data Use Scenario

A research project on children younger than age 13 is being conducted in a double-blind study for a new drug for ADD/ADHD. The research is sponsored by a major drug manufacturer conducting a double-blind study approved by the medical center's IRB, where the research investigators are located. The data are collected electronically, and all responses from the subjects are completed electronically on the same centralized and shared database file.

One of the investigators asked the principal investigator if he could use the raw data to extend the patient tracking for an additional 6 months or use the raw data collected for a white paper that was not part of the research protocols final document for his postdoctoral fellow program.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. IRB approval of any significant changes to the research protocol.
2. Research subjects have signed consents and authorization to participate in the research effort.

2.5.1 Stakeholders

All states included representatives from university research groups, health care providers representing both hospitals and clinics, members of IRBs, and consumer advocates in this discussion. States emphasized the inclusion of stakeholders from medical schools and their hospitals' clinical research staff members. Some states specifically mentioned the inclusion of correctional facilities officials. One state noted that its stakeholders for this scenario included participants in clinical trials, as well as a grants administrator familiar with human subjects research guidelines. A few states included stakeholders from hospice, long-term care, and nursing home facilities (Table 2-10).

2.5.2 Domains

Domains 9 and 2 were the 2 most often cited domains by the states. Eighty-eight percent of the states identified Domain 9—"Information use and disclosure policies that arise as health care entities share clinical information electronically"—as most relevant to the scenario's topic, and these states reported significant disagreement among their stakeholders about limitations of the permitted scope of research under the original IRB approval. In Domain 2, more than half the states focused on its requirement that the patient, or consumer, authorize the researcher to access that patient's data. The other 7 domains were nearly evenly selected by a third or so of the states (Table 2-11).

The other 7 were also mentioned in regard to proper data storage and data sharing activities. Stakeholders frequently discussed de-identification procedures, data encryption requirements, and the scope of the requested research protocol, as related to the other domains for user and entity authentication, information authorization and access controls,

Table 2-10. Stakeholder Groups Engaged in Scenario 7 Reviews

Stakeholder Group	Number of States Engaging Stakeholder Review of Scenario 7 (N = 34)	Percentage of States Engaging Stakeholder Review of Scenario 7 (%)
Medical and public health schools that undertake research	23	(67)
Hospital personnel/ER staff	17	(50)
Clinicians	15	(44)
Consumers	14	(41)
Public health agencies	11	(32)
IRB members	9	(26)
Physicians	9	(26)
State government	8	(24)
Federal health facilities	4	(12)
Homecare and hospice	4	(12)
Community clinics and health centers	3	(9)
Pharmacies	3	(9)
Professional associations	3	(9)
Laboratories	3	(9)
Payers	3	(9)
Long-term care facilities/nursing homes	3	(9)
Information security	1	(3)
Quality improvement organizations	1	(3)
Correctional facilities personnel	1	(3)
Attorney	1	(3)

information transmission security or exchange protocols, and administrative or physical security safeguards.

2.5.3 Critical Observations

State teams held many lively discussions about specific requirements the IRB imposed on the Scenario 7 researcher; nearly all stakeholders reported that the IRB approval process was the most significant discussion point for the provision of data in this scenario.

Stakeholder groups in 6 states expressed concerns that participating in a RHIO requires a high level of trust that patient information will be protected. Eight state stakeholder groups discussed ways in which personal health information can be used for quality improvement versus research purposes while meeting HIPAA Privacy Rule restrictions. Stakeholders agreed that identifiable health information can be used for quality improvement, but if the results are to be made publicly available and if the primary purpose for using the data is for generalizable knowledge, patient *authorization* must be obtained. Regarding physical data

Table 2-11. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 7 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X	—	X	—	X	—	—
Arizona	X	X	—	X	X	—	—	—	X
Arkansas	—	X	—	X	—	X	X	X	X
California	—	—	—	—	—	X	—	—	X
Colorado	—	X	—	—	—	—	X	—	X
Connecticut	X	X	X	X	X	X	X	—	—
Florida	—	X	—	—	—	—	—	X	X
Illinois	—	—	—	—	—	—	—	—	X
Indiana	—	X	—	—	—	—	—	—	X
Iowa	—	X	—	—	—	—	X	—	X
Kansas	X	X	—	X	X	X	X	X	X
Kentucky	—	—	—	—	—	X	X	—	X
Louisiana	—	X	X	—	X	—	—	—	X
Maine	—	—	—	—	—	—	—	—	X
Massachusetts	—	—	—	—	—	—	—	X	X
Michigan	X	X	—	X	X	—	X	X	X
Minnesota	—	X	—	—	—	X	X	X	—
Mississippi	—	—	—	—	X	—	—	—	X
New Hampshire	—	—	—	—	—	—	—	—	X
New Jersey	—	—	—	—	—	—	X	—	X
New Mexico	—	X	—	—	X	—	—	—	X
New York	—	X	X	—	—	—	—	X	X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio	—	X	—	—	—	—	—	—	—
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	—	X	—	—	—	—	—	X	X
Puerto Rico	X	X	X	X	X	X	X	—	X
Rhode Island	—	—	—	—	—	—	—	—	X
Utah	—	—	—	—	—	—	—	—	X
Vermont	X	X	—	X	—	X	—	—	X
Washington	—	X	X	X	—	X	—	—	X
West Virginia	—	X	X	—	—	—	—	X	X
Wisconsin	X	X	X	X	X	—	—	—	X
Wyoming	—	—	—	—	—	—	X	—	X
Total	10	23	10	11	12	11	14	11	30

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

security, state teams also noted the difficulty of assessing compliance with confidentiality policies and practices for access and use of data by researchers on personal laptops/computers.

In these groups, questions arose about how systems prevent or detect the unauthorized extraction of a data set from a server. Ten states noted that Privacy Rule–required *authorizations* for research may expire and that any reuse of data after the *authorization* expiration may require a new *authorization* from the patient. While the health care provider, not the researcher, typically recontacts the patient, these state teams suggested that opportunities to expand the initial *authorization* in consideration of information reuse and electronic information exchanges should be explored to better enable reuse of valuable research data. Lastly, they noted that if research data were de-identified, the Privacy Rule would no longer apply to the de-identified data.

In their critical observations regarding Scenario 7, states generally agreed that even with IRB approval of the revised protocol, their stakeholders would always obtain a new *authorization* to cover the extended time period or additional data use.

2.6 Law Enforcement (Scenario 8)

8. Scenario for Access by Law Enforcement

An injured 19-year-old college student is brought to the ER following an automobile accident. Standard procedure is to run blood-alcohol and drug screens. The police officer investigating the accident arrives in the ER, claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood-alcohol test results, and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff.

The patient is covered under his parents' health and auto insurance policy.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. County contracts with emergency department to perform blood-alcohol test draws.
2. Printing of additional copies of medical record reports for parents, insurance companies, and police.
3. Asking patient if it is okay to talk to parents or give information to parents about his condition.
4. Communicating with primary care provider.

2.6.1 Stakeholders

Overall, the state teams included a wide variety of stakeholders in discussions for Scenario 8. The average number of stakeholder groups with input to the scenario was 3.3. Three states, however, were able to draw from more than 7 different stakeholder groups. Because this scenario had a significant law enforcement component, 61% of the state teams (21 of 34) were able to secure the participation of law enforcement personnel in the discussion of this scenario.

Although the stakeholder variation among state teams was great, 26 of the 34 states included a hospital physician stakeholder in discussions, and 16 of the 34 included clinicians or physicians. These stakeholders, along with consumers who were engaged by 12 of the 34 state teams, are the groups that would be most directly affected by this scenario (Table 2-12).

Table 2-12. Stakeholder Groups Engaged in Scenario 8 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 8 (N = 34)	Percentage of State Teams Engaging Stakeholder Group in Review of Scenario 8 (%)
Hospitals	26	(76)
Law enforcement	21	(61)
Physician groups	16	(47)
Consumers/consumer organizations	12	(35)
Clinicians	11	(32)
State government	7	(20)
Payers/insurance	6	(18)
Public health agencies	6	(18)
Laboratories	4	(12)
Community clinics	4	(12)
Federal health facilities	3	(9)
Emergency services	2	(6)
Long-term care facilities/nursing homes	2	(6)
Homecare and hospice	1	(3)
Pharmacies	1	(3)
Professional associations	1	(3)

2.6.2 Domains

Wide variation emerged in how the state teams viewed this scenario. Some states felt that all 9 domains were relevant to this scenario, while other states felt that this scenario involved only 1 or 2 domains (Table 2-13).

Despite this variation among the state teams, 30 of the 34 teams stated that Domain 9—“Information use and disclosure policies that arise as health care entities share clinical information electronically”—was valid for this scenario. Most state teams agreed that hospitals must receive formal service of a subpoena before information can be released to law enforcement. However, several state teams noted that they were aware of variations in responses to law enforcement requests among emergency departments in their states, with some departments more willing than others to release information on the basis of a verbal request rather than a formal subpoena. State teams generally agreed that variations in business practices occur because health care organizations and law enforcement do not

Table 2-13. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 8 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	—	X	X	—	—	—	—
Arizona	—	—	—	—	—	—	—	—	X
Arkansas	—	X	—	X	X	—	—	X	X
California	—	—	—	—	—	—	—	—	X
Colorado	—	—	—	—	—	—	—	—	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida	—	X	—	—	—	X	—	X	—
Illinois	—	X	—	—	—	—	—	—	—
Indiana	—	—	—	—	—	—	—	X	X
Iowa	—	X	—	—	—	—	—	X	X
Kansas	—	X	X	X	—	X	—	—	X
Kentucky	—	X	—	—	—	—	—	X	X
Louisiana	—	X	—	—	—	—	X	X	X
Maine	—	—	—	—	—	—	—	X	X
Massachusetts	—	—	—	—	—	—	—	—	X
Michigan	X	X	—	X	—	X	X	—	X
Minnesota	X	X	—	—	—	X	X	X	X
Mississippi	—	—	—	—	—	—	—	—	X
New Hampshire	—	—	—	—	—	—	—	—	X
New Jersey	X	—	—	—	—	—	—	X	X
New Mexico	—	—	—	—	—	—	—	—	X
New York	—	X	—	X	—	X	X	—	X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio	—	—	—	—	—	—	—	X	X
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	—	X	—	—	—	—	—	X	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	—	—	—	—	—	—	—	X
Utah	—	—	—	—	—	—	—	—	X
Vermont	X	X	—	X	—	X	—	X	—
Washington	—	—	—	—	—	—	—	—	X
West Virginia	X	X	X	X	X	X	X	X	X
Wisconsin	X	X	X	X	—	X	—	X	X
Wyoming	—	—	—	—	—	—	—	—	X
Total	11	19	7	12	7	12	9	18	30

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

seem entirely sure about the law and because interpretation of the HIPAA Privacy Rule varies. At least 5 states expressed a related concern about the inadequacy of confidentiality training.

All state teams agreed that no information would be released to the parents of an adult child. Five state teams noted that hospitals handle the presence of parents of adult children patients in the emergency department in nonstandard and varying ways. Five state teams also noted that some children are legally emancipated before their 18th birthday and have the right to limit access to their personal medical record without parental consent, even if they are insured under their parent's medical insurance policy.

2.6.3 Critical Observations

State teams agreed that this scenario reveals a clear chasm between the medical community and law enforcement, and this chasm severely restricts the exchange of information. Because law enforcement personnel reported that they try to obtain as much information as possible before transporting a person to a hospital, several state teams noted how each group's lack of understanding and their differing roles could impact the treatment of the person detained. Law enforcement considered the delay in transportation a necessary operating procedure because difficulties in collecting information greatly increase once an injured person enters a medical facility.

Another critical observation related to the potential loophole in the privacy of the adult child's health information while he or she is covered by a parent's insurance. Several states noted that a parent's receipt of the explanation of benefits from the insurance agency would likely contain enough information about billing for the health care service to enable parents to learn medical information to which they would not otherwise be entitled. This situation could be viewed as a serious barrier to care if a person opted to forgo care because a related or unrelated third party was responsible for payment.

2.7 Prescription Drug Use (Scenarios 9 and 10)

9. Pharmacy Benefit Scenario A

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy for a hospital that is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's outpatient clinic.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Patient authorization to share information with the PBM.
2. Agreements for data sharing—BAAs.
3. Health care provider must determine *minimum necessary* access to PHI.

4. If allowed, role and access management.
5. Method for enabling secure remote access if allowed.

10. Pharmacy Benefit Scenario B

A PBM (PBM1) has an agreement with Company A to review the companies' employees' prescription drug use and the associated costs of the drugs prescribed. The objective would be to see if PBM1 could save the company money on its prescription drug benefit. Company A is self-insured and, as part of its current benefits package, has prescription drug claims submitted through its current PBM (PBM2). PBM1 has requested that Company A send its electronic claims to them to complete the review.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. BAAs and formal contracts exist between Company A and the PBMs.
2. The extent and amount of information shared between the various parties would be limited by the *minimum necessary* guidelines.

2.7.1 Stakeholders

For Scenario 9, RTI suggested that community clinics and health centers, pharmacies, and consumers (patients) should be engaged in the review of the scenario and asked to describe business practices. Additional stakeholder groups that might be able to describe practices associated with the scenario included clinicians, physician groups, and payers.

For Scenario 10, RTI suggested that, at a minimum, pharmacies, consumers (employees), and employers should be engaged in the review, and that clinicians, physician groups, payers, and community clinics and health centers might be able to provide additional insight.

Table 2-14 shows that those suggested stakeholder groups were among the most frequently engaged groups, along with hospitals/health systems and Medicaid/other state government.

Seven states did not report engaging pharmacies or PBMs. Other stakeholders included nurses and academicians.

2.7.2 Domains

Wide variation across states emerged, with 7 states reporting that 8 or 9 domains of privacy and security were affected by business practices, and 8 states reporting that only 1 or 2 domains were affected. The 3 most frequently cited domains were 9—"Information use and disclosure policies" (28 states), 4—"Transmission security" (25 states), and 2—"Authorization and access control" (20 states; see Table 2-15).

BAAs and *minimum necessary* were the most common issues raised in discussions of Domain 9—"Information use and disclosure policies." Twenty states reported that data could be exchanged with PBMs if the provisions in the HIPAA Privacy Rule were met; that is, if BAAs were in place and *minimum necessary* information were disclosed, data could be exchanged without patient *authorization*. One state explicitly noted that the patient would

Table 2-14. Stakeholder Groups Engaged in Scenario 9 and 10 Reviews

Stakeholder Group	Number of States Engaging Stakeholder Group in Review of Scenarios 9 and 10 (N = 34)	Percentage of States Engaging Stakeholder Group in Review of Scenarios 9 and 10 (%)
Pharmacies/pharmacy benefit managers	27	(79)
Payers	20	(59)
Hospitals/health systems	17	(50)
Physicians and physicians groups	16	(47)
Clinicians	15	(44)
Consumers/consumer advocates	14	(41)
Community clinics and health centers	12	(35)
Medicaid/other state government	11	(32)
Employers	10	(29)
Public health agencies or departments	6	(18)
Federal health facilities	5	(15)
Professional associations and societies	5	(15)
Medical and public health schools/research	5	(15)
Homecare and hospice	4	(12)
Electronic health records experts	4	(12)
Mental health and behavioral health	3	(9)
Long-term care facilities and nursing homes	3	(9)
Privacy and security experts/compliance officers	3	(9)
Regional health information organizations	2	(6)
Health information managers	2	(6)
Health IT consultants	2	(6)
Other	2	(6)
Emergency medicine	1	(3)
Laboratories	1	(3)
Quality improvement organizations	1	(3)
County government	1	(3)
Safety net providers	1	(3)

be informed of this relationship and the potential need for information-sharing at the time of enrollment.

One state reported that the state board has no oversight of PBMs, and suggested that adding this would strengthen their approach to data management. Two states noted that patient *authorization* would be required before specially protected mental health pharmacy data could be shared. Another state reported that their provider stakeholders believed that patient *authorization* was required for this data exchange, but their LWG determined that this was not based in state law. Regarding *minimum necessary*, states generally agreed that

Table 2-15. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenarios 9 and 10 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X	X	X	—	X	—	—
Arizona	X	X	X	X	—	X	X	X	X
Arkansas	X	X	X	X	—	X	X	—	—
California	—	—	—	—	—	—	—	—	X
Colorado	—	—	—	X	—	—	—	—	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida	—	—	—	X	—	—	—	—	X
Illinois	X	—	—	X	—	—	X	—	X
Indiana	—	—	X	X	—	—	—	X	X
Iowa	—	X	—	X	—	—	X	—	X
Kansas	X	X	X	X	X	X	X	—	X
Kentucky	X	X	—	X	X	X	X	X	X
Louisiana	—	—	—	—	—	—	—	—	—
Maine	—	—	—	X	—	—	—	X	X
Massachusetts	—	X	—	X	—	—	—	—	X
Michigan	—	X	—	X	—	—	—	—	X
Minnesota	—	—	X	X	X	X	X	X	—
Mississippi	—	X	—	X	—	—	—	—	X
New Hampshire	—	—	X	X	—	—	—	—	X
New Jersey	—	X	—	X	—	—	—	—	—
New Mexico	X	X	X	X	X	—	X	X	X
New York	—	X	—	—	—	X	—	—	X
North Carolina	—	X	X	X	X	—	—	X	X
Ohio	X	—	—	—	—	—	—	—	X
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	—	—	—	—	—	—	X	X	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	—	—	—	—	—	—	—	X
Utah	—	—	—	—	—	—	X	—	—
Vermont	—	X	—	X	—	—	—	—	X
Washington	X	—	—	X	—	—	X	X	X
West Virginia	X	X	—	—	—	—	X	X	X
Wisconsin	X	X	X	X	—	X	—	X	X
Wyoming	—	X	—	—	—	—	—	—	X
Total	14 (38%)	20 (59%)	13 (38%)	25 (74%)	9 (26%)	10 (29%)	16 (47%)	14 (41%)	28 (82%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

the disclosing provider is responsible for ensuring that only the *minimum necessary* information is disclosed. Four states noted that they would exchange only de-identified data.

Two states reported that most of the information described in these scenarios is being exchanged by fax or telephone and that practices are in place to ensure that these exchanges are secure. These states expressly noted avoidance of e-mail exchange or use of advanced technology to exchange data in these scenarios. Other states have begun to exchange pharmacy data via virtual private network (VPN). They also have some experience with e-prescribing, which introduces complexity because of the need to comply with the special federal regulations governing controlled substances and specially protected data.

Discussions of Domain 2 addressed the BAA as described under Domain 9. States reported that these agreements provided both parties mutual security practice knowledge sufficient to enable the information exchange.

2.7.3 Critical Observations

Critical observations concerning Scenarios 9 and 10 are as follows:

- Exchange of pharmacy data is largely paper-based at present, relying heavily on fax and telephone.
- Lack of trust in security between organizations is a major barrier to interoperable electronic health information exchange.
- Pharmacy data are particularly subject to requests from marketers. Stakeholders frequently use the HIPAA Privacy Rule as a shield to limit release of pharmacy data.
- States have requested clarification of the relationship between the federal Employee Retirement Income Security Act and state requirements.

2.8 Health Care Operations and Marketing (Scenarios 11 and 12)

11. Health Care Operations and Marketing Scenario A

ABC Health Care is an integrated health delivery system composed of 10 critical access hospitals and one large tertiary hospital, DEF Medical Center, which has served as the system's primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports containing patient-identifiable data to the system six-sigma team to analyze patient encounters and trends for the following rehab diagnoses/procedures:

- cerebrovascular accident
- hip fracture
- total joint replacement

Additionally, ABC Health Care is requesting that this same information, along with individual patient demographic information, be provided to the system marketing department. The marketing department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Decision to conduct marketing using patient data with their consumers.
2. Authorization from consumer to allow IHDS to market to themselves.
3. Determine mode of transferring information and type of information, i.e., identifiable or de-identified, to the marketing department.

12. Health Care Operations and Marketing Scenario B

ABC hospital has approximately 3,600 births per year. The hospital marketing department is requesting identifiable data on all deliveries, including mother's demographic information and birth outcome (to ensure that contact is made only with those deliveries resulting in healthy live births).

The marketing department has explained that they will use the patient information for the following purposes:

1. To provide information on the hospital's new pediatric wing/services.
2. To solicit registration for the hospital's parenting classes.
3. To request donations for construction of the proposed neonatal intensive care unit.
4. To sell the data to a local diaper company to use in marketing diaper services directly to parents.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Request of patient consent or permission to use and sell identifiable data for marketing purposes.
2. Decisions to conduct marketing using patient data.
3. Determining mode of transferring information and type of information, i.e., identifiable or de-identified, to the marketing department.

2.8.1 Stakeholders

Scenario 11 engaged stakeholders from hospitals, community clinics, and health centers. The scenario could easily be modified to apply to any provider wishing to market services to a targeted subset of patients. Thus, other relevant stakeholder groups included clinicians, physician groups, federal health facilities, payers, laboratories, pharmacies, long-term care facilities and nursing homes, homecare and hospice, and consumers.

Scenario 12 engaged stakeholders from hospitals, as well as consumers and employers. Also recommended were clinicians, physician groups, federal health facilities, payers, community clinics and health centers, laboratories, pharmacies, long-term care facilities, nursing homes, homecare and hospice, and law enforcement.

Virtually all stakeholder groups were engaged in the review of Scenarios 11 and 12 (Table 2-16). The most frequently engaged stakeholder group was hospitals, engaged by 30

Table 2-16. Stakeholder Groups Engaged in Scenario 11 and 12 Review

Stakeholder Group	Number of States Engaging Stakeholder Group in Review of Scenarios 11 and 12 (N = 34)	Percentage of States Engaging Stakeholder Group in Review of Scenarios 11 and 12 (%)
Hospitals/health systems	30	(88)
Clinicians	12	(35)
Community clinics and health centers	11	(32)
Consumers/consumer advocates	10	(29)
Physicians and physicians groups	9	(26)
Payers	9	(26)
Homecare and hospice	7	(21)
Medical and public health schools/research	7	(21)
Public health agencies or departments	7	(21)
Medicaid/other state government	7	(21)
Federal health facilities	6	(18)
Long-term care facilities and nursing homes	5	(15)
Pharmacies/pharmacy benefit managers	5	(15)
Professional associations and societies	5	(15)
Quality improvement organizations	3	(9)
Employers	3	(9)
Electronic health records experts	3	(9)
Laboratories	2	(6)
Regional health information organizations	2	(6)
Law enforcement and correctional facilities	2	(6)
Legal counsel/attorneys	2	(6)
Health IT consultants	2	(6)
Mental health and behavioral health	1	(3)
Safety net providers	1	(3)
County government	1	(3)
Health information management organizations	1	(3)
Privacy and security experts/compliance officers	1	(3)
Technology organizations/vendors	1	(3)
Other	1	(3)

of the 34 states. Clinicians, community clinics, consumers, physician groups, and payers were a distant second tier of stakeholder groups, each engaged in discussions by 9 to 12 states.

2.8.2 Domains

Wide variation among states emerged regarding domains: 2 states reported that 8 domains of privacy and security were affected, while 17 states reported that only 1 or 2 domains were affected. By far Domain 9—“Information use and disclosure policies” (31 states) was

the most frequently cited, followed distantly by Domain 2—“Authorization and access control” (17 states; Table 2-17).

Eight states reported variation between organizations about how these exchanges were interpreted. Some stakeholders felt that the exchanges were internal operations exchanges and, as such, were permitted by the HIPAA Privacy Rule and state law. Other stakeholders in these same states were surprised by this view and would not exchange data in the circumstances presented by these scenarios. Many stakeholders were certain that using patient-identified information for marketing purposes was not permitted without patient *authorization* and would be unethical even if it were permitted. A few states explicitly reported that they would never sell data for third-party marketing. Two states reported that the exchange of patient data for marketing purposes would be permitted if *minimum necessary* data were exchanged; one state reported that a BAA would be required between the hospital and the marketing firm.

Three states reported that access would require the involvement of their IRB or privacy officer before access to data for marketing would be allowed. One state reported that existing access controls prohibit access to the data for marketing purposes.

2.8.3 Critical Observations

Responses to Scenario 11 were fairly uniform. This scenario described the internal use of patient data for quality improvement and marketing efforts that amount to the hospital’s offering additional services to its existing customers. Most stakeholders felt the quality improvement use could be accomplished with de-identified data and did not present any areas where policy decisions might be needed.

States reduced Scenario 12 to the different information exchanges described. Disclosure to sell patient data to a local diaper service was widely viewed as disallowed either by the individual states or by the HIPAA Privacy Rule. Ten states viewed it as unethical behavior and would not sell such data even if state law allowed it. Three states reported that patient *authorization* would be required before data could be sold. States agreed that consumers would react negatively if their medical data were sold. This use would create consumer mistrust and concern about unauthorized and unknown access to and use of medical data.

States also agreed that the HIPAA Privacy Rule allows hospitals to provide information about pediatric services and parenting classes and that the Rule requires that patients have the opportunity to opt out of fundraising communications.

Table 2-17. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenarios 11 and 12 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	—	X	—	—	—	X	X	X	X
Arizona	—	X	—	X	—	—	X	—	X
Arkansas	—	—	X	X	X	—	X	—	—
California	—	—	—	—	—	X	—	—	X
Colorado	—	—	—	—	—	—	—	—	X
Connecticut	X	X	X	X	X	X	X	—	X
Florida	—	X	—	—	—	—	—	—	X
Illinois	—	—	—	X	—	—	—	—	X
Indiana	—	X	—	—	—	X	—	—	X
Iowa	—	X	—	—	—	—	—	—	X
Kansas	X	X	X	—	—	X	—	X	X
Kentucky	—	—	—	—	—	—	—	—	X
Louisiana	—	X	—	—	—	X	X	—	X
Maine	—	—	—	—	—	—	X	X	X
Massachusetts	—	—	—	—	—	—	—	—	X
Michigan	—	—	—	—	—	—	—	—	X
Minnesota	—	X	—	—	—	X	X	X	—
Mississippi	—	—	—	X	—	—	—	—	X
New Hampshire	—	—	—	—	—	—	—	X	X
New Jersey	—	X	—	X	—	—	—	—	X
New Mexico	—	X	X	—	—	—	X	X	X
New York	X	X	—	X	—	X	X	—	X
North Carolina	X	X	X	X	—	X	—	X	X
Ohio	—	—	—	—	—	—	—	—	X
Oklahoma	X	X	X	X	X	X	X	—	X
Oregon	X	X	—	X	—	—	X	—	—
Puerto Rico	—	—	—	—	—	—	—	X	X
Rhode Island	—	—	—	—	—	—	—	—	X
Utah	—	—	—	—	—	—	—	—	X
Vermont	—	—	—	—	—	—	—	—	X
Washington	—	X	—	—	—	X	X	—	X
West Virginia	—	—	—	—	—	—	—	—	X
Wisconsin	X	X	X	X	—	X	—	X	X
Wyoming	—	—	—	—	—	—	—	—	X
Total	7 (21%)	17 (50%)	7 (21%)	11 (32%)	3 (9%)	12 (35%)	12 (35%)	9 (26%)	31 (91%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

2.9 Bioterrorism Event (Scenario 13)

13. Bioterrorism Event

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases and, therefore, this could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the state declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well as informing the regional media to alert the public concerning symptoms and seeking treatment if feeling affected. The state also notifies the federal government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as it arises to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to specific symptoms to law enforcement, Centers for Disease Control and Prevention, Homeland Security, and health department(s) in a situation where a threat is being investigated.

2.9.1 Stakeholders

Many state teams reported that Scenario 13 was one of the more popular scenarios for discussion. Overall, the state teams were able to include a wide variety of stakeholders in discussions for this scenario (Table 2-18). The average number of stakeholder groups offering input to the scenario discussion was 4. However, 12 states received input from 5 or more stakeholder groups, and 2 states drew from more than 10 stakeholder groups. Given the significant public health component of this scenario, stakeholders from this sector were successfully brought into the discussion by all but a few states. Those states that did not have direct input from the public health sector brought information from state agency and federal agency staff familiar with public health procedures. This scenario, like Scenario 8, had a significant law enforcement component. However, only 10 states reported that they engaged law enforcement stakeholders in discussion for this scenario. As these states noted, increasing discourse with law enforcement is a much-needed step in addressing privacy and security concerns in the context of electronic health information exchange.

Between 15 and 20 states included a hospital physician stakeholder in discussions, and 13 of the 34 included either state or federal agency stakeholder input. Given the media relations component of the scenario and the threat to the public, it is somewhat surprising that only about one third of the states were able to include consumer stakeholders in their discussions.

Table 2-18. Stakeholder Groups Engaged in Scenario 13 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 13 (N = 34)	Percentage of State Teams Engaging Stakeholder Group in Review of Scenario 13 (%)
Public health agencies	27	(79)
Physician groups	16	(47)
Clinicians	16	(47)
Hospital personnel/emergency room staff	15	(44)
State government	13	(38)
Laboratories	11	(32)
Consumers	10	(29)
Law enforcement	10	(29)
Federal health facilities	8	(26)
Emergency services	5	(15)
Homecare and hospice	5	(15)
Payers/insurance	4	(12)
Community clinics and health centers	4	(12)
Pharmacies	3	(9)
Mental health	2	(6)
Emergency services	2	(6)
Long-term care facilities/nursing homes	2	(6)
Medical and public health schools that undertake research	2	(6)
Professional associations	2	(6)
Poison control	1	(3)

2.9.2 Domains

Wide variation emerged in how the state teams viewed this scenario (Table 2-19). Five state teams felt that all 9 domains were relevant to this scenario, while 7 other state teams felt that this scenario involved only 1 to 3 domains. The majority of states' business practices fell within 4 to 7 domains.

Despite this variation among the states, 17 of the 34 state teams said that Domains 2—"Information authorization and access controls," 4—"Information transmission security or exchange protocols," and 8—"State law restrictions" were more closely related to this scenario. Most state teams were in general (but not complete) agreement that required disease reporting superseded all patient confidentiality. States were aware that the HIPAA Privacy Rule provides specific exemptions to accommodate this requirement. Furthermore, many states suggested that, for notification purposes, the good of the community would make the privacy and security of health information secondary to treatment during the event. Several state teams reported widespread misunderstanding about what state law

Table 2-19. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 13 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	—	X	—	—	X	—	—	—
Arizona	—	—	—	X	—	—	X	—	X
Arkansas	—	X	—	X	—	—	X	X	—
California	—	—	—	—	X	X	—	—	X
Colorado	—	X	—	X	—	X	X	—	X
Connecticut	X	—	X	X	X	X	X	X	X
Florida	X	X	—	X	X	X	X	X	X
Illinois	X	X	—	—	X	—	—	—	X
Indiana	—	—	—	X	—	—	—	—	X
Iowa	—	X	—	—	—	—	—	—	—
Kansas	X	X	X	X	X	—	X	X	X
Kentucky	—	—	—	—	—	—	—	—	—
Louisiana	X	X	—	X	—	—	—	X	X
Maine	X	—	—	—	—	—	—	—	X
Massachusetts	—	—	—	—	—	—	—	—	X
Michigan	X	—	—	X	—	—	X	—	X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi	—	—	—	X	—	—	—	—	—
New Hampshire	—	—	—	—	—	—	—	—	X
New Jersey	—	X	—	X	—	—	—	X	—
New Mexico	—	—	—	—	—	—	—	—	—
New York	X	X	X	—	—	—	X	X	X
North Carolina	—	X	—	—	—	—	—	X	—
Ohio	—	—	—	—	—	—	—	X	—
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	—	—	—	—	—	—	—	—	—
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	—	—	—	—	—	—	—	X
Utah	—	—	—	—	—	—	—	—	—
Vermont	—	X	—	X	—	—	X	—	X
Washington	—	X	—	X	—	—	—	X	X
West Virginia	—	X	—	—	—	—	—	X	X
Wisconsin	X	X	X	X	X	X	X	X	X
Wyoming	—	—	—	—	—	—	—	X	X
Total	13	17	8	17	9	9	13	16	23

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

requires for verification or authorization of the data and for tracking automated release of data in such a scenario. At least 6 state teams noted that many providers and clinicians in their states do not understand the state law and regulatory reporting requirements during suspected bioterrorism or during a potential epidemic and that this misunderstanding results in broad variation in practice. This scenario often presented very clear differences in practices, depending on whether the organizations were using a paper-based or an electronic system. Similarly, states noted that the fact-sensitive nature of the outbreak would determine the amount of patient identifiable information to be given to various parties responding to the outbreak.

2.9.3 Critical Observations

A common theme in the state team reports is that state law and regulations are not yet sufficient to ensure private and secure electronic health information exchange with mandating stakeholders, such as law enforcement. Public health officials must participate in local and state planning for homeland security measures. Providers and public health agencies need to work with law enforcement and other organizations involved with bioterrorism to establish new standards and definitions about what health information is appropriate to disclose, when it is appropriate to disclose, and for what purpose. Some states also suggested that the Department of Health and Human Services, Office for Civil Rights', emergency preparedness decision tool could help remove many barriers nationally in this area, including privacy and security barriers. This web-based interactive decision tool, they note, was designed to help emergency preparedness and recovery planners better prepare for man-made and natural disasters.

Teams of states with experience in actual events (or trainings for them) noted a particularly critical observation: the need for hospitals to implement procedures to inform family members of missing relatives brought to the hospital. Although it is not clear how these conflicting interests can best be reconciled, this issue must be addressed because the ability to find relatives admitted to hospitals during an emergency is a vital area of public concern.

2.10 Employee Health Information (Scenario 14)

14. Stakeholder Organizations and Exchanges

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has exacerbated and is not work-related. The employee's condition necessitates a 4-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than 2 days' leave. The hospital emergency department has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information via e-mail to the human resources department of the patient's employer.

Potential areas of discussion of business practices based on this scenario:

1. Determining employee agreement to release information.
2. Determining what are the minimum necessary elements which can be legally transmitted.
3. Ensuring the data are secure as they are transmitted.

2.10.1 Stakeholders

The states/territory identified the appropriate stakeholders to review Scenario 14 and to discuss how their current business practices address the scenario in relation to the 9 domains of interoperability. The range of stakeholders was generally broad as were the various roles of the discussants (Table 2-20); see Appendix C for a list of stakeholders. The current business practices provided the opportunity for the states/territory to examine the system and to explore ways to improve or enhance it.

Hospital stakeholders who have not transitioned to an electronic system and continue to use hard copy forms reported that their policy was to release only a form that identified the days the patient was to miss work, return to work, or both. Stakeholders agreed that no personal health information would be released in paper or electronic form without a signed release of information from the patient. All stakeholders interviewed stated that a patient has to initiate the request for return-to-work documentation; employers are not able to directly request the information.

Hospitals and physicians are careful to release only limited information to satisfy employers' requests and will not reveal diagnosis-related information. Employers are wary of the liability associated with knowledge of their employees' health information. Consequently, many employers do not request diagnosis-related personal health information. Hospitals and physicians adhere to the standard that a patient *authorization* to release information to an employer is limited to the current request and does not extend to future requests.

State teams also discussed the use of e-mail and other electronic forms of transmission. Most stakeholders agreed that e-mail is not secure unless encryption is used. Other stakeholders agreed that caution needs be used when one is cutting and pasting information from an EHR: no patient information can be legally included unless a signed permission form is obtained from the patient. The stakeholders were diligent in distinguishing between an inhibitor to electronic health information exchange and measures of security.

Discussants reported that patient information is not usually transmitted to an employer via e-mail. Most often, a letter summarizing treatment or doctor's note is presented in person by the employee or faxed with an appropriate cover sheet by the treating facility. When patient information is transmitted electronically, the HIPAA Security Rule will govern that transmission if made by a covered entity. Such standards require covered entities to implement procedures to verify the identity of a person or entity seeking access to electronic

Table 2-20. Stakeholder Groups Engaged in Scenario 14 Reviews

Stakeholder Group	Number of States Engaging Stakeholder in Review of Scenario 14 (N = 34)	Percentage of States Engaging Stakeholder in Review of Scenario 14 (%)
Hospitals	26	(76)
Consumers/consumer advocates	14	(41)
Employers	10	(29)
Clinicians	9	(26)
Physician groups	7	(21)
Payers	5	(15)
Community clinics	5	(15)
Federal health facilities	5	(15)
Public health agencies	5	(15)
State agencies	4	(12)
Legal/compliance community	4	(12)
Other	4	(12)
Homecare and hospice	2	(6)
Professional associations	2	(6)
Researchers	2	(6)
Law enforcement/corrections	2	(6)
IT	2	(6)
Long-term care facilities	1	(3)
Mental health agencies	1	(3)
Laboratories	1	(3)
Pharmacies/PBM	1	(3)

protected health information (PHI), and to implement security measures to guard against unauthorized access to electronic PHI. Furthermore, covered entities are required to implement measures to protect electronic PHI from unauthorized access during transmission.

Health care institutions reported that they require employees to undergo training on confidentiality policies, and employees are required to sign an agreement that patient information will be accessed and viewed only for treatment, payment, or operational reasons that are required to carry out job duties.

Practices and policies associated with administrative safeguards are required to protect electronic PHI and to manage the conduct of a HIPAA covered entity’s workforce. Covered entities must limit physical access while permitting properly-authorized access. The specific

standards of the HIPAA Security Rule cover facility access controls, workstation use, workstation security and device and media controls.

2.10.2 Domains

Although all of the domains were identified as relevant, Domain 1—“User and entity authentication;” Domain 2—“Information authorization and access controls;” Domain 4—“Information transmission security or exchange protocols;” and Domain 9—“Information use and disclosure policy” were cited most often by the stakeholders (Table 2-21).

2.10.3 Critical Observations

Some stakeholders considered Scenario 14 to be among the least problematic of the scenarios they analyzed. They felt that, regardless of size, most health care organizations are keenly aware of the return-to-work rules in their state because they provide the documentation for the return-to-work forms. Larger organizations usually employ an occupational health manager who will instruct the individual’s manager about work restrictions and their duration.

Stakeholders reported that employers do not expect to get information from the emergency room electronically. Generally, an employer’s terms of employment or organizational policy requires that specific information about the employee’s health problem be shared in two instances: (1) if the length of time the employee would be absent from work triggers a claim for temporary disability or workers’ compensation issue, or (2) if the employee is performing direct care and needs to be certified as free of any communicable disease.

Transmission of the prescription form or letter from a doctor is usually by hand, mail, or fax.

Employers who participated in the discussions reported that they stored medical information, separate from their other employee records, in a locked filing cabinet in a secure location accessible to specifically assigned and authorized staff only.

One state identified highly variable business practice with respect to the disclosure of individualized health information by health care providers to employers. The implementation of an interoperable EHR system will make this issue an even tougher one for all concerned because of the relative ease of retrieving larger amounts of health information, and the ability to quickly and cheaply transmit such information.

The stakeholders in this state acknowledge the need to reach a greater consensus on the appropriate checks and balances to be used when communicating such information with employers, without sacrificing any more patient privacy than is necessary.

The main business practice raised by this scenario dealt with procedures for communicating with a patient’s employer about the patient’s ability to return to work. Organizations interpreted privacy responsibility issues differently when communicating with the patient’s

Table 2-21. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 14 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X	—	—	—	—	—	—
Arizona	—	X	X	X	—	—	—	—	—
Arkansas	X	—	X	—	—	X	X	—	X
California	—	X	—	X	—	—	—	—	X
Colorado	—	—	—	X	—	—	X	—	X
Connecticut	X	X	X	—	—	—	—	—	—
Florida	—	—	—	—	—	—	—	—	X
Illinois	X	X	X	X	X	—	—	—	X
Indiana	—	—	—	X	X	—	—	—	—
Iowa	—	—	—	—	—	—	—	—	—
Kansas	—	—	X	—	—	—	—	—	X
Kentucky	—	—	—	X	—	—	—	—	X
Louisiana	X	—	—	X	X	X	—	—	X
Maine	—	—	—	X	—	—	—	—	X
Massachusetts	—	—	—	X	—	—	—	X	X
Michigan	X	—	—	X	—	—	X	—	X
Minnesota	—	—	—	—	—	—	—	—	—
Mississippi	—	—	—	X	—	—	—	—	X
New Hampshire	—	—	—	—	—	—	—	—	—
New Jersey	—	X	—	X	—	—	X	—	—
New Mexico	X	X	—	X	—	—	—	—	X
New York	—	X	—	X	—	—	—	—	X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio	—	X	X	—	—	—	—	—	—
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	—	X	X	X	—	—	X	—	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	X	—	—	—	—	—	—	X
Utah	—	X	—	—	—	—	—	—	X
Vermont	X	—	—	X	—	—	—	—	X
Washington	—	X	—	—	—	—	—	—	X
West Virginia	X	X	X	X	—	X	X	X	X
Wisconsin	X	X	—	X	—	X	—	X	X
Wyoming	X	—	—	—	—	—	—	—	X
Total	14	18	12	21	6	7	9	6	25

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

employer. Some stakeholders removed themselves from the situation by only releasing information directly to the patient. The patient was then responsible for delivering the return-to-work form to the employer. Others said they would provide a note directly to the employer at the patient's request. All stakeholders agreed that no treatment or diagnosis information was required in return-to-work documentation.

Hospital stakeholders with an EHR stated that they would not cut and paste any information from the EHR; however, some EHRs have a software-generated letter on the hospital's letterhead containing limited information that includes treatment date(s), return-to-work date, and any physical limitations. Stakeholders without an EHR stated that they use standard forms with a hospital logo that contain limited information, treatment dates(s), return-to-work dates and any physical limitations.

Consumers who participated in the groups were concerned about employers' having access to their health information. Their specific concern was that the information would be used against them in hiring decisions, reduction in force, and promotion decisions. Also, employees do not want employers to know about mental health conditions, depression, substance abuse problems, or even chronic illnesses or medical problems requiring expensive drugs or frequent service utilization.

2.11 Public Health (Scenarios 15–17)

15. Public Health Scenario A—Active Carrier, Communicable Disease Notification

Without informing his physician, a patient with active tuberculosis (TB), still under treatment, has decided to move to a desert community that focuses on spiritual healing. The TB is classified MDR (multidrug resistant). The patient purchases a bus ticket—the bus ride will take a total of 9 hours with 2 rest stops across several states. State A is made aware of the patient's intent 2 hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to a specific communicable disease to law enforcement, nonhealthcare entities, and health department in a situation where authorities are responding to a threat.
2. Ensuring the data are secured as they are transmitted.

16. Public Health Scenario B—Newborn Screening

A newborn's screening test comes up positive for a state-mandated screening test, and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response (IVR) system. The state lab also enters the information in its registry and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to specific symptoms of a disease to a health department in a situation where a targeted disease is being investigated.

17. Public Health Scenario C—Homeless Shelters

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. This person does have a primary care provider, and he is sent there for medical care. The primary care provider refers patient to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement and back to the shelter to verify that the person is in treatment. Someone claiming to be a relation of the homeless man requests information from the homeless shelter on all the health services the man has received. The staff at the homeless shelter are working to connect the homeless man with his relative.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. The extent and amount of information shared between the various facilities would be limited by the minimum necessary guidelines.

2.11.1 Stakeholders

Although a wide variety of stakeholders contributed to these scenarios across the 34 participating states, most input for Scenarios 15 and 16 came from public health agencies, with 33 out of the 34 (97%) state teams mentioning input from a public health agency representative specifically when discussing these scenarios (Table 2-22). In many cases, additional input was gathered from laboratories and clinicians. For most states, Scenario 17 generated more widespread input than Scenarios 15 and 16; although public health and state government agencies were still strongly represented, hospitals, state government, community clinics, and physician groups were also active, strong contributors. Notable contributions also came from homeless shelters in five states. Four states combined Scenarios 15–17 with Scenario 18, while one state combined Scenarios 15–17 with Scenario 13. It was impossible to distinguish which stakeholders responded to each of the scenarios; therefore, all listed stakeholders were included in Scenarios 15–17 as well as with either Scenario 13 or 18, depending on the state.

2.11.2 Domains

As with stakeholder representation, 4 of the state teams combined Scenarios 15–17 with Scenario 18, and one state combined Scenarios 15–17 with Scenario 13. Again, these states did not identify which domains were pertinent to which scenarios, so all cited domains were included in both scenario groupings. The business practices collected for this scenario group focused on information exchange in public health, state government, and health oversight situations. Some state teams discussed how these scenarios touched on all 9 domains; however, some domains were clearly cited more frequently than others (Table 2-23).

Domain 9—“Information use and disclosure policy” was referenced most often, with 29 out of 34 state teams explicitly including discussions about business practices related to this domain. Although this domain is clearly important in discussions of public health issues, the

Table 2-22. Stakeholder Groups Engaged in Scenario 15–17 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenarios 15–17 (N = 34)	Percentage of State Teams Engaging Stakeholder Group in Review of Scenarios 15–17 (%)
Public health agencies	33	(97)
State government	22	(65)
Hospital personnel/emergency room staff	22	(65)
Community clinics and health centers	18	(53)
Clinicians	15	(44)
Physician groups	12	(35)
Laboratories	12	(35)
Consumers/consumer organizations	12	(35)
Correctional facilities/law enforcement	11	(32)
Medical and public health schools that undertake research	10	(29)
Federal health facilities	8	(24)
Payers	8	(24)
Professional associations	8	(24)
Mental/behavioral health	7	(21)
Homecare and hospice	6	(18)
Long-term care facilities/nursing homes	6	(18)
Pharmacies	5	(15)
Homeless shelters	5	(15)
Privacy officers	2	(6)
Health care attorneys	2	(6)
Health information personnel	2	(6)
RHIOs	2	(6)
Information security	2	(6)
Quality improvement organizations	2	(6)
Data vendor	1	(3)
County government	1	(3)

actual business practices about use and disclosure in these scenarios are relatively consistent when compared to other scenario groupings.

This consistency is especially true in Scenario 15. All state teams agreed that the provider’s disclosure of the patient’s condition to a public health authority is permitted pursuant to the HIPAA Privacy Rule in the case of TB. Then, in most states, the primary contact occurs between public health entities using interjurisdictional notification from one state to another. Once communication has been established, there is no noted resistance to the idea of exchanging the patient’s personal health information. However, one stated noted that

Table 2-23. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenarios 15–17 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	—	—	—	X	X	—	—
Arizona	X	X	—	X	X	—	X	X	X
Arkansas	—	—	X	X	—	—	—	X	X
California	—	—	—	—	—	X	X	X	X
Colorado	—	—	—	X	—	—	—	X	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida	—	X	—	—	—	—	—	X	X
Illinois	X	X	—	X	—	X	X	X	X
Indiana ^(a)	—	X	X	X	—	—	—	X	X
Iowa ^(a)	—	X	X	X	X	—	X	X	X
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	X	—	—	X	—	—	—	X	X
Louisiana	X	X	X	X	—	—	X	X	X
Maine ^(a)	—	—	—	—	—	—	—	X	X
Massachusetts	X	—	—	—	—	—	—	X	X
Michigan	X	X	X	X	X	—	X	X	X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi	—	—	—	X	—	—	X	—	X
New Hampshire	—	X	—	—	—	—	—	—	X
New Jersey ^(a)	—	X	X	X	—	—	—	X	X
New Mexico	X	X	—	X	—	X	—	X	—
New York ^(b)	X	X	X	—	—	—	X	—	X
North Carolina	X	X	X	X	X	X	—	X	X
Ohio	—	X	—	X	—	—	—	X	—
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	—	X	—	—	—	—	X	X	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	—	—	—	—	—	—	X	X
Utah	—	—	—	—	—	—	—	X	—
Vermont	X	X	—	X	X	—	—	—	X
Washington	X	—	X	X	—	—	X	X	X
West Virginia	—	X	X	X	—	—	—	X	X
Wisconsin	X	X	X	X	X	X	X	X	X
Wyoming	—	—	—	—	—	—	—	—	X
Total	18 53%	23 68%	16 47%	23 68%	11 32%	12 35%	17 50%	27 79%	29 85%

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain.

^a State team combined Public Health Scenarios 15–17 with State Government Oversight Scenario 18.

^b State team combined Public Health Scenarios 15–17 with Public Health-Bioterrorism Event Scenario 13.

public health entities have no agreement to communicate anything other than demographic data.

Some variation emerged among state teams about how much information was to be disclosed to either law enforcement or the bus company. Most state teams said that their public health agencies would share communicable-disease information with law enforcement and other entities (e.g., transportation companies), but the level of information shared differed. For example, some states would allow the public health departments to notify the transportation company of the incident but would not disclose the identity of the patient, whereas other states would identify the patient to the transportation company but would not disclose the diagnosis. In one state, however, no rules exist to govern the disclosure of information to either law enforcement or other entities; therefore, public health agencies generally *do not* disclose information. This nondisclosure often creates a conflict with law enforcement personnel, who feel it impedes their ability to do their jobs.

Few state teams mentioned the idea of releasing health information about the infected individual to passengers because doing so was not necessary to contain the threat to public health. However, most state teams discussed disclosure of exposure in general to the passengers. Some states notify passengers directly of their exposure, allowing the local public health office at the site of interception to manage the initial disclosure. Most states also relied on contact with the exposed individual's local public health department to follow up with the bulk of responsibilities, including release of follow-up information concerning their exposure and testing.

Minor variation among states also occurred in Scenario 16. All state teams recognized the right to collect and store data in a disease registry for public health reporting purposes; however, variation exists in *how* and *to whom* the data are disclosed. Many states agreed that they would not disclose the information directly to a specialty care center, but instead, would choose to disclose this information to the physician. In fact, a few state teams mentioned that the physician was the only source to whom they would release test results. In almost all states, the providing physician's job is to inform the parents about the services available for their child. In regard to disclosure to the parent, most states leave this disclosure up to the providing physician. However, in other states the public health department makes the disclosure directly to the parent by letter, which informs them about the specialty care service and centers that are available to them. Tracking additional treatment information for individual patients over time was not discussed.

The variation in use and disclosure for Scenario 17 became broader. Most shelters providing input on the scenario agreed that disclosure of any health record information, even to a relative, would require written consent of the patient. This is especially true of specially protected information such as substance abuse treatment. However, a good number of state teams debated the shelter's covered entity status under the HIPAA Rules. Consequently,

very few treatment programs reported that they would disclose information to the shelter. Although many state teams reported that homeless shelters would not, without written consent, even confirm or deny the presence of the patient to a relative, the fear of secondary disclosure in this exchange was extremely high.

The transmission of patient information for treatment purposes between the primary care provider and drug treatment clinic requires written consent of the patient in most states, even though consent or *authorization* is not required for such purposes by the HIPAA Privacy Rule. Further, 32 states agree that the release of patient information for *payment* purposes is permissible without written consent under the HIPAA Privacy Rule. Many stakeholders within the state referenced *minimum necessary* guidelines, although specifics concerning these guidelines were not clearly outlined in this section of the state reports, other than to say there were a multitude of interpretations across entities within the state. Three state teams cited specific state laws and 42 C.F.R. pt. 2 as requiring specific signed agreements before the drug clinic could disclose the information to the county for payment. Specifically, the 3 state teams reported that they would need either a BAA/qualified services organization agreement, a signed disclosure agreement, or a signed acknowledgement of confidentiality and disclosure agreement from the patient to exchange data for purposes of payment, even from a government program.

All 3 scenarios within public health touched on business practices that mapped to Domain 8—“State law restrictions,” and 27 of the state teams discussed this domain specifically. Many of the disclosure practices already discussed are governed by state law. In most cases, these state laws exist in order to reinforce or provide additional requirements around practices that are permissible, but not mandated, under the Privacy Rule.

In discussing Scenario 15, most state teams specifically referenced the existence of laws mandating the reporting of TB, but laws governing the release of that information vary (see discussion of Domain 9) and often are misunderstood by stakeholders outside the public health entities.

A wider variety of laws govern the practices in Scenario 16. In most states, some type of newborn screening is mandatory. In states where the screening is not mandated by law, information is still routinely collected after consent is given as part of consent to treatment related to birth. Only one state reported an opt-out provision for the actual screening itself. This opt-out seemed to be tied to the state statute requiring additional provisions for the collection of genetic information.

More variable state law restrictions appear in the release of the registry information (see previous Domain 9 discussion). Three states have an opt-out provision for their registry, which is usually presented as an option by the providing physician.

State teams were almost uniform in their discussion of the state law restrictions for Scenario 17, indicating that state laws impose greater restrictions on information exchange, even for treatment purposes, in substance abuse and mental health cases than in other cases. Although exchange of personal health information is often allowed for purposes of treatment or payment without written consent by the patient, written consent is almost always required for exchange of substance abuse or mental health information. Written consent seems to be the standard practice, regardless of the state law. Even in instances when exchange of information is permitted for treatment or billing, no team reported that its state would release this information to relatives without written consent of the patient.

Domain 4—"Information transmission security or exchange protocols"—was cited by 23 of the 34 state teams. For Scenario 15, transmission by telephone was the most common method because it was thought to be the most expedient and reliable form of data exchange in an emergency. Although some states have automated alert systems, these systems rarely cross state lines. The HIPAA Security Rule prohibits transmission of public health information by covered entities by e-mail without encryption or similar protections. Currently, states have had little or no discussion, even in geographic regions, about the security of their electronic systems, although this discussion might lead to eventual interstate data exchange between public health entities.

For Scenario 16, many state teams indicated that their state did not have an IVR system comparable to that presented in the scenario. Although the precise method of transmitting data varied among states, the majority of states collect information from a single state laboratory. In a minority of states, this process is not centralized and, therefore, results are sent from multiple laboratories. In states where multiple entities provide information for the registry, each individual health care provider has an agreement by which the registry uses and discloses information only as allowed by state statute. In all, the transmission between the laboratory and the registry in this scenario is likely to be electronic, especially if a central state laboratory is used. When electronic systems are not used, laboratories typically transmit information to the registry by telephone or fax. States with more advanced EHR systems transmit laboratory data to the state public health agency by secure VPN. These electronic systems usually have a disclosure log to track all disclosures.

At least one state team also reported returning the lab results electronically to participating physicians by VPN, although this level of advancement is rare. Notification is often centralized from the registry, and physicians are usually notified only in the event of an abnormal or positive result. In most states, this communication is done by phone and, in some cases, by fax.

Scenario 17 involved a greater number of data exchanges than the others. However, states reached a broad consensus that, because of very little electronic interoperability and because of the specially protected records being exchanged, most of these exchanges would

occur by fax or mail if they were allowed to occur at all. Most providers did not report using e-mail, because of the continuing lack of trust in it as a secure data transfer mode, especially when entities are discussing the transfer of mental health or substance abuse records.

Within Domain 2—“Information authorization and access controls”—23 state teams mentioned business practices. Most state teams agreed that exchange of information in an emergent situation or in an imminent public health emergency does not require patient *authorization*. Exceptions do exist in the case of substance abuse and mental health records. The range of public health scenarios unearthed the differences in procedures when there is no public health emergency. Because of lack of adequate information-sharing protocols, in nonemergency situations, exchange between state public health departments and those involving multiple entities are far more difficult than in emergencies. Unless the patient has clearly given *authorization* for the exchange to occur, this lack of information more often than not slows or prevents the exchange of data.

Analysis of Scenario 16 specifically shows that most states have a centralized, secure transfer of information between the state lab contracted to perform newborn screenings and the public health registry. Most public health registries are not open for access to individual physicians; therefore, access is limited to only a small number of public health employees. Although few states explained these systems in detail, the few that did outlined the use of passwords, various levels of access, audits of user activity, and high-level encryption. In one state, registry input can be done via the Internet, using a downloadable program installed at the physician’s office. The notification of individual patient data among the laboratories and providers, registry and providers, and laboratories/providers and parents is quite variable, as mentioned in the discussions of Domains 8 and 9.

For Scenario 17, the data are not kept in a central registry nor is reporting mandated to a central authority; therefore, a wider variety of authorization and access controls was reported for this scenario. For the majority of state teams reporting, these records would be largely paper based; therefore, the inconsistency of authorization and access controls would result in greater restrictions to the exchange of information—restrictions attributable to the specially protected records being requested. A few states that have electronic billing systems outline requirements such as electronic enrollment into the system and use of user IDs and passwords for submitting electronic patient information. Access roles are also assigned (such as “read only” or “add/modify”) according to job requirements. However, those state teams that discussed electronic systems of this type also mentioned that mental health and substance abuse data were kept separate from a patient’s regular health data.

2.11.3 Critical Observations

A variety of critical observations were noted by the state teams for the public health scenarios. This section discusses those concerns shared by many states, as well as those

that were raised by only 1 or 2 states but seemed particularly important or conveyed strong insight.

Many states mentioned that the use of TB in Scenario 15 made the situation fairly uncomplicated. Patients with active cases of TB are required to comply with treatment, and have restrictions on travel while in the infectious phase. States have clear guidelines and processes in place for notifying all involved parties regarding communicable disease transmission or outbreak. Some states mentioned that disease reporting is provided for in all patient confidentiality laws, including the HIPAA Privacy Rule.

For many other types of communicable diseases, variation in mandatory reporting exists and would create more difficulty for interstate cooperation. One state indicated that a national law is needed that standardizes the process for handling people with communicable diseases who intentionally put the public at risk when they cross state lines. Additionally, an agreement on diseases requiring cross-border sharing would be helpful, as would standardizing the means by which health information is transmitted from one jurisdiction to another. Currently, the response to a communicable disease would vary depending on the magnitude of the risk to public health, including whether the infected patient planned to travel by airplane and the type of disease.

Many state teams mentioned that, although processes for dealing with Scenario 15 in particular are fairly straightforward, the ability to verify facts and transmit to or coordinate with other states would be greatly enhanced by the availability of an interoperable, electronic clinical information system or registry. One state team also noted the value of knowing whom to notify in other states, including both the health authorities and the law enforcement authorities, and how to notify them outside business hours. This team indicated that such a system could provide this information. On the other hand, at least one state team mentioned that its stakeholders felt that personal relationships are often a key element in transmitting data in a public health emergency, and an electronic system might remove the important human element.

Although the status of the homeless shelter was debated in a number of state discussions, only one state reported that its stakeholders agreed that county health departments are generally not covered entities under the HIPAA Rules. Stakeholders in this state proposed that the HIPAA Privacy Rule be changed through whatever mechanism appropriate to include entities that function like their county health departments as covered entities. Stakeholders in this state reported that there was a lack of transparency surrounding health information disclosures related to public health, one reason being that public health entities are not required to provide an accounting of disclosures. Once involved in a public health situation mandating certain reporting, patient health information is shared as necessary, but stakeholders raised examples in which patients were surprised to learn of instances in which their health information had been shared.

Several states noted that public and state officials expressed concern about the lack of integration in their systems. They felt that public health remained compromised because of the inability of systems to easily track and monitor threats to public health. This observation also led to the general agreement that significant technological barriers related to adopting more integrated electronic systems exist among physician groups or clinicians, hospitals, county health departments, and the like.

However, a more advanced, centralized system does not remedy all technological issues. According to some providers, specific consents for specially protected information create significant difficulties from a technical point of view, because consent is required at every instance of disclosure. Initial technical effort to address the filtering of specially protected information within EHRs, such as genetic information obtained in a newborn screening registry, requires “filtering” logic to check against all available record information that may be transferred. From a consumer advocate point of view, specially protected health information consent requirements provide a high level of privacy protection for sensitive health information. For solutions to this particular issue, a more granular approach to the documentation of consent in different kinds of circumstances might be appropriate for consideration.

State teams also reported challenges that occur with public health HIEs when they require interstate communications. For example, a provider in State A examines a patient from State B; the provider must then report to one or both states. Conversely, a provider from the same State B sees a patient from State A and has to exchange public health data between agencies across states. The challenges arise because of the differences in state law governing reporting, differences in privacy and protection of health information, and disparate business practices.

One state team noted that the business practices related to reporting requirements and gathered from actual public health employees differed greatly from the practices assumed by nonpublic health stakeholders, and this difference illustrated a gap in understanding. In general, some state teams found that stakeholders believe a lack of transparency exists about health information disclosures related to public health. Some aspects of public health activities are not covered by the HIPAA Rules and do not require an accounting of disclosures. Once involved in a public health situation mandating certain reporting, health information is shared where necessary, and stakeholders raised examples in which patients were surprised to learn with whom their health information had been shared.

2.12 State Government Oversight (Scenario 18)

18. Health Oversight: Legal Compliance/Government Accountability

The governor's office has expressed concern about compliance with immunization and lead screening requirements among low-income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient-level health care data on an ongoing basis to determine if the children are getting the health care they need. This is not part of a legislative mandate. The governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is not an existing contract with the state university for services of this nature.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. What is the practice of the organization to provide appropriate information for health care oversight activities? These may include:
 - Determining minimum amount necessary.
 - How to release (electronically or paper—with existing claims data).

2.12.1 Stakeholders

For input on Scenario 18, 26 of the state teams gathered data from public health entities, 21 from state government officials, and 20 from schools that conduct research (Table 2-24). Other common stakeholder groups included hospitals (13), community clinics (10), and clinicians (9). Four of the states combined Scenarios 15–17 with Scenario 18. Because these states did not specify the stakeholders participated in particular scenarios, every stakeholder listed was included in both Scenarios 15–17 and Scenario 18. Additionally, one state reported no stakeholder participation for Scenario 18.

2.12.2 Domains

As with the stakeholder representation, 4 of the 34 state teams combined their analysis of Scenario 18 with the analysis of Scenarios 15 through 17 (public health; Table 2-25). The breakout of major domains identified by the state teams indicates that not only do the major stakeholders overlap between Scenarios 15–17 and Scenario 18, but the major privacy and security domain issues overlap as well. Additionally, two states did not list any domains for this scenario. One state had no stakeholder participation and, therefore, did not respond, while the participating stakeholders in the other state indicated that this particular scenario did not apply to their state.

Domain 9—"Information use and disclosure policies"—was cited by 28 of the 32 state teams. Almost all state teams indicated that the use of patient-level information outlined in this scenario is typically forbidden without signed patient consent and prior approval by an IRB. The general consensus among state teams was that collected data could not be

Table 2-24. Stakeholder Groups Engaged in Scenario 18 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 18 ^(a) (N = 33)	Percentage of State Teams Engaging Stakeholder Group in Review of Scenario 18 ^(a) (%)
Public health agencies	26	(79)
State government	21	(64)
Medical and public health schools that undertake research	20	(61)
Hospitals	13	(39)
Community clinics	10	(30)
Clinicians	9	(27)
Payers	7	(21)
Consumers	6	(18)
Professional associations	6	(18)
Physicians groups	5	(15)
Federal health facilities	5	(15)
Laboratories	4	(12)
Long-term care facilities/nursing homes	4	(12)
Quality improvement organizations	3	(9)
Privacy officers	3	(9)
Correctional facilities/law enforcement	3	(9)
Homecare and hospice	3	(9)
Mental/behavioral health	3	(9)
Health IT/information	3	(9)
Health care attorneys	2	(6)
RHIOs	2	(6)
Data vendor	1	(3)
County government	1	(3)

^a One state did not have stakeholder representation for this scenario.

transmitted from a state health agency to a university without legislative authorization or a data-use-and-sharing agreement. Even though a data-use-and-sharing agreement could allow disclosure of the data in many states, the lack of standard data-sharing agreements and lack of a common language among stakeholders from different states make sharing data across state lines difficult, given this scenario. The state teams found this to be infeasible because of the sensitivities and the regulations that would have to be met for the state health agency to share identified data with the university. Many state teams discussed the slightly more realistic goal of just combining data from multiple entities. Although some states have a centralized database to collect this information, many do not. To construct a complete picture, data from different agencies would have to be combined, which would pose difficulties because the information was collected with different intentions and

Table 2-25. Nine Privacy and Security Domains Affected by Business Practices Associated with Scenario 18 (N = 32)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	—	—	—	—	—	—	—	—	—
Arizona	—	—	—	—	—	—	X	X	X
Arkansas	—	X	—	X	X	—	X	X	X
California	—	—	—	—	—	—	—	—	X
Colorado	—	—	—	X	—	—	—	—	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida	—	X	—	—	—	—	—	X	X
Illinois	—	X	—	X	—	—	—	—	X
Indiana ^(a)	—	X	X	X	—	—	—	X	X
Iowa ^(a)	—	X	X	X	X	—	X	X	X
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	—	X	—	—	—	—	X	—	X
Louisiana	X	X	—	X	—	—	X	X	X
Maine ^(a)	—	—	—	—	—	—	—	X	X
Massachusetts	—	—	—	—	—	—	—	—	X
Michigan	X	X	X	X	—	X	X	X	X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi	—	—	—	X	—	—	—	—	X
New Hampshire	—	X	—	—	—	—	—	—	X
New Jersey ^(a)	—	X	X	X	—	—	—	X	X
New Mexico	—	—	—	X	—	—	—	X	—
New York	—	X	—	—	—	—	—	X	—
North Carolina	—	—	—	—	—	—	—	—	—
Ohio	—	X	—	X	—	—	—	X	—
Oklahoma	X	X	X	X	—	X	X	X	X
Oregon	—	—	—	—	—	—	—	—	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island	—	—	—	—	—	—	—	—	X
Utah	—	—	—	—	—	—	—	—	X
Vermont	X	X	—	X	X	X	X	—	X
Washington	—	X	—	—	—	—	X	—	X
West Virginia	—	—	—	X	—	—	—	X	X
Wisconsin	X	X	X	X	X	X	X	X	X
Wyoming	—	—	—	—	—	—	—	—	X
Total	9	20	10	20	8	8	14	18	28
	28%	63%	31%	63%	25%	25%	44%	56%	%

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An em dash (—) indicates that no business practice was identified in association with that domain. Two state teams did not list domains for this scenario.

^a State team combined Public Health Scenarios 15–17 with State Government Oversight Scenario 18.

permissions. To provide patient-identifiable data for secondary public health use, health organizations must have either patient *authorization* or a legal mandate.

Domain 2—“Information authorization and access controls”—was cited by 20 of the 32 state teams. Most state teams that entertained the idea of the exchange (if all other considerations mentioned in Domains 8 and 9 were met) stated that authorization would have to be given by all individuals included in the database because the data would supposedly be identifiable when transmitted to the university. State teams discussed some of the issues in Domain 2 that were required for their own state immunization databases (without discussing the issue specifically of supplying these data to other entities or across state lines). In all these systems, users were required to sign confidentiality agreements before gaining access to the information.

Domain 4—“Information transmission security or exchange protocols”—was listed by 20 of the 32 state teams. A few states that have advanced electronic immunization and lead-screening systems provided guidelines for secure transmission. Transmission of identifiable information from a public health laboratory happens via secure FTP or secure VPN connection, using assigned log-in names and passwords. In one state, the electronic system employs complete role-based access to secure the information. States that theorized the sharing of information between the state agency and the university assumed that this transaction would almost always be electronic. The information would be exchanged via a secure site utilizing public or private encryption keys assigned to users.

Domain 8—“State law restrictions”—was cited by 18 of the 32 state teams. In states with complex legal structures, an enormous amount of legal analysis—taking into account immunization laws, general information privacy laws, and federal and state laws governing the disclosure of information from state agency programs—would have to be undertaken to determine whether this data collection was even permissible. In a few states with advanced electronic systems, the reporting of immunization data is mandated, but most states have optional reporting. Even states that had advanced systems agreed with most other states, indicating that the action of actually combining data with that from other states would require a legislative mandate.

2.12.3 Critical Observations

One suggested reason for the strong resistance to sharing data electronically is that the HIPAA Security Rule requires that a covered entity implement procedures to prevent unauthorized access to PHI that is being transmitted (see 45 C.F.R. § 164.312(e)). However, the Rule does not offer specific guidance about how to achieve this protection against interception of transmitted information.

Although the HIPAA Privacy Rule permits a covered entity to disclose PHI for purposes of data aggregation with the PHI of another covered entity under a BAA (45 C.F.R.

§ 164.504(e)), in this scenario states are asked to imagine a data aggregation by public health and other government agencies that in many cases are not covered entities. These agencies are often required by state statute to maintain confidential records, and this fact is seen as potentially problematic for interoperable health information exchange.

Several states also mentioned the Family Education Rights and Privacy Act (FERPA). Even if appropriately strong business agreements could be put in place, FERPA controls all school records, and it has its own privacy and security concerns that are not entirely consistent with the HIPAA Rules. Therefore, parents' authorization or consent will likely be required for the release of the educational record, although an exception may or may not apply to this scenario (34 C.F.R. § 99.31 permits disclosures in cases of health and safety emergency).

One state reported that it already has a state registry of childhood immunizations that operates as a public authority under a contract with the state. No *authorization* is required for a health care provider to disclose immunization information to the registry. However, Medicaid does not share immunization data with the registry, creating an incomplete picture of immunization rates among low-income children. The state has suggested trying to negotiate a memorandum of understanding between the registry and Medicaid to remedy this situation. Another state is currently considering a system similar to that proposed in the scenario and has encountered major problems with sharing Medicaid data. Medicaid data cannot be shared for purposes other than to administer the Medicaid program. The proposed alternative is to gather consent from all participants.

One state has already successfully addressed issues related to accessing Medicaid data. The team noted that Medicaid generally allows data sharing with data use agreements when the study seeks to improve the administration of the state Medicaid plan. They found that university faculty will often participate in a state initiative that requires their expertise. Additionally, their health department already collects and maintains immunization and lead data through statutory authority or legal agreements, with processes in place to maintain confidentiality of the data. In this state, Medicaid frequently contracts with state universities on issues described in this scenario. Another team suggested that other state teams may want to consult this team's Medicaid electronic records system findings related to barriers encountered during its pilot program, because it involves Medicaid data exchange.

The state with the existing immunization registry also has state statutes that require the Board of Health to establish a lead-screening method and frequency. The Board of Health adopted rules in 2001 requiring that all low-income and at-risk children be screened for lead at 12 and 24 months. Lead levels are a reportable event and use and disclosure of the information is required to be reported by the state. Their governing statutes and regulations allow their Public Health Department to receive and use the data collected from lead screenings to promote the health and welfare of the children. This state reported that no

additional parental authorization would be needed for the Public Health Department to share the data with the university, unless the university uses the data for other purposes, such as research.

Ultimately, many stakeholders expressed uneasiness about providing information in identifiable form to the university when analysis could be conducted with information in de-identified form. Although the HIPAA Privacy Rule allows the sharing of information by a covered entity for research purposes, subject to conditions, implementation guidelines could differ among organizations. Many state teams felt that the variations in agreements among entities created a chasm that could not easily or quickly be remedied to create an interstate data-sharing program.

3. SUMMARY OF KEY ISSUES RAISED BY THE STATE TEAMS IN THE ASSESSMENT OF VARIATION

This section provides an overview of key issues that the state teams have raised and that have implications for the development of privacy and security requirements for electronic health information exchange.

3.1 Variation in the Interpretation and Application of Consent

The state teams have identified broad variation in the *need for* (perceived or otherwise) and the actual *process of* obtaining appropriate patient consent or *authorization* to disclose identifiable health information. The variation in application and implementation of obtaining patient consent is due to a number of factors, primarily including

- a basic misunderstanding of whether and when the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires patient permission for the disclosure of health information and, in particular, a misconception that patient permission is required to disclose information for treatment;
- differing state laws, some of which require consent to disclose health information either in all circumstances or only in some circumstances;
- professional ethical obligations to obtain patient consent to disclose information; and
- organizational decisions to require patient consent as an added protection to reduce risk of liability for wrongful disclosure.

Widespread confusion exists about the terms used for obtaining patient permission. This confusion results partly from the HIPAA Privacy Rule's use of different terms and requirements for permissions that are related to different purposes: the term *consent* applies to written patient permission to use and disclose health information for treatment payment and health care operations, while the term *authorization* is used to describe patient permission to use and disclose health information for other purposes not otherwise permitted or required by the Rule. Adding to the confusion is the variance of terms in state laws such as *consent*, *authorization*, *release*, and others to describe written patient permission to disclose health information.

3.1.1 Consent for Treatment, Payment, and Health Care Operations

The HIPAA Privacy Rule specifically permits, but does not require, a covered entity to obtain written patient permission (called *consent*) for uses and disclosures of protected health information (PHI) for treatment, payment, and health care operations (see 45 C.F.R. § 164.506(b)). No form is required for consent to share information for treatment, payment, and health care operations under the Privacy Rule; the content and format of consent to share information for these purposes are wholly within the discretion of the covered entity. The Privacy Rule, however, does require patient permission to disclose health information

for many purposes *other than* treatment, payment, or health care operations (called *authorization*). The Privacy Rule imposes specific content requirements on such authorizations. The Privacy Rule provisions are not well-understood and are frequently confused with state law requirements and federal requirements. Many states believe that patient consent is required for treatment, payment, or health care operations.⁹ In addition, many states fail to make the distinction between *consent* and *authorization* under the Privacy Rule and use the terms interchangeably.

Although the Privacy Rule allows the disclosure of health information for treatment, payment, or health care operations without consent, many state laws require such written consent to disclose health information for these purposes, using various terms in addition to *consent*, such as *permission*, *authorization*, or *release* (here, collectively referred to as *consent*). In most states, the content of such patient *consent* forms is not defined, leaving health care entities free to develop their own forms. In addition, many providers and other covered entities require patient consent to disclose health information for these purposes because of professional ethical requirements or for risk management purposes. In fact, the state teams reported that most stakeholder organizations participating in this project require patient consent for treatment in the absence of state laws or regulations requiring such permission. Even though the variation in the requirement for and content of patient permission to disclose is found primarily in the state laws and organizational practices, the Privacy Rule is often cited as the basis for requiring consent.

The term or acronym *HIPAA* appears to have become a generic explanation for nearly all privacy practices and policies that restrict the disclosure of health information; it is frequently cited as a source of concern and the reason that organizations adopt conservative disclosure policies. However, fear of sanctions for being found noncompliant with the HIPAA Rules is not the only source of concern. State teams have reported concerns about federal regulations governing chemical dependency treatment records; state regulators who conduct reviews based on licensure; state licensing boards that license individual providers such as physicians, nurses, chiropractors, and others; litigation by patients; and negative publicity.

Although all sources of liability are of concern to health care organizations, negative publicity was reported to be a significant source because of the resulting damage to the “brand” or reputation of a health care organization. Once damaged, a reputation is difficult to restore; only the passage of time can lessen the damage. Such liability is difficult to measure and difficult to counteract. Negative publicity can also result in the loss of patient confidence, a reduction in the number of payers willing to do business with a provider, and

⁹ Some of this confusion may be the result of the consent provision’s being amended between its original release in 2000 and its implementation in 2003. When it was originally released, the HIPAA Privacy Rule required patient consent for treatment, payment, and health care operations. This provision was amended in 2002, and obtaining consent became optional.

a reduction in the value of goodwill and reputation that the provider has developed over time. Because liability for inappropriate or unauthorized disclosures of health information can result in significant loss that is not easily remedied, health care organizations are cautious in their approach to exchanging data. When health care organizations have liability concerns about the exchange of information, the exchange will generally not occur. They want to be confident that any mechanism for HIE has adequately addressed privacy and security issues and minimizes their organization's liability.

3.1.2 Specially Protected Information

In general, the HIPAA Privacy Rule considers all PHI equally sensitive and, with the exception of psychotherapy notes, permits PHI to be used and disclosed for treatment, payment, and health care operations without patient permission. In contrast, a variety of federal and state statutes and regulations (laws) afford special protections for certain classes of information generally perceived as particularly sensitive and in need of a higher standard of privacy protection (e.g., HIV, substance abuse, mental health, genetic information). These laws typically require patient consent to disclose health information, often even for treatment. Several state teams reported confusion about how to handle specially protected information in accordance with these federal laws, including 42 C.F.R. pt. 2, Federal Substance Abuse Regulations, and state laws and business practices. State teams cited concerns about how to electronically meet the requirements of these laws, particularly how electronic systems will handle specially protected data and restrict the sharing of specially protected patient information. States are also struggling with how systems will effectively manage the consent for the disclosure of specially protected information. The latter concern arises from federal and state legal requirements that downstream recipients also obtain consent to redisclose information once it is in their possession.

The state teams have made it abundantly clear that the interplay among the HIPAA Rules, federal regulations that afford special protections to sensitive data, and state privacy laws creates confusion for many stakeholders. Some state teams have called for treating all health information the same by requiring patient permission for disclosure of all categories of health information.

3.1.3 Challenges Ahead

Many opportunities exist for variation as organizations navigate the regulations and policies governing consent. Four important elements affect the way organizations implement patient consent procedures: (1) federal privacy laws and regulations; (2) state privacy laws and regulations; (3) specific program requirements (such as Medicaid and public health); and (4) professional ethical obligations and additional business practices, policies, and procedures established by organizations, above and beyond what laws and regulations require. Additionally, other factors that must be considered include the following: (1) who is

disclosing the health information; (2) what information is being disclosed; (3) to whom the information is being disclosed; (4) when and how the information will be disclosed; (5) who collects the patient consent (the submitter of data vis-à-vis the requester of data); and (6) the purpose of the disclosure.

The reported variability in the interpretation and application of privacy laws and regulations concerning patient consent or authorization has additional factors, many of which can be mitigated (if not eliminated altogether) by using an electronic consent management system. Although the state teams have not developed specifications for a consent management system, they have identified many issues that will need to be resolved to move in that direction. For example, a common approach to consent is needed, one that includes definition of terms and what the required and optional elements might be.

The state teams reported multiple approaches to patient consent and the role of consumers, including, but not limited to:

- a must-all approach, in which patient consent is required in all health information exchange (HIE) circumstances;
- an opt-in approach, in which HIE is not permitted unless a patient authorizes it;
- an opt-out approach, in which HIE is permitted but patients can choose to not authorize it; and
- a no-opt approach, in which HIE is permitted and patients do not have the ability to opt out or otherwise stop it.

Additional models, such as the full opt-out approach, give patients an all-or-nothing choice about whether to include their health information in a regional exchange. The partial opt-out approach allows patients to selectively withhold the sharing of certain information (e.g., mental health) while exchanging the rest of the health information.

As already noted, the HIPAA Privacy Rule prescribes the content of a HIPAA patient *authorization* form (used in connection with those disclosures not related to treatment, payment, and health care operations and those that do not have a regulatory permission within the Privacy Rule), but most states requiring patient consent for disclosure offer no definition of what the patient consent form is or what the required and optional elements should be. In addition, accepted methods must be identified to collect and secure patient consent. In some circumstances, an e-mail submission was believed sufficient; in others, a faxed form was an acceptable method; and yet in others, a “wet signature” document was required to be on file. State teams are also working through issues related to the lack of standard procedures and business practices to confirm a patient’s signature on a patient consent form. Many questions remain about the validity, applicability, and acceptability (legal and otherwise) of digital signatures to support patient consent procedures. The lack of a recognized standard for the use of electronic signatures in conjunction with electronic patient consent forms was highlighted by a number of state teams as a major barrier to

automating the process of securing, processing, and storing consents and authorizations. Most states still rely on a “wet signature” to go along with a paper-based patient consent form, even though in most of these states electronic signatures are already recognized as legally acceptable business practices in other industries.

Moving to an electronic consent management system will require the state teams to clarify when patient consent is required under state or federal law, the requisite processes for obtaining such consent, and the mandated content of such consent. The difference between the terms *consent* and *authorization* as used in the HIPAA Privacy Rule, as well as the circumstances under which each term applies, requires clarification. Many of the state teams have identified as a priority the need for a model consent form that can be modified to accommodate the needs of the state to reduce the variation.

3.2 Misunderstandings and Differing Applications of HIPAA Privacy Rule Requirements

States reported many business practice variations based on different interpretations and applications of the requirements of the HIPAA Privacy Rule. The variation in the application of the Privacy Rule provisions was often identified as a barrier to interoperable electronic health information exchange. Many state teams reported broad variation in how the provisions of the Privacy Rule are interpreted and applied at the organizational level. This variation in the application of the rule has been identified as a barrier to interoperable electronic health information exchange by the majority of state teams.

The state teams report a general lack of understanding about the Privacy Rule’s premise to generally allow for uses and disclosures of PHI for the core treatment, payment, and health care operations purposes (those activities necessary for the health care system to operate). This lack of understanding is reflected in the business practices and policies of many stakeholder organizations. In some cases, the organizations understand the basic provisions of the Privacy Rule but do not understand how and when state law applies. Additional variation is introduced by organizational policies, many of which predate the Privacy Rule and, in an effort to reduce the risk of incidental or accidental disclosures, are more restrictive than the Privacy Rule, but which are now erroneously attributed to the Privacy Rule provisions. Summarized in this section are some examples from the state teams regarding HIPAA-related issues. The state teams’ most commonly reported source of variation related to the Privacy Rule is the interpretation and application of the *minimum necessary* standard.

3.2.1 Minimum Necessary

The HIPAA Privacy Rule states that “a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request” (45 C.F.R. § 164.502(b)). In order to meet this standard,

with respect to many routine uses and disclosures of health information, a covered entity must establish policies and procedures to limit information used and disclosed to that reasonably necessary for the purpose. Much as with consent, many states believe that *minimum necessary* applies to disclosures to providers for treatment purposes (even though the HIPAA Privacy Rule explicitly exempts this specific purpose from the *minimum necessary* requirement). A number of business practices documented by the state teams show that *minimum necessary* was applied to such treatment disclosures even in emergency-related transfers of records, creating inappropriate barriers to otherwise necessary HIE. This area clearly requires education about and harmonization of what is *reasonable*, in order to reduce the variation in how the standard is applied.

A second set of issues involved the inconsistent application of (and lack of models and best practices for) *minimum necessary* in non-treatment-related disclosures, including payment, health care operations, public health, health oversight, and judicial and administrative proceedings. What one health care provider may determine to be minimally necessary may vary greatly from another's definition. In addition, several state teams reported that some stakeholder organizations apply the *minimum necessary* standard to uses (i.e., internal disclosures) and others do not. With respect to uses, the HIPAA Privacy Rule requires a covered entity to identify those workforce members who need access to PHI and the categories of PHI to which such access is needed, and to make reasonable efforts to limit such access accordingly. This variability in the application of the *minimum necessary* standard may present a barrier to information exchange and to patient care.

A third set of issues is related to the burden of meeting the *minimum necessary* requirement in a paper-based environment. Some state teams reported that the federal requirement to limit HIE to the *minimum necessary* standard, where covered entities are involved and the standard otherwise applies, increases the time required for the exchange and affects the ability to receive comprehensive records for certain types of disclosures. Furthermore, the state reports indicate that they are unaware of current models for what *minimum necessary* for a given purpose consists of, that they believe current technology cannot limit disclosures to the *minimum necessary*, and that, as a result, processes that could be electronic must be manual. For organizations that use paper records, sifting through records to make sure that the *minimum necessary* standard is met is an onerous and inconsistent process. In addition, some state teams have noted that because the process is so burdensome and staff and resources are frequently limited, for payment-related disclosures some providers have reported a tendency to furnish payers access to the information the payer claims is necessary to obtain payment. And the HIPAA Privacy Rule allows for covered entities to rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the *minimum necessary* for the stated purpose when the information is requested by another covered entity. The burden and inconsistency issues may be mitigated by the use of electronic systems. The state team reports indicate

widespread agreement that current variation in the interpretation and application of the *minimum necessary* standard is a barrier to electronic health information exchange and that common understanding of what constitutes *minimum necessary* data sets, as well as who should receive them and under what circumstances, will be required for widespread interoperable electronic health information exchange.

3.2.2 Re-release or Redisclosure of PHI Obtained from Another Provider

Although the HIPAA Privacy Rule does not distinguish among the original sources of PHI held by a covered entity, except possibly to deny a patient's right to have his or her record amended if it "was not created by the covered entity," some state teams reported confusion about whether the rules for disclosing PHI that had been received from another provider were the same as or different from that generated "in house." Frequently, information from another provider is incorporated into an organization's internal medical records. However, some organizations limit the information incorporated into the record to information used in the course of treatment, while others incorporate all information provided.

The issue of redisclosure is another area where there is not a clear understanding among stakeholders about which state or federal regulation applies. A number of state teams reported that stakeholders were unclear whether a subsequent request for a patient's record should include the information obtained from the other organization. Many organizations reported that they would disclose only patient data that were collected by the organization. In other words, many providers believe that they cannot redisclose another provider's records. On the other hand, some organizations were concerned that specially protected information could be incorporated into the patient's record and then be released downstream without appropriate consent. Most state teams recognize that the misunderstanding around re-release and redisclosure is a source of variation that will need to be addressed to permit widespread interoperable electronic health information exchange.

3.2.3 Importance of Human Judgment Factor in Disclosures

As noted earlier, many issues related to inconsistency in practice and burden can be mitigated by moving to electronic management systems. In addition, many situations call for professional judgment or a reasonable decision to be made based on current circumstances. Several states raised the issue of perceived liability under these circumstances. Many state teams reported that fear of penalties and sanctions for violating the provisions of the HIPAA Rules creates an environment where staff interpret disclosure rules conservatively, which sometimes prevents or interrupts HIE, even in treatment situations.

3.2.4 Accounting of Disclosures

State teams consistently identified the issue of accounting for certain disclosures, required by the HIPAA Privacy Rule, as an unnecessary burden not consistently implemented by

organizations and not well understood by patients and consumers. Entities that collect and maintain information about accountable types of disclosures expressed concerns about the ongoing resources, time, and effort being spent in documenting such disclosures so that, if patients or consumers request an accounting of disclosures, they can produce it efficiently and within the time required by the Privacy Rule.

In accounting of disclosures, providers and others report that (1) very few patients and consumers have exercised their right to such accounting, and (2) the type of disclosures recorded in a HIPAA-required accounting are not consistent with the disclosure information that consumers and patients seek when they request a copy of the disclosure list. Although this mismatch is not directly a barrier to electronic health information exchange, states consistently identified it as an issue that has created confusion and added burden to the process of health information management. The main issues include the following:

- Significant confusion remains about which types of disclosures must be documented and to what extent.
- Organizations have invested significant resources in creating a mechanism to document such disclosures, and organizations continue to invest significant resources in maintaining such systems.
- Consumers rarely use these systems (only on very rare occasions do consumers request an accounting of disclosures).
- Even when consumers request such accountings, they discover that the disclosures being accounted for are not the ones they are interested in.

3.2.5 General Issues

State teams consistently reported that they continue to observe a general lack of understanding among providers and consumers about some of the basic tenets of the HIPAA Privacy Rule and how state laws interact with the Rule. Electronic systems can mitigate this source of variation and inconsistency in practice, but decisions will need to be made by stakeholders about how they want permissions for disclosures managed. State teams will also need to make decisions beyond permission for treatment in order to clarify how to manage disclosures to public health for legal and judiciary proceedings and for health oversight. In addition, state teams must decide how to manage the disclosure of information for health care operations and research.

State teams also raised issues related to the inconsistent way patient rights are administered across organizations, including the right to request an amendment to their health record, and the right to access and obtain a copy of their health information. It is clear that many health care consumers sign the forms without understanding their rights which is more an issue of education than an issue related to law or policy. Gray areas also exist in patients' rights and responsibilities about the data and the lack of standard procedures for handling breaches of privacy, the meaning of standards that address internal

issues with procedures and personnel, and external effects on individuals and relationships with other entities.

The continued lack of understanding (or clarity in definition) around these various issues leads to fear of liability among entities and to conservative disclosure policies, consequently creating unnecessary and in some cases inappropriate barriers to electronic health information exchange.

3.3 Misunderstandings and Differing Applications of the HIPAA Security Rule

A review of state reports indicated some confusion and misunderstanding about appropriate security practices; it also indicated misunderstandings regarding what was currently technically available and scalable to the health care industry and consumers. This lack of knowledge, understanding, and trust among organizations and consumers was more evident in the business practices than in state laws. For the most part, state laws did not pose challenges to sound security, nor did the HIPAA Security Rule. Sometimes the matter was simply that, even though the Security Rule accommodates scalability in security programs, organizations voiced concern related to liability when one organization that believes its security program is robust sends PHI to another organization that it perceives as having a less robust security program.

The different types of security required by the HIPAA Security Rule were also sources of confusion. The Security Rule addresses administrative, physical, and technical security. Even though more than one third of the rule addresses administrative security requirements, many organizations focused more on needed technology than on administrative safeguards.

3.4 Security

3.4.1 Authentication and Authorization

A number of state teams identified the lack of standard authentication and authorization protocols as a barrier to electronic health information exchange, especially in more routine settings. Although authentication did not seem to be as great an issue when personal health information had to be exchanged for emergency reasons, it did represent a significant barrier to the exchange of personal health information for more routine purposes, such as the movement of a patient from one primary care physician to another or the sharing of personal health information with a specialist or hospital.

State teams noted that the lack of a common method for authenticating individuals created mistrust between organizations and reduced their comfort level with other organizations' standards or policies regarding who may authorize access to personal health information. Most of the concerns were raised about interorganizational exchange of personal health

information, as opposed to intraorganizational processes for appropriate user authentication methods and standards.

The primary authentication and authorization issues were lack of standards and interorganizational mistrust. This section does not address the mistrust issues except to state that a commonly accepted set of standards regarding authentication and authorization would go far in alleviating mistrust.

Currently, for authentication some health care entities rely on phone calls or faxes from someone known to that entity while they impose stricter standards on other organizations, including the requirement that the consumer sign a consent form (although not necessarily required by law) before the PHI is exchanged. It becomes a cumbersome process that does not lend itself well to electronic health information exchange.

3.4.2 Inadequate Application-Level Data Access or Screening Controls

The state reports clearly indicate that many stakeholders are not using or are not familiar with currently available technologies. Those stakeholders that are either current users or who are exploring available technologies have identified as another critical issue current inadequacies in existing applications used to manage personal health information and used for HIE, including electronic health records (EHRs), data repositories, and the like. For example, some stakeholders indicated that they were required to print out copies of records from EHRs and redact specially protected information, or information that should not otherwise be disclosed, because the EHRs did not accommodate segregation of certain types of data. The current business practice is to print a paper copy, redact the information, and fax the redacted copy of the record to the intended recipient.

The perceived technological inadequacy stemming from the inability to appropriately segregate data was also identified as a challenge to appropriate role-based access, or to appropriate management of entities' access, to personal health information. In some cases, organizations are left with the decision to either permit internal access to excessive information or to withhold information to a degree sufficient to hinder the job duties of a member of an organization's workforce. This problem was reportedly associated with technical inadequacies and led to limiting or barring external parties' electronic access to appropriate portions of the consumer's health record. A number of the states are looking to technology vendors to address these perceived inadequacies.

3.4.3 Audit Programs

Several state teams indicated that the current lack of auditing capability because of technical inadequacies and nonexistent or poor audit programs was a challenge to electronic health information exchange, particularly when the management of community health records or HIEs was addressed.

This challenge is especially true when personal health information is shared across networks or between multiple entities, particularly regarding inadequacies in the current technical infrastructure to appropriately audit any user's access to, creation of, modification of, destruction of, or transmission of personal health information. Because community health records and the creation of HIEs are relatively new, robust standards and related audit log technology have yet to be developed.

Many applications currently used in the health care industry for transmitting or processing PHI do not include adequate audit log capability, especially so-called legacy applications (older applications built on what would be considered an outdated software platform). Several state teams raised concerns about the inability to track within their own applications external entities who may have accessed PHI stored in proprietary databases and in EHRs.

Moreover, some state teams indicated that, once again, a lack of trust exists between organizations where one organization perceives adequate audit processes have not been implemented by others. Adequate audit processes mean more than activating the appropriate audit logs; they include the development and regularly scheduled use of an appropriate audit program that addresses potential security risks and privacy risks and is based on an established set of audit criteria that match the organization.

3.4.4 Secure Transmission of Personal Health Information

Several state teams identified the secure transmission of personal health information between health care organizations, and between health care organizations and consumers, as a significant issue. Reports cited the lack of interoperable solutions and the high cost of implementing appropriate forms of secure transmission that protect the data in transit and protect against inappropriate interception and potential modification. It is more of a technical issue than an administrative security issue.

Concerns raised appear to be related to a lack of understanding of what is currently available on the market and the cost of such solutions. Many vendors serve small to large organizations, as well as consumers, and offer solutions that are scalable, affordable to small to large organizations, and interoperable.

3.4.5 Lack of a Sound Security Infrastructure

A number of the state reports addressed interorganizational security issues but did not examine barriers related to these issues (administrative, physical, and technical). Early on, the Technical Advisory Panel (TAP) noted a significant gap, especially in the provider community, between those organizations that have established sound security programs within their organization and those that have yet to meet the requirements of even the HIPAA Security Rule. Most reports addressed situations in which PHI moves outside their control, as opposed to situations within their control.

The lack of appropriate security program investment by health care and related organizations stems generally from 3 areas that should be reviewed and addressed at the organizational, state, and federal levels:

- lack of knowledge about appropriate security practices and HIPAA Security Rule requirements;
- lack of investment in security on the part of the industry (and, in some cases, government); and
- lack of HIPAA Security Rule enforcement by the US Department of Health and Human Services.

The fact that most state teams did not specifically address intraorganizational security issues per se demonstrates, in part, a lack of knowledge of appropriate security standards. The HIPAA Security Rule is scalable so that small to large organizations can appropriately implement sound security practices. Ultimately, interorganizational security solutions cannot be fully addressed if participating entities in an HIE have not established security programs that adequately protect personal health information managed by any participating entity. The lack of a sound security program represents a weak link in the exchange process.

One area addressed by the state teams was the potential cost of implementing appropriate security practices, the lack of infrastructure to support such practices, and other potential technical barriers (such as applications without audit logs, EHRs without the ability to partition data to meet *minimum necessary* standards, and the like). This area must be addressed, even though it is not within the scope of this project. The lack of a sound privacy and security infrastructure in a number of areas, and a lack of funding to create one, was a fairly common theme.

3.4.6 Variability in Administrative and Physical Safeguards

A number of state teams noted that the lack of adoption of consistent and appropriate administrative and physical safeguards within health care organizations has resulted in mistrust between organizations and increased concerns related to liability (where an organization with a sound security program transmits PHI to an organization that lacks a sound security infrastructure). As previously mentioned, most appropriate security measures fall within the administrative and physical realms.

This issue is not related to technology; rather, it involves lack of understanding about, or insufficient emphasis on, appropriate security for any size organization. Several state teams noted that such inconsistency resulted in barriers to electronic health information exchange and that a good part of the solution would be to address such inconsistencies or inadequate security programs through education and properly understood minimum standards sufficiently flexible to fit the needs of all sizes of health care organizations. Some would say that the Security Rule was designed to do just that—set minimum standards that are

scalable. The state reports did not describe specific measures or processes thought to be lacking in the Security Rule, nor did the reports discuss what would make these organizations more comfortable than the existing Security Rule standards. For example, the problem could be a lack of standards, a lack of enforcement, or some combination. Some state teams alluded to accreditation as a potential solution.

State teams noted that reducing the variability in the application of administrative and physical security would do much to reduce certain challenges to electronic health information exchange, improve trust among organizations, and reduce liability concerns. It makes sense that an organization would be more willing to engage in electronic health information exchange with another organization if the exchanging organization had a higher comfort level and that the recipient had adopted adequate administrative and physical security safeguards.

3.5 Trust in Security

Trust, especially as it affects the potential viability of electronic health information exchange, was a critical issue raised in many of the state reports. Specifically, consumers and providers expressed concerns. Consumer concerns tended to focus on privacy risks arising from the implementation of new technologies and the potential for unauthorized disclosures of specially protected information to payers and employers. Providers were principally concerned about potential liabilities from the activities of other participants in electronic health information exchange and about consumers' lawsuits for inappropriate disclosures of their information; they were secondarily concerned about potential uses of information about consumers by payers and the government.

The review of trust issues was complicated by the fact that data on critical issues and business practices were not typically categorized under this heading and, in some cases, trust (or lack of it) may have been a motivating but unidentified reason for business practices. In a number of cases, stakeholders other than consumers (e.g., providers) articulated their impression that consumer lack of trust was a critical issue, but no consumer data were provided. Ten of the reports lacked information that either expressly or by reasonable inference raised trust as a critical issue.

The leading trust issue was provider fear of lawsuits and liabilities associated with electronic health information exchange. This issue was identified by 10 reports and was based mostly on the fear of liability for errors or improper actions by other parties participating in HIE. One state identified trust (or lack thereof) as their single most significant issue, one that had been repeatedly raised, and the reason providers were not willing to participate in electronic health information exchange. Whether this fear has actually been validated by experience is unclear; however, one team identified as a concern a specific statute giving patients a cause of action for inappropriate disclosure, and another reported that HIPAA-

based claims are being included in lawsuits by patients frequently enough that one provider had reported 6 such claims within the preceding 6 months. (The specific legal basis for such claims is not identified, and the HIPAA Rules do not provide a cause of action for individuals.)

The second most significant trust issue was consumer lack of trust, which appeared to have been expressed directly by consumers in 4 reports and was apparently an issue perceived by nonconsumer participants in 6 others. The principal basis articulated for this lack of trust was concern about payer and employer access and, secondarily, distrust of new technologies. It appears that one major reason for this lack of trust is the substantial number of security breaches that have been reported over the past few years, including several involving health care organizations.

The most significant general impression that arose from this review was that providers' trust concerns, in particular, appear to be directly correlated with HIE experience. In other words, providers in states with relatively few electronic health information exchange activities, or a briefer history of such activities, appear to fear they may be held liable or penalized for engaging in them and, in some cases, do not trust the technologies. Providers in states with more experience appear not to have such concerns or to have them to a lesser degree.

Finally, one noteworthy finding is that 2 states reported similar reliance on good faith and personal relationships in current practices and identified this reliance as a positive value that participants wished to preserve.

3.6 State Laws

The stakeholders identified a number of difficulties with the state laws governing privacy and security, including a general misunderstanding of the intersection of state laws and the HIPAA Rules, general confusion about where in the state code the law was found and how it was applied, and concern that when the law was readily identified and understood it was often too antiquated to apply sensibly to electronic health information exchange.

In fact, the leading issue was the absence of state laws clearly applicable to HIE (sometimes referred to as laws pertaining to regional health information organizations [RHIOs]), which was identified by 11 state teams. Ten state teams identified the generally confusing conditions of state laws as a critical issue, and 11 state teams reported the use of overly conservative business practices because of confusion or lack of knowledge about state laws. ("Overly conservative" in this context means more restrictive in information sharing than actually required by law.) At least 2 state teams noted that a number of stakeholders, particularly providers, were unaware of the need to comply with state laws more restrictive than the HIPAA Rules and were, in effect, treating the HIPAA Rules as a federal ceiling rather than a federal floor.

Beyond these general issues, the principal challenges identified involved lack of clarity surrounding the sharing of information with law enforcement (6 state teams), public health and bioterrorism reports (5 state teams), and confusion about minors' consent (5 state teams). Three state teams reported confusion about both genetics laws and electronic signatures.

One difficulty in reviewing these reports for state law awareness is identifying state laws that the participants may have entirely overlooked. For example, Scenario 3 included facts involving execution of an electronic signature. Although almost all states have some form of electronic signature statute and most have enacted the Uniform Electronic Transactions Act, this was not raised as a legal issue. Likewise, none of the reports discussed the possible implications or barriers raised by practices responsive to the security breach notification statutes now in effect in 17 of the reporting states.

The lack of awareness of and confusion about state laws not only raises risks for electronic health information exchange participants, but it may also cause them to overlook opportunities such as the liability limitations available under some state digital signature laws (Illinois, Utah, Washington) or useful principles available under other electronic signature laws. (Digital signatures are a specialized form of electronic signature.) Confusion about sharing information for law enforcement, public health, and bioterrorism purposes, in particular, appears to be a critical problem, given concerns about possible bioterrorism incidents, natural disasters, pandemic flu, and other mass crises. Current practices appear to rely heavily on goodwill, which is necessary but perhaps not sufficient, especially when interstate coordination is necessary.

The perception that most state laws need reform may present an opportunity to develop uniform (or at least consistent) HIE-related state laws. If so, this opportunity should be pursued promptly because legal reform may be one of the key solutions pursued by many of the reporting states. Unless an effort is made to coordinate such efforts, the various states may implement inconsistent reforms, perhaps resolving some of their own problems but raising new barriers to regional and national interoperability.

3.7 Networking Issues

This section is included because a number of state teams identified network issues as critical to health information networking and limitations that will result in barriers to electronic health information exchange. A common concern across states was the lack of well-defined, operational, and deployable models for regional networking. Significant concerns emerged among the state teams regarding, for example, the legal status of such organizations, their ability to legally operate HIEs, and their ability to store and maintain data. States were also concerned about the lack of uniform legal models and business practices for stakeholders to use after they joined a regional health network. Most state teams reported quite limited

interorganizational exchanges of clinical information electronically for 3 reasons: (1) lack of implementation of regional networks, (2) limited deployment of EHR systems, and (3) lack of interoperability in those EHR systems that have been deployed. The electronic health information exchanges between organizations are limited mainly to content-specific clinical messaging in the areas of pharmacy/prescription drug information (e-prescribing), laboratory data, and radiology/digital imaging data.

Significant capacity gaps and variations exist in the levels of resources, technical capabilities, and financial means of organizations (i.e., large versus small, urban versus rural). These gaps create significant variation in HIE practices among organizations; in turn, these variations in HIE practices limit or restrict the ability of organizations to conduct interorganizational electronic health information exchanges (lack of compatible systems, lack of compatible practices, lack of trust). State teams also noted that different types of electronic health information exchange (i.e., provider-to-provider, provider-to-payer, payer-to-payer, and between others) require different handling: some will occur through true message exchanges, some will be done via “pull” mechanism, and others will be achieved with a “push” approach.

States also noted a high comfort level with existing paper-based and manual systems practices and processes for data exchanges. Many expressed the general belief among state participants that current manual practices are timely, are effective, and produce accurate data.

3.8 Linking Data from Multiple Sources to an Individual

The ability for a health care provider to identify the correct records for a patient is critical to clinical medicine and to electronic health information exchange. The lack of a standard, reliable way of accurately matching records to patients introduces the potential for inappropriate use or disclosure of personal health information from the wrong patient, which is both a clinical and a privacy risk. This risk is particularly acute when information is shared across institutions that use different methods of patient and record identification.

Patient and provider identification across organizations is required to

- improve administrative efficiencies and reduce health care costs by minimizing the collection of redundant information and by reducing or eliminating the need to perform redundant tests (because of the inability to access information about a patient in a timely fashion);
- provide better-quality care, avoid medical errors, and improve patient safety;
- control against identity theft, fraud, and abuse;
- appropriately match data about an individual from one organization to another when HIEs are performed;

- appropriately authenticate a patient or a provider to come into an organization's system;
- establish access controls to certain health information on the basis of the authenticated identity of a patient or a provider;
- implement mechanisms to prevent inappropriate access to data or monitor the access to data by patients and providers; and
- implement core HIE functionality.

Recent developments in the area of personal health records have also advanced the need to establish a consistent and reliable method for linking patients to their records so that authorized providers and other users can locate the right information about the right patient.

Unique patient and provider identification was also discussed as part of the overall review of critical *security* issues. Identifying patients and providers appropriately is not only critical in the delivery of quality care to patients and for HIE, but is also a fundamental issue in other information security domains, such as authentication and authorization.

The variability in methods across organizations to link patients to records and the lack of agreed-upon patient-to-record matching standards to apply when interorganizational HIEs are conducted were perceived as major challenges by many state teams. These challenges were not the case in uniquely identifying *providers* across the health care system because new federal HIPAA regulations have now established a national standard unique identifier for health care providers (the National Provider Identifier, or NPI). Providers, payers, and others are required to fully implement the NPI by May 23, 2007. As enacted by Congress, HIPAA (the Act) provided for the creation of national unique patient identifiers; however, HHS and Congress have put the development of such a standard on hold indefinitely. In 1998, HHS delayed any work on this standard until after comprehensive privacy protections were in place. Since 1999, Congress has adopted appropriations language to ensure no appropriated funds are used to promulgate such a standard.

3.8.1 Types of Patient Identification Used

Current practices reported by participating stakeholders from most states pointed to the use by organizations of unique, asynchronous, and incompatible methods to establish the identities of their patients, enrollees, clients, and consumers. State teams reported instances, even within organizations, in which the same patient had been assigned more than one ID (e.g., a patient's ambulatory or primary care clinic record vis-à-vis the same patient's inpatient or hospital record). Although this multiple assignment of ID is often caused by errors, such as spelling variations in names and transpositions of dates, some hospitals intentionally assign a different ID number to the same patient for each admission.

Given the lack of a national (or state) unique patient identifier, state teams discussed several alternatives for future use under organized regional networks to address the need for matching patients to their records across systems. One frequently cited mechanism is a record locator service. This type of service holds information that has been authorized by the patient and tells the system where authorized information can be found, but not the actual information the records may contain. It enables a separation of the function of locating authorized records from the function of transferring them to authorized users. Release of information from one entity to another is subject to authorization requirements between those parties; in certain specially protected treatment situations, patients or providers may choose not to share information. Record locator services are operated by multistakeholder collaboratives or exchanges and are based on a master patient index, a database that contains a unique identifier for every patient in a health care organization or system. The master patient index includes the medical center, outpatient clinics, practice offices, and rehabilitation facilities. All registration systems would use the master patient index to obtain patient information based on several identifiers.

A master patient index may employ deterministic indexing, in which searches are based on an exact match of the combination of name, Social Security number, date of birth, and gender. A master patient index may also use a rules-based searching mechanism (i.e., perhaps using the first 4 letters of the last name or other key identifiers). A commonly used search mechanism is probabilistic matching that may or may not use a Soundex formula. Soundex coding helps to ensure that spelling variations are accounted for in the search.

A number of states have discussed the need to adopt the use of these mechanisms and systems and are debating the associated policy issues related to uniquely identifying patients across organizations as a foundation of the evolving HIEs.

3.8.2 Different Identification Systems: Common Challenges

States highlighted the following challenges associated with the variability and incompatibility of patient identification systems and approaches. These included the following:

- inability to appropriately link patient information across systems for delivery purposes (applicable to both paper and electronic environments);
- inability to create longitudinal, multifacility continuum-of-care episodes for a patient;
- inability to track patients across a full episode of care and monitor performance of the health care system (public health functions); and
- lack of interoperability across systems for purposes of identifying providers, which forces a patient's providers to "jump" from one system to the next in order to gather and manually integrate all the information available on him or her instead of using automated methods to aggregate the information across sources.

Provider-related challenges included the need to access health information about a patient (residing in different systems) and the need to know all the unique identifiers assigned by those systems to the patient in order to access the information accurately and reliably.

Consumer-related challenges included the fact that consumers with health information residing at various organizations and in various systems are required to maintain different types of identifiers to access their information reliably.

3.8.3 Patient Identification: Consumer Communication and Education

Many state teams noted the need to engage consumers early and throughout the process of establishing such unique patient ID approaches, to help them buy into the proposed approaches, and to support any legislative and funding initiative necessary to support the implementation of the proposed methods.

The state teams were acutely aware of the potential increase in risk of privacy violations and identity theft, a risk increase brought about by any attempt to implement a unique patient ID across institutions or regions, and they were aware of the need to counter possible negative public reaction with effective security controls and extensive consumer education.

3.9 Interstate Issues

Interstate issues were typically raised by states for 3 reasons: (1) they had considerable sharing of health care information across state lines; (2) when the state experiences very large seasonal inflows of both out-of-state workers and tourists, its temporary residents make substantial use of out-of-state providers; and (3) a number of interstate health systems and plans have facilities and do business in the state. One markedly rural state noted that, because of its relative paucity of certain types of health care facilities, access to other states' hospitals and specialty services is crucial for its residents: any meaningful health information infrastructure would have to reach major metropolitan areas in 3 other states.

The legal variations noted as potential barriers to electronic health information exchange include differences in standards for genetic information; electronic prescriptions; immunization, HIV/AIDS, and minors' rights; minors' consents; workers' compensation; and mental health and substance abuse. In addition to interstate issues, at least one state team reported that variations between state and Native American tribal standards were critical to developing statewide HIEs. Several states noted that they did not believe interstate issues to be problematic and indicated that the disclosing state's law generally controlled the electronic health information exchanges. Most issues were among organizations rather than among states, and interstate issues tended to be resolved within organizations.

No state identified variations in security breach notification laws as an issue (although this important issue has been widely discussed in the past 2 or 3 years). Security breach notification laws have been adopted in at least 26 states, including 17 of the states reporting and 14 states adjacent to reporting states. The application of a state's law is triggered by a security incident, in electronic form, affecting health information about residents of the state, wherever the incident occurs. Organizations in states without security breach statutes are required to notify residents of other states with such laws if information about them has been affected. For example, in a notorious incident last year, the multistate Providence Health System experienced a security incident when electronic media were stolen in Portland, Oregon. Although Oregon does not have a security incident law, the organization was required to notify residents in several states that did, including the adjacent state of Washington.

3.10 Disclosure of Personal Health Information

The ability of one entity to disclose health information to another is at the core of the implementation of interoperable HIEs. Several federal and state laws and regulations, as well as specific program requirements, affect whether specific disclosures can take place and the way such disclosures can be achieved. Overall, state teams consistently identified the variation in business practices related to the disclosure of health information as a significant factor affecting the ability to conduct electronic health information exchange between organizations.

3.10.1 Interpretation of Requirements for the Re-release or Redisclosure of Health Information

One of the common challenges identified by state teams was the variability in the understanding of when health information can be re-released or redisclosed by an entity that received the information from another entity. Although this issue spans several scenarios, it was particularly noted in discussions of specially protected health information, such as mental health or substance abuse records.

Some states mentioned that the current paper environment is more conducive to preventing "unintended" redisclosures than a future EHR environment, although other states noted that the electronic environment was more capable of effectively controlling information that could or could not be disclosed.

3.10.2 Differences in How Specially Protected Health Information Must Be Treated

Almost all states highlighted as a major concern the differences in how certain health information (generally considered more sensitive than other types) must be specially handled when one is disclosing such information. In particular, the variability in the

understanding, interpretation, and implementation of federal and state laws and program requirements results in more stringent protection of these data.

One concern noted by state teams was the creation of a dual standard for handling health information: the basic standard for all health information not considered relatively sensitive, and a more stringent set of requirements for specific health information considered sensitive. Examples of sensitive data include

- data about minors,
- data concerning reproduction,
- data about communicable diseases,
- data about sexually transmitted diseases,
- HIV/AIDS data,
- mental health data,
- chemical dependency data,
- genetic information,
- prescription drug information (when it may lead to the disclosure of a sensitive condition), and
- abuse and neglect exposure.

In some cases, the additional requirements for protecting these types of data create the need to implement dual or separate patient consents, “per instance” consents when recurring disclosures are going to be needed, or even special re-release consents when a second provider is making the disclosure.

Other issues and concerns expressed regarding sensitive health information involved determinations about what is specially protected health information; specially protected information is usually defined by the provider on the basis of his or her understanding of the rule and the type of data being disclosed. Concerns about interstate exchange of specially protected information abound because of differences among states on the handling of specially protected information.

3.10.3 Issues of Ownership of Health Information

State reports also identified the lack of a clear and consistent definition of ownership of health information (and the variability in the interpretations of who owns the data) as a challenge to electronic health information exchange.

Most state teams reported that the HIPAA Privacy Rule did not address ownership and that state laws also lacked any specific references to the issue. Nevertheless, some state teams did identify specific state laws that defined ownership of medical records, although in many

cases the state laws identified the provider who generated the record as the owner of the record while in other states the individual was considered to be the owner of the record.

3.10.4 Need for Fast, Easy, and Secure HIE Under Medical or Health Emergency Circumstances

State teams agreed on the need to ensure that, under emergency circumstances, health information will be able to be exchanged quickly, easily, and securely between and across providers, as well as across state borders. In the description of business practices related to the emergency circumstances scenario, many state teams noted confusion about when, how, and by whom a patient consent must be solicited for an entity to receive health information about the patient from other providers. States also expressed concerns about the minimum amount of data that should be exchanged in emergency situations, or whether all data should be accessible and available.

Additional concerns included specific state laws that might restrict the disclosure of certain information even in emergency situations without a proper patient consent, and challenges attributable to exchange of data across state borders when different state laws and regulations apply.

3.10.5 Variations in Interpretation of Reporting Requirements for Public Health Purposes

When dealing with reporting of health information to public health agencies, states reported the following issues:

- Most participating stakeholders were able to identify appropriate and relevant state laws that required and defined the parameters under which specific disclosures of health information to public health must be performed.
- Stakeholders also noted a lack of standardized rules for all public health entities across states when they were requesting access to patient information. Some states may be reluctant to disclose patient health information to states that have less stringent privacy protections.
- Many types of public health notifications exist, and in some cases the *minimum necessary* standard may apply to such disclosures. When disclosing health information to public health authorities, providers may rely upon public health officials' representations that the information they have requested is the minimum amount necessary, but public health authorities have no consistent mechanisms by which to determine the level of information that is necessary.
- Entities have difficulty identifying and relating to the multiple layers of public health laws and regulations covering the release of health information.
- Many states reported that they tend to not disclose information for fear of being sanctioned for a particular privacy law of which they were not fully aware or did not understand appropriately.

- Covered entities expressed concerns about providing health information that is protected by the HIPAA Privacy Rules, and losing control over the privacy and security of the same information once it is released to a noncovered public health entity.
- Many participating stakeholders reported a lack of trust in public health agencies because of a lack of transparency about health information disclosures related to public health.
- Most public health reporting currently is paper-based, and most providers find it an onerous process that may be improved tremendously with the adoption of electronic health information exchange.

3.10.6 Handling of Disclosures Related to Judicial Proceedings and Law Enforcement

The disclosure of health information in instances in which judicial proceedings and law enforcement are involved was also reported to have some variations as to when such disclosures may occur, how they can be achieved, what specific requirements must be met for providers and others to be able to make the disclosure, and whether a patient must consent to such disclosures (even though the HIPAA Privacy Rule permits such disclosures, subject to certain conditions, without patient *authorization*).

In most cases cited by state teams, the determination of whether a particular disclosure could be made to law enforcement followed strict parameters and business practices. Most states also had laws that required either patient consent or a court order for such disclosures. The issues identified by states related to whether front-line staff dealing with such situations were appropriately trained on the implementation of the business policies and procedures established by the organization for this type of disclosure.

3.11 Cultural and Business Issues

States referenced cultural and business issues that pose challenges to electronic health information exchange. One example is concern about liability for incidental or inappropriate disclosures, which causes many stakeholder organizations to take a conservative approach to developing practice and policy. Another example of a business issue that poses a challenge is general resistance to change, a common issue that organizations face whenever a change in business causes a work flow process to change. Such resistance is frequently cited as a cultural issue in discussions about decisions to adopt electronic systems. Some individuals within organizations are comfortable with existing paper-based or manual systems and data exchange practices and processes, and they believe that current manual practices produce accurate data and are timely and effective. Implicit in some discussions is an assumption that security slows down the process: the data are secure but are not transmitted as fast as they can be with a quick phone call. In fact, most data exchanges take place via person-to-person contact, especially in emergency situations, and human judgment plays a large role in how and when information is exchanged. It will be critical to

include these points at which human judgment is required in the specifications for any system developed to exchange information.

A third business issue that cuts across all the scenarios and domains is the need for clear definitions of terms within state and federal laws. For example, terms like *medical emergency*, *current treatment*, *related entity*, and *minimum necessary* do not have agreed-upon definitions and, therefore, increase variation as organizations attempt to meet compliance by defining terms in ways that protect the interests of the organization. The term *health record* is a good example: organizations disagree about whether or not a patient's demographic data and a pointer to the location of a patient's health information constitute a *health record*.

One example of a cultural and business issue involves the tension among health care providers, hospitals, and patients concerning who controls or owns the data. A number of providers indicated that they did not think that patients should have full access to their records, especially to doctors' notes. They were concerned that providers would not enter complete notes if patients had access to them. Although the Privacy Rule provides patients the right to access their medical records, the stakeholders who raised this issue either appear to be unaware of that provision, or are not HIPAA covered entities. Liability was also a concern. However, the majority of stakeholders agreed that, to be successful, electronic health information exchange must be designed to address patients' needs, interests, and concerns.

4. REVIEW OF STATE SOLUTION IDENTIFICATION AND SELECTION PROCESS

The process of developing solutions required each state project team to review barriers to private and secure electronic health information exchange and select a subset of issues to address based on an assessment of impact. At the same time, state project teams were to review best practices (those that protect privacy and facilitate interoperability) for possible statewide adoption. Work groups would then meet with relevant stakeholders and develop solutions. For each proposed solution, state teams were asked to discuss the issue or problem that the solution was intended to resolve, the relevant domain area, the specific type of use or disclosure, and the relevant stakeholder groups. State teams were also asked to describe how their proposed solutions had been vetted, evaluated, and prioritized, and whether each solution had been tested, partially implemented, or was in use by a limited set of stakeholders. State teams needed to assess the feasibility of each proposed solution or recommendation and were asked to consider the structural, legal, legislative, and economic impediments to implementation.

4.1 Solutions Work Group Formation

Nearly all state teams made a conscious effort to ensure continuity between the assessment stage and the solutions stage by including members of their Variations Work Group (VWG) and Legal Work Group (LWG) in their Solutions Work Group (SWG) and then adding key resources through targeted recruitment. The teams noted that the composition of the SWG often evolved through time, depending on the knowledge and experience required to address specific barriers. Two state teams reported carrying the notion of continuity further by merging their SWG with their Implementation Planning Work Group (IPWG). Table 4-1 summarizes the makeup of the SWGs across the 34 states. Each state team submitted a table reporting stakeholder group membership in work groups and participation through outreach. The tables submitted by the state teams made it possible to summarize stakeholder group participation consistently and accurately.

Each category row (in bold typeface) summarizes the results for the related subcategories reported in the rows immediately below it. Not all categories required subcategories. For example, of the 34 state SWGs, 33 or 97% included technology and health information experts as members, and the number of state teams that included each specific type of expert is reported in the 8 subcategory rows that appear immediately below this row in the table. On average, membership of state SWGs included 8 of the 11 bold categories of stakeholder groups and 17 of the 34 more specific stakeholder groups. (Categories that do not have subcategories are treated here as specific groups.) Technology and health information experts were most frequently cited as members of SWGs. From 90% to 95% of the teams also included public health agencies, providers, and attorneys. About three

Table 4-1. Stakeholder Group Representation of Solutions Work Group Members

Stakeholder Group	States Including Stakeholder Group in Solutions Work Group Membership (N = 34)	States Including Stakeholder Group in Solutions Work Group Membership (%)
Technology and health information experts	33	(97)
Privacy and security experts/compliance officers	28	(82)
Health IT consultants	25	(74)
Electronic health records experts	21	(62)
Technology organizations/vendors	19	(56)
Health information management organizations	17	(50)
Quality improvement organizations	17	(50)
Regional health information organizations	15	(44)
Other health data and technology experts	5	(15)
Public health agencies or departments	32	(94)
Providers	32	(94)
Hospitals/health systems	31	(91)
Physicians and physicians groups	28	(82)
Clinicians	27	(79)
Professional associations and societies	23	(68)
Community clinics and health centers	20	(59)
Mental health and behavioral health	18	(53)
Pharmacies/pharmacy benefit managers	15	(44)
Emergency medicine	11	(32)
Long-term care facilities and nursing homes	10	(29)
Homecare and hospice	9	(26)
Laboratories	9	(26)
Federal health facilities	8	(24)
Safety net providers	8	(24)
Other health care providers	6	(18)
Legal counsel/attorneys	31	(91)
Other government	26	(76)
Medicaid/state government except public health	24	(71)
County government	6	(18)
Consumers	26	(76)
Consumer organizations and advocates	21	(62)
Individual consumers	19	(56)
Medical and public health schools/research	25	(74)
Payers	25	(74)
Employers	12	(35)
Law enforcement and correctional facilities	7	(21)
Other	5	(15)
Foundations/other policy consultants	1	(3)

fourths of the SWGs included other government, consumers, medical and public health schools/research, and payers.

State teams also reported on the stakeholder groups that participated in solutions development and evaluation through outreach (see Table 4-2). Providers, technology and health information experts, and payers were the most frequently reported stakeholder groups participating in solutions analysis through community outreach.

4.2 Process Used to Identify and Propose Solutions

All state teams described an iterative process of solution development, review, validation, and refinement. The overall process usually involved meetings at which barriers were reviewed and categorized, brainstorming sessions for developing solutions, followed by targeted outreach to the stakeholder community for additional input.

Materials were often prepared and distributed prior to meetings. These materials described the background of the study (for participants who had not participated previously), the barriers that had been identified, key topics and issues, and in a few instances, a set of preliminary solutions that had already been developed by the core team.

Meetings were held in person whenever possible, with some members participating by telephone. Additional input was collected via the Agency for Healthcare Research and Quality (AHRQ) National Resource Center portal, by e-mail, and by interviewing key stakeholders. A few state teams reported using Webex meetings during solutions development, and 2 states used surveys to collect proposed solutions from stakeholders.

One key challenge was to reduce the task to a manageable size. Nearly all states sorted barriers into categories by domain, by cluster of domains, or by topic area. Many teams used the topic area categories developed by RTI for the regional meetings. This categorization allowed teams to focus on barriers that tended to cluster and offer wide impact through broad application. Teams usually reduced the task further by breaking the SWG into smaller subgroups assigned to specific topic areas or categories. These smaller subgroups met, brainstormed solutions, and reported back to the larger group. Solutions development usually required a series of meetings to complete the process of review, validation, and refinement. Additional approaches included identifying root causes and developing use cases to test solutions.

4.3 Process Used to Vet, Evaluate, and Prioritize Solutions

Nearly all state teams described a vetting process that involved review by the SWG, the LWG, the steering committee, the broader stakeholder community, and key government officials. The process established regional health information organizations (RHIOs). In a few states, evaluation and prioritization activities continue to be reported as planned rather than having occurred by the report date. State teams reported a number of ranking, scoring, and

Table 4-2. Stakeholder Group Engagement in Solutions Development and Evaluation

Stakeholder Group	States Engaging Stakeholder Group Participation in Solutions Analysis through Community Outreach (N = 34)	States Engaging Stakeholder Group Participation in Solutions Analysis through Community Outreach (%)
Providers	30	(88)
Physicians and physicians groups	30	(88)
Hospitals/health systems	28	(82)
Clinicians	27	(79)
Professional associations and societies	22	(65)
Mental health and behavioral health	18	(53)
Pharmacies/pharmacy benefit managers	16	(47)
Community clinics and health centers	15	(44)
Long-term care facilities and nursing homes	14	(41)
Emergency medicine	13	(38)
Homecare and hospice	11	(32)
Federal health facilities	10	(29)
Laboratories	8	(24)
Safety net providers	8	(24)
Other health care providers	8	(24)
Technology and health information experts	29	(85)
Health IT consultants	23	(68)
Privacy and security experts/compliance officers	22	(65)
Quality improvement organizations	20	(59)
Electronic health records experts	19	(56)
Regional health information organizations	17	(50)
Technology organizations/vendors	15	(44)
Health information management organizations	14	(41)
Other health data and technology experts	4	(12)
Payers	28	(82)
Public health agencies or departments	27	(79)
Medical and public health schools/research	25	(74)
Legal counsel/attorneys	25	(74)
Other government	25	(74)
Medicaid/state government except public health	25	(74)
County government	5	(15)
Consumers	23	(68)
Consumer organizations and advocates	21	(62)
Individual consumers	14	(41)
Employers	14	(41)
Law enforcement and correctional facilities	7	(21)
Other	2	(6)
Foundations/other policy consultants	1	(3)

weighting methods for seeking consensus during priority setting. One state prioritized solutions, reporting that they first eliminated those they considered not feasible and then ranked the remaining solutions based on ease of implementation, resources required, technological feasibility, comportment with the current legal and regulatory environment, and the readiness of the affected stakeholder community to adopt the solution. Evaluation criteria mentioned in other states included impact on consumer protection and privacy, relationship to national standards, timing, and compatibility with pilot testing. SWG participants in one state submitted ballots via e-mail, which allowed them to rank solutions and narrow their focus. Another state team reported their plan to test their solutions through use cases and the need to align their priorities with other state projects.

4.4 Determination of Feasibility

In most states, preliminary determination of the feasibility of solutions was based on an evaluation of cost, ease of implementation, and time required for implementation. One state team noted that the most feasible solutions are those that can be implemented without new technological development and do not require substantial modification of existing laws and regulations. One state team reported that they tested feasibility through a discussion of solutions currently in use, potential alternatives, outcomes and constraints associated with alternative solutions, cost, implementation strategies, and best practices. Another state team's feasibility criteria included economic, technical, organizational and cultural, time, and the level of participation required.

5. ANALYSIS OF STATE PROPOSED SOLUTIONS

State solutions were organized into 5 general categories according to the needs that they addressed: practice and policy; legal and regulatory; data standards; education and outreach; implementation and governance; and ancillary issues (such as funding and incentive for electronic health record [EHR] adoption). Within each subsection, solutions were clustered according to the specific issue that they address.

5.1 Reducing Variation: Practice or Policy Solutions

5.1.1 *Interpreting and Applying the HIPAA Privacy Rule*

The Privacy Rule is frequently cited as limiting exchange, even though it allows the exchange of information, without consent or *authorization*, for the purposes of treatment, payment, and health care operations, among other purposes.¹⁰ Three key issues have been raised by the state teams in regard to the Privacy Rule. First, providers may genuinely misunderstand the law and how and when it applies: at least 3 state teams observed misunderstanding to be more common among small physician practice groups or individual providers, who often do not even know if they are covered entities and, if they are covered entities, may not have access to legal counsel. In addition, office staff members may not be properly trained, and may follow different protocols when releasing information. Second, some payers or providers may use the law as a shield to even permitted disclosures in an effort to protect proprietary information. Third, many providers fear sanctions for inappropriate disclosures and adopt a conservative stance toward exchange to protect their organizations from prosecution or civil penalties.¹¹ Thus, although the Privacy Rule allows exchange under many circumstances, it is a convenient excuse for ignorance, for a desire to retain proprietary information, or for fear of liability.

In many instances, state law is more restrictive than the Privacy Rule. The Privacy Rule serves as a federal floor with respect to privacy protections, rather than a ceiling, and does not preempt state laws that offer more protections. The state teams have identified the need to review many of the more protective state laws to determine whether they will apply sensibly to the electronic exchange of health information. Some of these laws may pose barriers to exchange because they were enacted on the basis of requirements for paper-

¹⁰ Other permissible disclosures that do not require consent or authorization include instances when disclosure is required by another law; for research, subject to approval by an institutional review board; incident to an otherwise permitted use and disclosure; for public health; for law enforcement; for other specified disclosures in the public interest. In addition, information can be disclosed in a patient directory or to family/friends only with the opportunity for the patient to agree or object to the disclosure.

¹¹ The US Department of Health and Human Services (HHS) may impose fines of \$100 per failure to comply with the HIPAA Privacy Rule, up to \$25,000 for violations of the same requirement. Individuals who knowingly disclose personally identifiable information face fines of up to \$50,000 and a year in prison. These penalties increase if there was intent to profit from the disclosure or if the information was obtained under false pretenses.

based exchanges. For example, a state law that requires a wet signature poses a barrier to electronic health information exchange. State teams will need to work through a solution that fits the rationale behind the wet signature law to permit electronic exchange and maintain the appropriate protections as determined by the stakeholders.

State teams offered a variety of solutions aimed at reducing variation resulting from differing interpretations and applications of the Privacy Rule and the *minimum necessary* standard. Solutions included standard policies or policy guidance, standard documents, Privacy Rule education, and requests for clarification regarding certain Privacy Rule requirements from appropriate authorities.

The HIPAA Privacy Rule states that “a covered entity must make reasonable efforts to limit protected health information to the *minimum necessary* to accomplish the intended purpose of the use, disclosure, or request.” However, the *minimum necessary* standard does not apply to disclosures to or requests by a health care provider for the purposes of treatment or use or disclosure that is required by law. However, some providers are extending the *minimum necessary* standard to treatment disclosures, which presents a challenge and may also harm patients if information is not provided promptly or is incomplete. Providers may also have technical difficulties in extracting the information from records. One state sought to address the standardization of the application of the *minimum necessary* standard and the *medical need to know* (a term governing the disclosure of HIV/AIDS information) by including specificity for read and write access in the exchange of personal health information. Nine states specifically referenced the *minimum necessary* standard and offered solutions to remedy misunderstandings and differing applications related to the standard.

Issue: Providers do not understand when the *minimum necessary* standard applies.

Solution: Create standard policies and procedures and training regarding use and disclosure of health information in accordance with the Privacy Rule and state law.

Solution: Identify standards to address limiting data to the *minimum necessary* for requested purposes.

Solution: Adopt statewide health information exchange (HIE) standards/protocols to define uniform cross-enterprise digital documents/content to represent routine health care exchanges and noncare exchanges.

Solution: Develop consensus model documents regarding clear definitions of terms relevant to sharing information, such as *minimum necessary*.

Solution: Clarify and standardize *minimum necessary* data sets by role of accessing party, use situation, or both.

Issue: Providers may have technical difficulties in applying the *minimum necessary* standard.

Solution: Design a more sophisticated and systematic means of providing access to the minimum information required in hospital information systems.

In addition to state-level solutions, 5 state teams requested federal guidance related to the Privacy Rule to reduce misunderstanding and promote common application. Two state teams suggested that the *minimum necessary* requirement be reviewed and that the US Department of Health and Human Services (HHS) should develop updated and more detailed guidance to clarify when and how the standard should be applied. The other 3 teams called for more general guidance regarding the Privacy Rule, including a compilation of frequently asked questions on the application of the Privacy Rule and additional explication of the extra protections afforded to psychotherapy notes (see Section 6 for additional discussion on requests for federal guidance). Other options for addressing variation related to the interpretation and application of the HIPAA Rules include educational programs, development of standard policies and protocols, and model documents.

Eighteen state teams proposed offering a training program to promote common understanding of the Privacy Rule overall and the *minimum necessary* standard specifically. The proposed programs varied in their intended audience, content, and scope. State teams recommended Privacy Rule training for providers and other office personnel, payers, consumers, law enforcement, public health officials, and first responders. These groups all require access to protected health information (PHI) but may not be fully aware of covered entities' responsibilities under the Privacy Rule, particularly those who need access to PHI relatively infrequently. Training for providers was designed to ensure that providers understood the relevant state law and Privacy Rule requirements. As one state team succinctly put it, "The purpose of provider education is to avoid unnecessary barriers to sharing personal health information over networks due to misunderstandings of the HIPAA Privacy and Security Rules and state privacy law."

Issue: Providers and office personnel do not have a clear understanding of what the HIPAA Rules and state law require, or vary in application of such requirements, resulting in broad variation that creates a barrier to electronic health information exchange.

Solution: Formulate a general, state-mandated HIPAA training course detailing what is required by the HIPAA Rules and other state laws.

Solution: Educate health care organizations about the inconsistent application of the HIPAA Rules and how that variation affects health information exchange.

Solution: Have the state health department issue policy guidance clarifying that personal health information may be shared in an HIE after a general release supplemented by notice giving patients ample opportunity to object to participation, where the HIE discloses only the health information to providers for the purpose of treatment.

Nine state teams recommended educational programs for consumers. If consumers are better educated about the value of information exchange and understand existing legal protections, they may be more likely to allow information to be exchanged electronically. Educating consumers offers an opportunity to increase support for electronic health information exchange and improve trust. Some state teams also felt that consumers did not have an adequate understanding of their rights and responsibilities in an electronic health information exchange environment, and proposed educating consumers on these points.

Issue: Consumers are unaware of legal protections.

Solution: Educate consumers regarding legal protections, rights, and responsibilities to increase trust in electronic health information exchange.

Finally, state teams proposed educational programs for law enforcement officials, public health officials, and first responders. Although the Privacy Rule allows disclosures without *consent* or *authorization* to these individuals under various circumstances, confusion still existed at the state level as to what disclosures were allowed, and under what circumstances. Both health care providers and potential recipients of personal health information may be confused as to what sharing is allowed. To address this, 4 state teams proposed providing training for law enforcement and public health officials.

Issue: Law enforcement officials, public health officials, and first responders often need to access personal health information. The circumstances under which they may access personal health information without *authorization* are not understood.

Solution: Offer training for law enforcement officials, public health officials, and first responders.

Solution: Enhance communication with other state agencies, such as the department of public health, that frequently require access to personal health information.

State teams also proposed drafting model documents or policies for the exchange of personal health information. Suggested model documents included business associate agreements (BAAs), notices of privacy practices (NPPs), and other nonspecified documents. Standardized documents may increase HIE participants' confidence that they are complying with the HIPAA Rules and relevant state law. Offering standard agreements may decrease the effort required to initiate exchange. Another source of variation is that persons may not understand if and when they should sign an agreement, particularly a BAA. Although this is outlined in the HIPAA Privacy Rule, confusion persists. Issuing guidance, or including this information on the model BAA, may help reduce this confusion. Standardized language or documents may reduce fear of liability, especially if they receive broad acceptance and are compliant. Since many different documents already exist, state teams may be able to analyze and standardize a boilerplate document that complies with relevant state and federal laws.

Issue: Exchange participants are not confident that forms comply with relevant state and federal law.

Solution: Provide model or standardized documents (9 states).

Issue: Exchange participants may not understand when a contract or other legal agreement is required.

Solution: Educate providers as to when an agreement is required (2 states).

States have introduced a variety of strategies for reducing variation stemming from differing interpretations and applications of the HIPAA Privacy Rule, ranging from educational program to standardized documents, to policy guidance and clarification of terms. See Section 5.2 for additional discussion on options for addressing variation stemming from state law and the intersection of state and federal law.

5.1.2 Uniform Consent

Uniform consent is another mechanism for reducing variation and was addressed in some form by 13 state teams.¹² State teams proposed 3 general designs for consent documents. States may choose a uniform consent form to be used by all entities within the state. A second option is to offer standardized consent forms that include certain elements, but may be modified based on institutional preferences. A third option is to provide model forms and allow institutions to draft their own forms. Payers or providers may be reluctant to exchange information if they are not confident in the standards and procedures maintained by others. Model consent forms may reduce these fears.

Issue: Consent forms and procedures vary.

Solution: Implement uniform, standardized, or model consent forms (13 states).

While all 3 design options may reduce liability concerns, each offers challenges. A uniform consent form, recommended by 3 state teams, may be politically unfeasible, as it requires consensus among a wide range of participants. Standardized consent forms were mentioned by 5 states, and model forms by 3 state teams. One team was still exploring the challenges and benefits of these 3 types of solutions. Standardized consent and model forms may be more feasible, although they must offer sufficient consistency if they are to improve HIE. In addition to offering forms, one state recommended providing consent criteria, which may be less controversial, but still offering exchange participants a greater degree of confidence. As noted above, many model documents exist, so states do not face the challenges of starting from scratch to develop model forms.

¹² The terms *consent* and *authorization* have specific meanings in the context of various state and federal laws. Although context must be considered when examining a specific statute, here the terms are used to generally mean a signed permission to release or disclose personal health information.

5.1.3 Policies to Govern Interstate Exchange

Several state teams have already initiated contact with neighboring states to examine the issue of interstate exchange. Outreach and collaboration efforts have begun in a variety of regions including New England, the Pacific Northwest, the Middle Atlantic, and Midwest. Although state teams frequently indicated a desire for national standards or policies for interstate exchange (see Section 6, National-Level Recommendations, for additional discussion), they recognize that federal standards may not be forthcoming and are pursuing state-level options. Concerns expressed by state teams include a lack of policies to govern interstate exchange, particularly in emergency situations, varying levels of protection and requirements, and different state-level patient identity management systems.

Issue: Lack of policies to govern interstate exchange.

Solution: Develop a task force to examine interstate exchange issues (2 states).

Solution: Establish compacts or memoranda of understanding with neighboring states for HIE purposes (2 states).

Issue: Lack of exchange policies for emergency situations.

Solution: Collaborate with neighboring states and territories to resolve cross-border issues.

Solution: Create a plan for addressing the sharing of patient health information between states in the event of a natural or manmade disaster resulting in patients being displaced.

Issue: State laws vary in levels of protection and requirements.

Solution: Attempt to harmonize laws across states.

Issue: States may develop different patient identity management systems.

Solution: Research and propose options on a system of patient identification that will allow speedy and convenient acquisition of information across jurisdictional lines.

The teams have had an opportunity to meet and discuss these issues, which resulted in collaborative efforts that will enhance interstate exchange.

5.2 Legal or Regulatory Issues

5.2.1 State Laws: Finding and Interpreting Them

Finding and interpreting state laws can pose a challenge. Law pertaining to privacy may be scattered throughout multiple chapters of a state's code, be inconsistent with other state and federal laws, or be overly vague. Similarly, case law is scattered and may also be inconsistent or contradictory. This situation can make it difficult for stakeholders to determine which laws apply to them and under what circumstances. State teams proposed 3 general solutions to enhance understanding: creating an advisory committee, consolidating state law, and aligning definitions in state law with those in the HIPAA Rules.

Issue: Stakeholders misunderstand state law.

Solution: Create an advisory committee to offer guidance on state law (8 state teams).

Issue: State law is scattered, inconsistent, or contradictory, impeding consistent interpretation and understanding.

Solution: Consolidate state code into a single chapter (5 state teams).

Solution: Develop a compendium of relevant state law, case law, federal law, and analysis.

Issue: Definitions in state law are not consistent with definitions in the HIPAA Rules.

Solution: Amend state law to mirror definitions in the HIPAA Rules (9 state teams).

5.2.2 State Law Governing Secure Exchange of Health Information

In many instances, state law governing the privacy of personal health information did not anticipate electronic exchange of information and, thus, does not sensibly apply to electronic health information exchange. Privacy laws may also not have anticipated other advances, such as genetic testing for certain diseases or changes in mental health treatment options, and definitions in existing statutes may be unclear. In either case, states have the option of amending or updating existing law, or drafting new law. The solutions immediately following were generally phrased but often included references to relevant state statute.

Issue: State law does not sensibly apply to electronic health information exchange.

Solution: Draft new state laws to govern electronic exchange (6 states).

Solution: Update existing state privacy laws to include electronic exchange (9 states).

In addition to the more general updates to state law mentioned above, the majority of states proposed amending state law more specifically. Possible amendments to state law or new legislation often dealt with the management of specially protected information or HIEs. Seven state teams proposed new laws related to specially protected information. Although definitions of specially protected information depend on state statute, they generally include HIV/AIDS information, mental health information, substance abuse treatment information, and genetic testing results. Three state teams sought to clarify the legal status of an HIE.

Issue: Specially protected information is inadequately defined.

Solution: Statutorily define specially protected information and create policies and procedures for how it is to be handled.

Issue: The legal structure for HIE authority and liability is not established.

Solution: Draft legislation to address the legal status of an HIE, including authority and liability.

Amending specific statutes will be easier to accomplish than drafting an entirely new set of privacy laws. State teams noted the prudence of this limited approach, explaining that it allowed for the most pressing problems to be remedied and limited the possibility that the changes will create more problems than they solve. Although state teams did not specifically address implementation in their final Assessment of Variation and Analysis of Solutions (AVAS) reports, 2 state teams mentioned drafting policy briefs to inform legislators and to begin to build support for this process.

Liability was another key issue that emerged in the AVAS reports. Payers and providers may be wary of electronic health information exchange if they feel it opens them to greater risk. Although there are liability concerns with paper documents, the chance of a large-scale breach is more likely in an electronic environment. Another perceived challenge posed by electronic records is the possibility that a patient's records would be aggregated, and that, absent a national patient identifier, the information in the record might not apply to the patient currently being treated. Electronic records may give patients more control over what information is disclosed (within the limits of technology). Some stakeholders voiced the concern that if patients are more selective in choosing to disclose information, physicians may not be able to provide the best treatment, which may also generate liability concerns if the patient is harmed as a result.

Nine state teams addressed the issue of liability by proposing new state laws. Limitations on liability were frequently tied to technical standards. That is, if a participant in a health information exchange complied with certain technology standards, liability would be limited (see Section 6.3 for additional discussions of technology standards). Legal professionals or patient advocacy groups may resist caps on damages or other limits. State teams will likely have to make a case that the benefits of improved exchange, such as improved quality of care, outweigh the disadvantages of those legal protections. One state also addressed the issue of who (the disclosing or receiving provider) is liable if inappropriate information is disclosed. Finally, one state team recommended that the HIPAA Rules include safe harbors (see Section 6, National-Level Recommendations, for additional discussion of national recommendations).

Issue: Providers are unwilling to participate in an HIE, because of liability concerns.

Solution: Draft state law limiting liability of exchange to participants meeting certain technical and policy standards (7 states).

Solution: Offer standardized agreements that conform to state and federal law (9 states).

Issue: Liability rests solely with the disclosing provider.

Solution: Amend state law so that either the disclosing or receiving provider may be liable, depending on each entity's conduct.

Enforcement was a final key issue in the state AVAS reports. As mentioned above, state privacy laws frequently did not anticipate electronic exchange of information; thus, no specific penalties deal with electronic health information exchange. The issue of enforcement is closely tied to liability, but also to consumer trust and education. Consumers are also more likely to trust a system where they know that those who disclose information inappropriately will be held accountable. In addition, consumers must be aware of their rights and responsibilities to seek redress. One state team planned to develop a dispute resolution process, anticipating the need for mediation and sanctions. Another 5 state teams mentioned the issue of enforcement.

Issue: State law does not sufficiently address the issue of enforcement.

Solution: Draft new state law to create new penalties and enforcement mechanisms for unauthorized disclosures (6 state teams).

5.2.3 Intersection of State and Federal Regulations (HIPAA Rules, 42 C.F.R. pt. 2, CLIA Rules)

The intersection of state and federal law offers significant challenges. The HIPAA Privacy Rule serves as a federal floor rather than a ceiling, for privacy protection, and many state laws are more protective than the Privacy Rule. In addition to the Privacy Rule, states must also comply with 42 C.F.R. pt. 2, which governs drug and alcohol abuse treatment records, Medicaid regulations, the Clinical Laboratory Improvement Amendments (CLIA), and the Family Educational Rights and Privacy Act (FERPA). These federal regulations are overseen by different agencies, a regulatory framework that requires the creation of crosswalks to explain where given provisions apply. Even finding and interpreting state law can be a challenge; layering on federal regulations makes legal analysis all the more complicated.

State teams generally recognized that changes to federal law were unlikely, although such changes may have been their preference (see Section 6, National-Level Recommendations, for recommendations of changes to federal law). Absent federal changes, states proposed alternative solutions to improve HIE. As discussed in the previous section, 9 state teams proposed aligning state law with the HIPAA Rules to make definitions consistent between state and federal law, thereby reducing ambiguities and improving the foundation for HIE. Additional issues presented by the state teams include the following:

Issue: Providers are unaware of all relevant state and federal law.

Solution: Create and maintain an index of state and federal law that applies to HIE privacy and security.

Issue: Preemption analysis may be out of date.

Solution: Update preemption analysis to include recent updates to state and federal law (3 states).

Title 42 C.F.R. pt. 2 also posed challenges for state teams and health information exchange: it governs drug and alcohol abuse treatment information and is intentionally restrictive; it was not designed to facilitate the flow of information, but to protect the privacy of individuals seeking substance abuse treatment. There are narrow exceptions as to when disclosure of information without consent is permissible, and treatment (outside of an emergency) is not among them. As discussed in Section 6, National-Level Recommendations, several state teams called for an amendment of 42 C.F.R. pt. 2, usually for allowing the release of information for treatment purposes without consent. States continue to struggle with this issue, attempting to balance privacy concerns and obstacles to HIE.

CLIA and FERPA were not widely addressed, although one state team developed possible amendments to CLIA to expand the list of permissible recipients of laboratory testing results. Another state team recommended aligning FERPA with other federal privacy laws (again, see Section 6 for additional discussion).

Issue: CLIA narrowly limits the individuals authorized to receive clinical laboratory test results directly from laboratories.

Solution: Amend CLIA to expand the list of permissible recipients.

Finally, state teams addressed the issue of Medicaid. Federal statutes and regulations require that disclosure or use of Medicaid data concerning applicants or recipients must be limited to “purposes directly concerned with administration of the plan.”¹³ Medicaid plan “administration” is narrowly defined and only includes determining eligibility and amount of assistance, providing services to recipients, and conducting or assisting with investigations, prosecutions, and civil and criminal proceedings related to administration.¹⁴ In addition, information concerning Medicaid applicants or recipients may be shared only with persons who are subject to standards of confidentiality that are comparable to the Medicaid confidentiality standards. These restrictions apply to all requests for information from outside sources, including other governmental bodies. These restrictions make it difficult for Medicaid and non-Medicaid providers to share information, and also inhibit sharing information between states’ Medicaid agencies and other state agencies.

New challenges arise when considering the possibility of changes to the Medicaid benefit package. One state team has secured an amendment to its state Medicaid plan that allows it to offer different benefit packages to recipients if they comply with certain responsibilities, such as routine screenings, medication compliance, and keeping scheduled appointments,

¹³ The federal regulations require that state Medicaid programs implement safeguards to protect Medicaid data. Thus, state standards actually restrict exchange, although federal statute and regulations mandate those standards.

¹⁴ The federal law can be found in the Social Security Act, 42 U.S.C. §§ 1396a(a)(7), 1902(a)(7). The regulations can be found in 42 C.F.R. § 431.300 *et seq.* The definition of plan administration is found in § 431.302.

detailed information that previously had not been reported to the plan. This amendment requires physicians to report whether patients are meeting those responsibilities. Although the privacy implications of these decisions have not been fully explored, the state believes that such reporting is directly concerned with administering the plan. In addition, other states may decide to similarly amend their Medicaid plans or seek other waivers under the Deficit Reduction Act (this does require approval from the Centers for Medicare & Medicaid Services). The state that has secured an amendment to its Medicaid plan is exploring the implications of the amendment and working to ensure that beneficiaries' information is appropriately protected.

Issues resulting from the intersection of state and federal law can be addressed at either level. The solutions described above apply to those that can be implemented at the state level, while federal recommendations are discussed in Section 6.

5.3 Technology and Standards

In the assessment of the variation process, state teams captured details about the confusion and misunderstanding among stakeholders concerning appropriate security practices. Stakeholders frequently misunderstood what standards and practices were technically available and scalable to the health care industry and consumers. This lack of knowledge, understanding, and trust among organizations and consumers was more evident in the business practices than in state laws. For the most part, state laws did not pose challenges to sound security, nor did the HIPAA Security Rule. Sometimes the matter was simply that, even though the Security Rule accommodates scalability in security programs, organizations voiced concern related to liability when one organization that believes its security program is more robust sends personal health information to another organization with a perceived less robust security program.

Confusion also exists regarding the different types of security required by the HIPAA Security Rule. The Security Rule addresses administrative, physical, and technical security. Even though more than one third of the rule addresses administrative security requirements, many organizations focused more on needed technology than on administrative safeguards.

Thirty-one of the 34 state teams offered solutions to the technology-related issues defined by the stakeholders throughout the course of the project. The level of specificity in the solutions presented by the state teams varied widely, from general statements that certain technological issues would need to be resolved to very specific and detailed discussions of how to resolve very specific issues. For example, one report provided 173 specific, detailed solutions covering 20 technical issues that were encountered while working to create the HIE program in the state. Another state team developed a set of 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in an HIE.

The principles were proposed to be specific enough to assist organizations in making decisions regarding electronic exchanges, yet flexible enough to adapt to a variety of network architectures for the exchange, evolving and new information technologies, updated national standards, and experiences gained by health care organizations with the implementation of an electronic exchange.

The variation in the level of specificity in the description of the recommendations generally reflects the level of technology adoption and use by the stakeholders within a given state and the level of advancement of HIE initiatives within the state. This makes it even more critical that the state teams continue to work collaboratively and share information. State teams reported that the primary issues include the need for broad agreement on standards for data security, quality and transmission, patient and provider identity management, and defining common data elements that need to be segments in electronic systems. At least seven states indicated that they would pursue proliferation of these standards through a centralized exchange (RHIO-type) model that would be responsible for determining and enforcing standards with the entities involved in the program. A number of states also noted that inclusion of the ability of systems to incorporate interaction with the patient should increasingly become an important consideration when defining the necessary technical elements of a system. The risk that states will develop their own, potentially incompatible standards, absent extensive coordination of these efforts, is real.

5.3.1 Data Security and Transmission

Data security appears at the forefront of almost every discussion about the technical issues concerning electronic health information exchange. Twenty-three state teams addressed issues related to one or more of the following domains: authorization, authentication, audits, and access controls. Some discussions were fairly general regarding the importance of developing or proliferating common security standards for the storage and transmission of health record data, while others outlined very specific solutions, indicating that they were prepared to move forward with some level of implementation.

This report does not support one standard over another; however, only 6 of the state subcontractor reports suggested modeling any of their data standards solutions on the work of such entities as the Health Information Technology Standards Panel (HITSP) or the Certification Commission for Healthcare Information Technology (CCHIT). The following summary captures the basic issues under data standards and solutions that have been proposed by the state teams. The following summary captures the fundamental issues under data standards, and solutions that have proposed under this contract.

Data Security

Authentication. Authentication is defined as the ability to verify that a person or entity seeking access to electronic health information is whom he or she claims to be. At least 19

states discussed authentication issues as an important component of ensuring data security. Maintaining a minimum standard for authentication between entities involved in an exchange was cited as a major factor in building trust between the entities participating in an HIE and to ensuring that records have the appropriate privacy and security safeguards within the receiving organization.

Issue: For organizations to feel comfortable transmitting information electronically to another organization, is important to trust that only appropriately identified users at the receiving location will have access to the private health record data being sent.

Solution: Require agreed-upon minimum requirements for a password system to allow access to health information.

Solution: Actively support initiatives that move the common standard between organizations toward biometric authentication for all network users. Although user ID and passwords are used most frequently to authenticate user access, biometrics provide authentication that is far less subject to misuse.

Solution: Designate an individual within each organization involved in an exchange program to serve as an end user or super user. This individual ensures that the authorization of individuals or entities transmitting or receiving health information electronically falls within the security guidelines agreed upon between entities. The super user is established through an authentication process following a site visit by the central HIE authority (such as a RHIO). Once the super user is established, that entity could authorize system access of others in that organization. The super user must maintain a credible system that prevents inappropriate access and allows local and consistent monitoring.

Solution: Encourage the ability for HIE systems to incorporate the use of telephone technology built into the system that would automatically call a designated representative of the user requesting information to verify the identity. Many users may be more comfortable with this option, as it does not entirely remove the human element from disclosure decisions; however, it does take steps toward automating the current process, and makes it more efficient. Also, the use of integration messaging technologies and fax forwarding services should be considered as components of the HIE telephony technology. The implementation would be similar to a transcription service.

Issue: Although standards for authentication exist, they have not achieved widespread consensus, and individual providers feel uncertain when transferring data from one system to another.

Solution: Undergo an effort to determine standards for authentication that can be shared between organizations seeking to transfer health information electronically. Individual solutions proposed by states include:

- Determine defined minimum standards for authentication that are acceptable to the individuals or entities participating in a given HIE program, and require that each organization meet those standards. An enforcement component should be

included as a way to assure all parties in the exchange that these standards are being followed.

- A standard exchange agreement could be formulated to encourage secure transfer between entities. The solution provided by the state suggests that this agreement should include requirements for unique digital user/entity/machine identifiers.
- Many states are not yet in a position to encourage widespread electronic health information exchange, usually because of the lack of EHR use within the population. These states need to make an effort to familiarize themselves with standards by researching the use of existing authentication protocols and services.

Authorization and Access Control. Information authorization and access controls allow access only to people or software programs that have been granted access rights to electronic health information. Consumers and those responsible for maintaining their data are concerned not only that the level of information shared among entities is appropriate, but also that the individuals receiving the information are appropriately authorized to view the data. Authorization solutions were usually included with discussions about role-based access, both of which are included below.

Issue: Many entities reported a sense of unease when sending data to another entity, because they had no way of knowing whether the information would be seen only by an appropriately authorized individual. Most stakeholders agreed that full access to all data contained in an electronic system should be restricted. It is not enough for users to be authenticated into a system; they must be assigned access that allows them to see only the information appropriate to their authorized position. The levels of access must be comparable between entities for a sending organization to feel comfortable that the receiving organization will manage the data in a manner all parties agree upon.

Solution: Require participants in an exchange to institute role-based access for any individual authorized to utilize the system. This requirement would assure other participants involved in the exchange that the data being transferred will be used appropriately.

- Separate users requiring access to clinical information from those that only need clerical access to the data.
- Develop and adopt a role-based, context-based, and information-based access control “rules engine” for health information, leveraging existing standards and integration profiles where possible. Identify and develop additional access control services and interfaces. These implementations may include, but are not limited to, Public Key Infrastructure (PKI) and Security Assertion Markup Language (SAML).

Issue: A variety of disclosures allowed under the HIPAA Privacy Rule for treatment, payment, and health care operations would require a guest user to have access to a system if the interaction were to be carried out electronically. Therefore, nonaffiliated providers (including payers) might require short-term or limited access to information in a system that they are not typically authorized to access.

Solution: Define parameters for temporary authorization of nonaffiliated providers, health plan representatives (payers), and others who might need access for allowable treatment, payment, and health care operations disclosures. Create a uniform system to allow payer access to minimal and necessary personal health information. Only those with proper and predetermined authorization are permitted to access appropriate portions of the file.

Issue: User roles and the health information authorized for use and exchange vary widely among entities. Entities are often uncomfortable with the idea that information provided only to a physician within their organization may be open for viewing and use by other clinicians or administrative staff in another organization.

Solution: Create a common set of role-based access levels for all users of a system. Common standards established for all entities participating in the exchange would be relevant for a wide range of organizations.

Solution: Create a centralized provider directory within the state. A centralized system or service could ensure all users have been given levels of access appropriate to their use of the system.

Solution: Authenticate and designate a site-specific role manager at each participating location. The role managers would be responsible for verifying the appropriate access level at their location.

Issue: Use of the National Provider Identifier (NPI) can be used as an authentication component, but the National Plan and Provider Enumeration System (NPPES) does not validate licensing or credentials. Although the NPI may identify an individual or organization as a provider, it does not accurately authenticate the entity or help to determine the access rights that entity should be given.

Solution: Local or state efforts must establish criteria for the credentialing and granting of access rights to HIE system users to ensure they have the proper licensing or other credentials for gaining access to the health information within the system.

- Require agreements among organizations that include credentialing, user registration, and authentication factors.
- Work with entities such as the health department, hospitals, and the Department of Insurance to propagate regulations establishing a set of minimum criteria for credentialing and granting access rights to HIE users; delegate an authority to audit on a periodic basis.
- Use ISO IS17090 Health Informatics PKI international standards to create profiles related to provider identification.

Issue: Although issues affecting electronic exchange within a state were the primary focus of this project, state teams were also encouraged to think about issues that would prevent interstate exchange. One such issue is that licensure classes across states are widely varied; therefore, it could prove difficult to engage multiple states in an exchange requiring role-based access if standards are based on state-specific licensing criteria.

Solution: A standard coding system across states, such as STEM E1986 Standard Guide for Information Access Privileges to Health Information, would better enable interoperability across state lines.

Audit. Information audits refer to system requirements that record and monitor the activity of health information systems. The ability to create and communicate audit trail events for privacy and security related to the communication of patient health identified information has long been identified as a core building block for HIE systems.¹⁵ Stakeholders from the states indicated that it was important to ensure all organizations were monitoring the access of data by users, as a safeguard against improper use or modification of personal health data.

At least 3 states mentioned the support staff needed to maintain, monitor, and analyze the complex and voluminous data captured if stringent audit requirements were imposed. Many smaller providers would require additional funding to secure that staff, which poses a significant barrier. Although minimum audit requirements are essential to ensuring the privacy and security of the data, decisions regarding the functions should be made in light of these practical considerations.

Issue: Many stakeholders related the difficulty of implementing adequate audit systems in their own EHRs and recognized the fact that auditing capabilities varied widely from organization to organization. The fear was that data would not be audited appropriately to ensure proper handling by the entities authorized to use it. To encourage sharing of EHR data, systems should require similar audit functions to ensure appropriate monitoring of access to data.

Solution: Establish auditing standards to ensure appropriate monitoring of access to data is comparable between entities involved in the same HIE system. Individual solutions include:

- Create guidelines for audit control and proactive monitoring (audit schedules, definition/ID/actions on inappropriate breaches), audit logs, record retention standards.
- Include documentation of time and date stamp and source for all read and write access to health information as a requirement under state regulations for all HIE.
- Audit requirements should include parameters for (1) audit event selection (what is audited); (2) audit data generation, storage and retention; (3) audit data review and analysis; (4) penalties for unauthorized access; and (5) provisions for consumer access to audit information.
- Require periodic audits and a standardized method of testing system hardness against breaches.
- Require audit capability of e-mail, which is currently not a widely accepted method of transferring health information because of the inherent possibility of security breach.

¹⁵ Appendix C: HITSP Common Building Blocks, June 2006 standards.

Issue: Many current EHR systems only keep audit information of the most recent access to the record and may not have the technical requirements or personnel necessary to support vigorous audit requirements.

Solution: Create cost-effective, efficient, automated proactive mechanisms for audit.

Transmission

Issues surrounding the standardization of transmission requirements crossed into the realm of legal and policy solutions. Ultimately, the technology exists to ensure private and secure transmission, but too often there is little or no communication among organizations to allow for electronic transmission. Therefore, 7 state teams offered specific technical suggestions to encourage electronic health information exchange.

Issue: A minimum set of rules and guidelines are necessary for secure transmission between two or more entities. Currently, these guidelines are individualized and highly variable because of the widespread ambiguity regarding standards stringent enough for secure transfer of patient health information. Also, many stakeholders related a feeling that the complexities involved in outlining such guidelines are prohibitive and discourage entities from pursuing electronic exchange agreements.

Solution: Begin developing standard policies for encryption and transmission of electronic data that can be utilized as a common ground or starting point for entities to begin exchanging health information. Individual solutions include:

- Mandate adoption of national standards for entities interested in pursuing electronic health information exchange with other entities within the state.
- Develop a single set of regulations governing the parameters for electronic health information exchange that harmonize with the any state-specific requirements.
- Utilize a coding system across the states, such as ASTM E1986 Standard Guide for Information Access Privileges to Health Information, for license classes would better enable interoperability.

Solution: Clarify rules governing the use of electronic signature.

Solution: Evaluate the policies concerning e-mail use between organizations.

Solution: Use PKI to access health data between entities.

Solution: Develop a secure web portal for health data exchange that can be utilized by any entity within the state interested in adopting the shared guidelines and security measures.

Issue: One option for exchanging information among physicians while the patient's record is active would be to provide messaging functionality within the facilities participating. This would include the technology necessary to transfer information from one system to another. This practice would allow physicians to request a consult and provide the consulting physician access to the patient's medical information. Currently, however, definitions for secure electronic messaging solutions to support provider-to-provider communication do not exist.

Solution: Create a consensus framework for a shared secured messaging platform, including technical and functional requirements.

- Require dual or multifactor authentication as the minimum for requests to transmit information. While there is additional effort and cost involved in installing and maintaining a dual factor system, the industry is quickly moving toward dual factor authentication as a best practice, and several viable, scalable and affordable technical solutions currently exist.

Issue: Without the development of a standard data set, entities will be responsible for determining which data elements should be included in every transfer, decreasing the efficiency an electronic transfer could provide over a paper-based transfer.

Solution: Develop a standard set of data elements for use for exchanges of information that take place when the patient is receiving services from a consulting physician.

- Encourage or require compliance with the continuity of care record standard.
- Include name of patient, previous conditions, allergies, and diagnosis in a standard set of data elements.

5.3.2 Patient Identity Management

The ability to accurately identify patients across systems is a major issue. Sixteen state teams discussed technical solutions, although, as with previous technical solutions provided in this report, the issue of patient identity management crosses over heavily into policy and legal discussions. For the most part, these state teams agreed that some system of identifying patients between entities must exist for true interoperability to occur, and that these systems must include stringent criteria for matching patients so that the confidentiality of patient records could be assured.

Solutions ranged from the use of a unique patient identifier to the establishment of a centralized patient identity management service. The solutions offered by many states called for a mix using more than one of these individual propositions.

Issue: When exchanging personal health data between entities, an HIE system must ensure that the appropriate records are matched to the appropriate individual.

Solution: Create standards for matching patients, using minimum and optional data elements. Individual solutions include:

- Establish biometrics as the preferred method of verifying the identity of patients. Using biometrics such as fingerprints, eye retinas and irises, facial patterns, and hand measurements may contribute to the security of health information because they are less prone to fraud than methods such as swipe cards. However, biometrics are also ineffective in some cases, especially with children and senior citizens, where fingerprints may not be clear or be altogether difficult to obtain. Another barrier is user resistance. Many patients do not like to have their fingerprint taken and saved for later recognition; this attitude may limit the large-scale adoption of these technologies.

- Create model policies and procedures to ensure appropriate capture of patient identifiers; adopt nationally defined standards for patient identification once available.
- Develop a master patient index with patient identification algorithms to facilitate accurate exchange of information.
- Use a number generated for each individual (such as a National Provider ID) or to use algorithms to uniquely identify individuals in the health information exchange.
- Require certified patient identification solutions as determined by Certification Commission for Health Information Technology (CCHIT) and supported by the assessment process determined by the state.

Solution: Pursue the use of a unique identifier for patient identification, either on the state or national level. Although this solution is currently prohibited by federal law, at least 2 states expressed the viewpoint that matching patients to their records could not happen with the level of accuracy needed (presumably 0% likelihood of either a false positive or false negative match) without a national patient identifier.

- Identify and use a unique identifier for patient identification for widespread Health Information Exchange, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier. A risk assessment of the use of any national unique identifier should be included.
- Assign a unique patient identifier at the state level to all residents to facilitate the identification of patients across health information systems. Initially, the pilot project that considered implementing a unique patient identifier assigned a 13-digit number to all potential participants in the public insurance plan, whether an application was approved or declined.

Solution: Still other states believed that patient identification could be managed but recommended establishing a centralized patient identity management service.

- Build a patient identity cross-referencing service into the RHIO or other central HIE entity. This solution would enable providers to use standards already supported by their health information system vendors and will enable sharing of patient information.
- Require all accrediting agencies to adopt a universal standard for patient identification, with official, verifiable means of both primary and secondary identification defined.

5.3.3 Segmenting Data

The management of health information deemed specially protected is another area with a complex set of drivers. Because these sets of specially protected information are often determined by state or federal law to require additional consent or other considerations when transmitting between entities, many providers prefer not to exchange them at all. In fact, while 17 states included a discussion on specially protected health information in their solutions reports, only 6 discussed technical solutions for integrating this data into HIE systems. For these states, the answer was usually to segment the data in the systems. However, this solution requires extensive planning, programming and could potentially

increase the workflow burden on the provider. While segmenting specially protected information in an electronic system is likely the only way to enable transmission in many situations from one entity to another, the complexity it adds to these systems can be prohibitive.

Many states in the later stages of planning, implementing, or expanding local or regional data exchange programs have considered the need to include technical specifications ensuring that all specially protected information is collected, stored, and exchanged in accordance with state and federal law. They must also consider policies that participating organizations are comfortable with when they enter into an exchange with other entities.

Issue: To ensure it is not included in standard data transfer, specially protected information requires additional technical considerations in HIE systems, such as the ability to “mark” a piece of data as protected, and the ability to specify the conditions under which the data can be transferred. This capability currently does not exist.

Solution: Because of the increased consent requirements in many states, specially protected information would require additional and sometimes item specific opt-in/opt-out procedures for patients and methods for capturing and transmitting that information within and between systems.

Solution: Specially protected information requires some additional technical considerations for increased control of access to data. Individual solutions include:

- Use filters to suppress access of data to end users.
- Increase layers of security and flag specially protected information.
- Remove specially protected information from electronic transfers of health information, but implement a functional requirement to notify end users that some specially protected information has been blocked.

Solution: Create functional requirements for suppressing specially protected information concurrently with creation of consensus policies.

Solution: For the very few states that do not have stringent legal requirements on the transfer of specially protected information, establish parameters to ensure that all health information is treated with the same privacy and security standards, including regular and specially protected health information.

5.3.4 Standards That Affect Technology

HIE Agreements

Seven states noted that the standardization of HIE agreements, such as business associate agreements (BAAs) and other data use agreements that enable the sharing of data between

entities, would be extremely beneficial.¹⁶ While the construction of model or standardized agreements is largely an issue of creating consensus around policies, these policies must include specific indications of technological minimum requirements. BAAs define standards for data confidentiality and integrity during end-to-end electronic exchanges and also outline parameters for the interoperable mechanisms used to uniquely identify patients and health care providers between systems.

Consent

While the majority of states discussed consent as a policy issue, 6 state teams also examined the technological implications of consent. Typically consent is paper based, but as electronic health information exchange becomes more widespread, consent will likely need to be noted within the electronic record, especially in cases of specially protected information (as discussed earlier in this section). Consent is also closely tied to other issues discussed at the beginning of this section, namely authorization and access control. If appropriate disclosure within an electronic system is driven by a user's authority and level of access within that system (especially if the access is role based), issues of consent become more important. The ability to capture consent uniformly within an electronic system also enables the transmission of that information between entities.

At least 6 states noted the importance of establishing uniform consent policies across a RHIO for those exchanges to be successful. None of the states involved in this project reported having a functional system with for the technical capacity to capture, share, and implement patient consent. At least one state mentioned that this was due almost entirely to current technical restrictions. However, eventually, electronic systems will not only need to capture patient consent, but also to record and implement changes in consent over time and with changes in the patient's medical and clinical conditions.

Patient-Centered Health Information Exchange

Many states noted the importance of involving the individual patient in more profound ways. In recent years, considerations of the value of a health data exchange that puts the consumer/patient at the center of the exchange process have emerged as private and public activities. Therefore, at least 3 states are considering systems that would allow the patient to direct where and how much of their health record data is sent. In one proposed model, when a request for data occurs, the provider of the data would send it to a person-controlled software agent. The agent, as configured by the person who is the subject of the

¹⁶ As noted earlier in the report, none of the states distinguished *business associate agreement* from the more specific term *business associate contract*. The Health Insurance Portability and Accountability Act (HIPAA) Rules require covered entities to document they have obtained satisfactory assurance that their business associate will safeguard health information through a written contract or other written agreement or arrangement. The Rules have specific provisions for business associate contracts and other arrangements. The other arrangements category includes, for example, memos of understanding between agencies. Here, the term HIE agreement is used as a means to encompass all forms of arrangement between entities.

data, permits and completes appropriate exchanges and rejects others. This approach draws the patient into the health care process, eases the creation of personal health records and their associated applications, permits individual flexibility related to privacy, and returns the issue of who is included in the information flow related to a patient's care back to a dialogue between the patient and his or her health care provider(s).

This particular model would address many of the current concerns regarding electronic health information exchange, although for many groups, it raises other issues that are just as complex. Individual consumer involvement at the center of the health care information exchange may result in an enhanced awareness of privacy and security issues across the general population. However, what happens if a patient blocks access to data that could potentially save his or her life? What is the best way to reach patients who do not have access to computers or do not understand the complex issues involved in making these decisions?

Although these questions should remain important counterpoints for consideration, models exist for creating such consumer-oriented programs, such as the guidelines for personal health records described by the Markle Foundation's Connecting for Health report, and person-centered RHIOs such as the Louisville Health Information Exchange (LOUHIE). Regardless of consumers' level of control of the exchange of their health record data, their needs must be seriously considered when determining the technical requirements of HIE systems.

5.4 Education

Twenty-nine state teams recommended some form of education program(s) to increase the knowledge within stakeholder groups ranging from providers to the general public. The majority of these education-based solutions are proposed to reduce variation in how policies are put into practice or to increase general awareness of various stakeholder groups regarding the advances and trends in electronic HIE. These discussions of education-based solutions were commonly directed at consumers and providers, although the formula for achieving this outreach tended to vary widely. Some state teams proposed creating educational materials to be used by both groups, although most state teams proposed separate programs tailored to each group. Also, a significant number of states included educational programs as fundamental components of an HIE regulatory body, whether that body currently exists, or is in the planning stages.

The majority of the state teams recommended informational campaigns as a method to educate consumers. The plans for developing education for individual providers and organizations typically followed a more institutionalized method, such as training requirements for users of HIE systems. While specific solutions contain some variation depending on the state's unique context and environment, the underlying assumption was

almost always the same: if the solutions proposed in these reports are to be successfully implemented, consumers, providers, and organizations need to be educated on the advantages of electronic HIE and fully aware of the privacy and security safeguards that are being established to protect health information.

5.4.1 Consumer Education

As mentioned above, a majority of states highlighted the need for consumers to be educated about their rights as well as how to work with providers to understand who can access their information and how it can be done.

The consumer-focused solutions discussed in detail below can be summarized in the following major groups:

- general communication to the public regarding electronic health information exchange opportunities;
- education regarding privacy issues, including data security safeguards;
- knowledge necessary for consumers to engage in their health care, including the use and maintenance for a personal health record; and
- mechanisms to collect continuous or frequent consumer input.

A major issue that these solutions confront is the wide variation in knowledge of privacy and security issues among consumers, not only underlying the electronic exchange of their personal health information, but also a fundamental lack of understanding about their health information rights and responsibilities. In such an environment, it is difficult to begin a discussion about the benefits of electronic health information exchange.

Misunderstandings and mistrust about the current paper-based privacy and security protocols for storage and exchange of health information creates a general hesitancy toward authorizing such exchanges. In a wider, patient-centric lens, this also profoundly limits patients' ability to maintain and monitor their health information. Patients' ability to review their own health records would often be the first line against privacy and security breaches. Individual solutions provided below address the issue of general public misunderstanding.

Issue: Patients lack knowledge about their rights, which leads to trust issues, although patient trust will be critical to the success of electronic health information exchange.

Solution: Implement a campaign to educate the public about privacy and security issues and electronic health information exchange. Individual solutions include:

- Leverage existing consumer education venues, such as doctor's offices, clinics, and established websites to deliver educational content.
- Host information sessions statewide to inform stakeholders about electronic health information exchange.
- Create "learning communities" that bring together multiple stakeholders to participate in public listening exercises.

- Create an education package based on the laws and regulations that deal with patient consent. Any educational materials should contain accurate information in language accessible in layman’s terms, about electronic health records, rules governing disclosure of patient data, risks associated with paper charts, and the positive aspects of electronic health information.
- Educate patients and consumers concerning federal and state privacy laws at both the national and state level. Include an explanation of the conditions in which their individually identifiable health information can be disclosed without their permission.
- Develop lists of frequently asked questions (FAQs) or recommendations regarding how consumers may ensure the maximum privacy of information, while obtaining needed care as efficiently as possible.

Solution: Establish a centralized method to develop and distribute educational materials concerning patient rights and responsibilities and enable them to protect and monitor their health care information.

- Create privacy and security speakers’ bureau.
- Create online tools (website, blog, education, resource portal) to encourage patient interaction and provide a resource to answer questions about electronic health information exchange.
- Educate state legislators about the current HIE environment.
- Encourage RHIOs and other local exchange programs to develop materials that raise awareness of electronic health information exchange.
- Develop a participation permission form based upon the Markle Foundation Connecting Health Principles that incorporates the plain-language privacy and security practice descriptions and test form with consumers to assess understandability of language and concept.
- Take advantage of opportunities to educate patients at the point of care on major issues such as *consent* and *authorization*.

Issue: Patients may be unaware of the privacy and security safeguards available in an HIE system or may not have the technical knowledge to adequately monitor their data or make informed decisions leading to frustration and confusion.

Solution: Create standardized educational materials for patients to ensure they understand the technology as well as their ability to interact with it.

- Provide documentation on the limits of information use in a RHIO for patients whose data will be included in an HIE.
- Provide sufficient education materials for patients to inform their choices in an opt-in or opt-out system.
- Educate patients on how, when and why to control access to their information as well as understand the circumstances under which the data will be transferred.
- Encourage patients and physicians to participate together in a personal health record service via the Internet.
- Provide information on baseline expectations for network level security (e.g., secure sockets layer) and how transmission level security follows HIPAA Security

Rule provisions, where applicable, during an internal HIE or external HIE (or both).

Issue: Consensus among stakeholders can be difficult to find, and the attitude of the general public is likely to change and shift during this transition period.

Solution: Implement a process for collecting information from consumers to monitor progress and ensure satisfaction with electronic health information exchange decisions.

- Conduct polls and focus groups to determine consumer knowledge about the realities of HIE, privacy and security; their expectations of participating entities and government; as well as understanding of their rights, and their obligations.
- Conduct a consumer needs assessment to see what consumers most want from an EHR/HIE environment; focus on providing these functionalities to encourage public acceptance.
- Suggest that administrative/oversight entities engage consumer participation in HIE administration and oversight activities and decisions.

5.4.2 Provider Education

While consumer education is a major concern, many states reported misunderstanding of the capabilities and benefits of electronic health information exchange, as well as fears regarding data security within the provider community. Solutions requiring provider education included:

- Educate providers on state and federal privacy and security laws and regulations to increase their comfort with electronic health information exchange.
- Educate providers on the types and benefits of HIE systems available to them.
- Provide continuing education for all professional health care staff in an organization that uses an HIE system to ensure proper privacy and security procedures are followed.

These solutions highlight a few key issues. For instance, adoption rates for HIE systems continue to be quite low in most areas of the country, making it difficult in some very low adoption areas to encourage robust discussions on interoperability. Startup costs could be part of the problem, but as a number of states pointed out, a significant barrier to adoption is lack of provider trust and education about the systems themselves. Increasing awareness about certification, standards, and the advancements in capabilities of systems to increase private and secure transmission of data could lead to higher adoption of EHRs and, therefore, increased discussions about interoperability.

Issue: Many health care professionals do not accurately or completely understand the HIPAA Rules or relevant state privacy laws.

Solution: Provide education for health care providers about state and federal privacy and security laws and regulations, specifically in reference to electronic health information exchange.

- Establish a committee to develop and recommend education curriculum and an implementation process to improve the medical industry’s knowledge of the requirements of the HIPAA Privacy and Security Rules.
- Provide an education package based on the legal requirements, the technical standards and the policies and procedures for access control, and all other security policies and procedures developed in the community standards.
- Provide a hotline for call-in questions about state and federal laws and regulations governing the exchange of private and secure health information available to all stakeholders, including providers.
- Set up a website posting information regarding privacy and security issues; produce an FAQ brochure that could be posted and distributed.
- Provide training on privacy and security laws for health care professionals, administrators and the public to promote a better understanding of the “break the glass” principle, which allows an authorized professional to have access to previously unauthorized information, after verifying emergent need for the additional information.
- Develop a core competencies guide for appropriate staff (key support staff, office managers) within an organization to include privacy and security training and awareness of the technical issues relevant to their job responsibilities and electronic health information.
- Produce educational materials that explain the laws specific to that state regarding specially protected health information and under what circumstances it can be transferred. Including discussions of the interaction between specially protected information and electronic storage and transfer of the data would also be an important component.

Issue: Within the health care provider community, states found a lack of knowledge about the capabilities of HIE programs. Many did not believe that the expense was worth the risk of buying a system that might significantly hinder their workflow or require complete retraining of the staff to use the system.

Solution: Implement a campaign to educate providers about HIE opportunities available to them.

- Encourage, through education and financial incentives, the purchase of EHR systems that are CCHIT-certified.
- Provide education and training for providers about proper procedures, the need for standardization, and the benefits of HIE and local initiatives.
- Focus efforts on provider groups that have the most difficulty with buy-in so that those groups can be targeted for communications/education efforts.
- Promote awareness of data exchange programs that have been successful in adequately protecting privacy and security.
- Create a solution that includes basic elements for every vendor’s product. Physicians and personnel in hospitals and health plans will be educated and encouraged to demand that any software they purchase meet these basic functional needs. This solution is especially useful for small covered entities.

Issue: State teams uncovered a significant lack of knowledge within the health care provider community on how to adequately ensure protection of privacy and security when implementing electronic health information exchange. Many providers believe electronic transfer of records is too risky, either because they are unaware of how the HIPAA Privacy and Security Rules apply to electronic transfer, or because they are afraid a security breach will create negative publicity that will affect the trust of their patients.

Solution: Provide education and training for providers regarding proper procedures, the need for standardization, and benefits of HIE.

- Establish core competencies for staff education, to include not only privacy and security training, but also awareness of the technical issues relevant to their job responsibilities and electronic health information exchange.
- Implement an education, training, and possibly a certification program to help small covered entities secure their computer networks.
- Create a collaboration among trade groups, universities, and community colleges to provide IT distance learning opportunities for health care providers in all areas of the state.

5.4.3 Integrated Education

Many states discussed education as a fundamental and ongoing issue that required consistent structure and funding. At least 18 states proposed harnessing either proposed or existing entities to provide or oversee some aspect of the required educational activities within the state as part of their mandate.

Issue: The need for education to all stakeholders will be ongoing, although funding sources and consistency of these efforts is often lacking.

Solution: Integrate education efforts as part of existing efforts, such as:

- Charging the entity responsible for overseeing HIE within the state (RHIO, for example) with developing and maintaining current educational materials for both the participating clinicians, and the individual patients involved in the exchange.
- Create a collaborative effort among trade groups, universities, and community colleges to provide IT distance-learning opportunities for health care providers in all areas of the state. This collaborative would also develop IT scholarships for students in all areas of the state.
- Encourage the health department and Privacy and Security Advisory Board to work together to develop public awareness campaigns, in coordination with consumer advocacy groups, to educate consumers on the benefits and risks of electronic health information, and to engage consumers to take a more active role in managing their own health.
- Develop and recommend a structure, purpose, membership, and activities for a committee of health care industry stakeholders from the public and private sectors. The committee shall identify opportunities to educate health care industry stakeholders and patients on privacy and security provisions and the benefits and detriments of HIE.

- Require inclusion of a privacy and security component in the continuing education required of physicians.

5.4.4 Education Targeted to Specific Groups

Although education of health care providers and the general public dominated the educational solutions, some important education-based solutions were proposed for special groups of stakeholders. Special considerations needed for these groups were often uncovered in the assessment of variations process when it became apparent that a general disconnect existed between certain stakeholder groups that are either often forgotten in discussions involving electronic health information exchange, or groups that have particular interest in an aspect of electronic health information exchange that may be more controversial. Targeting these groups focuses on solutions that will help decrease variation in business practices across all involved entities affected by electronic health information exchange.

Issue: Certain stakeholder groups might require focused attention to ensure that their unique perspective is reflected in electronic health information exchange decisions.

Solution: Create targeted education and outreach materials to these groups.

- Conduct joint training events for law enforcement and public health at annual conferences and seminars sponsored by local and state public health departments.
- Offer targeted training/educational program for law enforcement and public officials (including judges) to explain HIPAA Privacy Rule requirements.
- Work with health management organizations and employer groups to educate them on the benefits of the use of data for research purposes.

5.5 Implementation and Governance of Privacy and Security Solutions

5.5.1 General Implementation and Governance Issues

Twenty-two states identified solutions that involved implementation and governance issues. Implementation and governance policies usually varied according to the degree of electronic health information exchange within the state. States with limited electronic health information exchange penetration were more likely to propose governance structures that would consider basic technical issues, such as those discussed in Section 4.3. In states that were more advanced, proposed governance structures were predicated on the assumption that the technical considerations were already addressed. Eight states proposed forming a committee or some other centralized authority to address implementation and governance.

Issue: Both advanced and early-stage states indicated a lack of coordination within the state on issues of ensuring privacy and security that would encourage interoperability within the provider community.

Solution: Institute a centralized authority to coordinate these efforts along with any other HIT efforts in the state. This would provide a means to ensure consistent, long-term input as the transition between a paper-based and electronic health care system continues to take place. Some examples of authority/committee duties include:

- Recommend standard privacy and security policies, procedures, and technology controls.
- Explore and possibly recommend legal solutions.
- Integrate and link state e-Health information with existing websites to provide updates on state activities.
- Reach consensus regarding rights and responsibilities with respect to health information privacy and security.
- Develop rules for HIE in the event of a bioterror attack or other disaster.
- Draft a strategic plan for HIE and health information technology (HIT) adoption.
- Support education for providers, payers, and consumers.
- Review interpretation, compliance, and practice with respect to state and federal law.
- Devise quality assurance protocols.
- Establish a statewide public/private HIE Privacy and Security Advisory Board to oversee and facilitate aspects of privacy and security for statewide HIE: identify the proper public and private Advisory Board members and chairpersons to represent both the health care industry and the state; establish consensus and develop a charter defining the scope of governance, authority, roles, and responsibilities; oversee the various committees that report to the Advisory Board and review the products these committees produce.

Solution: For states that have more complex legal issues, require any proposed authority/committee to interact with the state legislature.

- Convene a statewide consortia comprised of representatives from each community exchange to foster and ensure consistency of approach to protecting privacy and security across the state.
- Provide recommendations to state legislators and policy makers through analysis, briefings and testimony.
- Provide coordination for government programs that interface with the private sector.
- Work with the governor’s office to draft and pass legislation.

Solution: 10 states identified multiple ways in which increased coordination among those involved with electronic health information exchange (providers, payers, technology providers, clinicians, etc.) could enhance the adoption of electronic health information exchange and provide increased privacy and security safeguards. Examples of proposed coordination tasks/solutions are:

- Organize stakeholders to create a statewide resource center

- Determine best practices for identifier assignment mechanisms for nationwide health information exchange. Provide guidance to state consumers, providers, payers, through workshops and web-based resources.
- Establish an HIE Commission, or use an existing independent statewide entity, to continue to engage in rigorous dialogue regarding patient control issues and any associated system mechanisms, and to develop related policies and standards.
- Create a collaborative effort among trade groups, universities and community colleges to provide IT distance-learning opportunities for health care providers in all areas of the state. This collaborative would also develop IT scholarships for students in all areas of the state.

Solution: 4 states suggested the use of contractual agreements (exclusive of BAAs) as another solution to governance issues. (BAAs were mentioned by 11 states, although not generally in the context of improving governance or implementation.)

In addition, many states discussed factors that would be included when and if they moved toward implementing solutions. Although some might be obvious goals of a governance body, they begin to inform a framework, built on some of the lessons learned during the project, around which the direction of these bodies could be built. Factors to consider when implementing a governance body include:

- Consider a pilot project to determine best practices for other HIEs in the state.
- Leverage existing electronic infrastructure.
- Encourage use of common security and privacy procedures.
- Request that state health departments develop operating rules and procedures.
- Legislate targets for implementation/compliance (i.e., by a given fiscal year).
- Provide guidelines and assistance for small provider groups.
- Enhance communication with Native American Nations to facilitate HIE.
- Standardize policies for varying degrees of physical and technical security required.
- Use secure web portals for information exchange.

5.5.2 Governance and Implementation of HIEs

Although a number of states have some form of HIE projects in place, the legal status under the HIPAA Rules and state law of certain entities that participate in HIEs is often unclear. Several states reported that they were working to form an HIE, while others were reluctant to do so absent clarification on this issue. Despite this uncertainty, many states have functioning exchanges and have developed a variety of solutions for the governance of existing exchanges including:

- Publish a policy and procedure manual for HIE online (2 states).
- Establish HIE-wide information exchange policies and BAAs.

- Create a post office within the HIE for the cross-referencing of patient identifiers.
- Leverage the HIEs' expertise to improve infrastructure in other markets in the state.
- Provide educational seminars.
- Accredite HIEs.
- Form a statewide collaborative to serve as a resource and communications nexus for HIEs within the state.
- Develop guidance to help determine whether an entity participating in an HIE is a HIPAA covered entity.
- Require regular updates of list of authorized users.
- Establish manual or secondary flow business processes in the event of technical problems.
- Publish aggregate results of audits.

States that were interested in forming an HIE, but had not yet done so, offered the following solutions:

- Draft legislation to authorize HIE roles, sanctions, and functionality.
- Consult with other states to determine best practices.
- Request legal clarification.

5.6 Ancillary Issues and Solutions

5.6.1 Funding

Solutions related to funding fall into two broad areas: sources of support and methods for demonstrating the need or merit for funding. States generally suggested a combination of funding sources including government appropriations, grants, and user fees. Alternatively, 4 states indicated that they would attempt fundraising efforts, and 3 other states planned to seek discounts or donations from technology vendors. To demonstrate the merit of funding HIT initiatives, 4 states have planned a cost-justification or cost-benefit analysis. Finally, one state is planning a statewide collaborative effort to reduce the overhead costs of installing components of HIT infrastructure.

Although some states identified strategies for financing HIT initiatives, they did not usually match with the states proposing new legislation and regulations. Only one state noted the need to include funding provisions in order to avoid unfunded mandates.

5.6.2 Incentives/EHR Adoption Issues

Financial incentives are an obvious solution to EHR adoption issues. Small providers, those located in rural or low-income areas, or providers with a large percentage of underinsured or uninsured patients may have financial difficulty in purchasing and implementing EHR. The

states proposed of the following incentives designed to facilitate EHR and HIT more generally:

- tax incentives for providers (3 states),
- unspecified incentives (3 states),
- combination of public and private incentives, and incentives for organizations that implement best practices for privacy and security.

States also suggested nonfinancial methods for encouraging EHR adoption. Seven states proposed general advocacy of EHR, including education (see Section 4.4 for additional information on educational programs). Finally, one state planned a mentoring program for providers who were implementing EHR.

5.6.3 Stakeholder Engagement

Several states noted that stakeholder engagement was crucial to the success of the proposed solutions. Stakeholder engagement was cast as a method to understand consumer and provider wants and needs, and also as a method to educate stakeholders about existing efforts and their potential participation in those efforts. Stakeholder engagement solutions were aimed at consumers, providers, payers, or some combination. Six states planned consumer-specific engagement programs. These included:

- holding community forums;
- assessing consumer needs (determining what consumers want most from the HIE environment);
- determining consumer perceptions and understanding of specially protected clinical data to see if it aligns with state and federal law; and
- strengthening the communication channels between the state, Indian Health Service, and sovereign Native American tribes.

Four states described a more comprehensive approach that would target consumers, providers, and payers in the same initiative. In the majority of cases, stakeholder engagement included educational programs. One state noted the need for outreach to consumers who do not have access to a computer or who otherwise may not have a voice in the stakeholder process, such as individuals who do not speak English as their first language.

6. NATIONAL-LEVEL RECOMMENDATIONS

Throughout this project, the state project teams focused primarily on generating potential solutions that could be implemented at the local or state level to develop privacy policy and security standards that enable electronic health information exchange nationwide. However, state teams also recommended solutions at the federal level that would be highly valuable to states as they develop their privacy policy and security standards.

Many of the ideas summarized in this section were also raised by state teams as potential solutions to be implemented at the state level. The state teams that chose to offer national-level recommendations generally indicated that privacy policy and security standards for electronic health information exchange could achieve faster uptake if adopted at the national level rather than trying to come to agreement nationwide at the state level. The following recommendations represent the contributions of all 34 state project teams.

6.1 National Standards

6.1.1 National Standards for Transferring Health Information Among States

State teams most frequently called for national standards that would collectively guide the transfer of patient health information between states. Although most of the states have made significant strides under this project in moving toward data standards that work for the context of their state, they were concerned that, without a centralized effort, states might go in disparate directions or that the effort would take far longer to coordinate. Nineteen states included some discussion about national-level standards that would ensure transfer could be attained from state to state. These states were interested in standardizing both a basic set of data elements to be included and accompanying data standards for the interstate transfer of personal health information. Both major areas are broken out below, providing some of the specific state recommendations.

Standard Set of Data Elements

States could begin developing initial exchange programs if they were provided a basic list of health information to be included in a patient health summary or standardized medical record (excluding specially protected health information), such as normalized clinical patient demographics, eligibility data, allergy list, prescription list, laboratory and radiology (text and image) results, and potential immunization records. One state team suggested the use of the continuity of care record standard as the first adoption target. Another state team suggested the use of standard reports, such as the Reports of Verified Cases of Tuberculosis, as model standards.

Technical Security Standards

A frequent suggestion included establishing national guidelines and adopting standards for the implementation of authentication, authorization, access controls, and auditing for adoption by state and regional health information exchanges (HIEs). The significant variability and lack of standard methods, practices, and policies (sometime even within an organization) on each of these 4 security domains were cited in all states as major barriers to HIE. Some specific national-level recommendations included:

- Establish minimum criteria to authenticate and verify the identity of users in an HIE that can be consistently used across states and regions. Five states suggested re-opening the discussion regarding a national patient identifier, feeling that this was perhaps the most efficient possibility enabling cross-state patient identification. They believe that, in addition to establishing the proper identity of the patient, this identifier would also enable the appropriate controls to access defined sets of health information.
- Define the minimum requirement for user authorization to access, use, and disclose health information within the context of a state or regional HIE.
- Identify and adopt guidelines and provide best practices to address access control issues within a state or regional HIE.
- Establish minimum requirements for routine auditing of access to health information through a state or regional HIE.
- Address the use of specific methods and technologies, such as biometrics, digital signatures, and encryption.

All states expressed an interest in sharing data across state lines; however, many were concerned that expecting each state to broker the set of health information to be shared and establishing the methods by which this would happen would lead to a fragmented and disjointed system. States also noted that while technical solutions can be designed and implemented at local and regional levels, the choices made for each of these systems might be so different that they would be unable to find ways to interoperate. Use of different data elements to accurately locate a patient or to segment specially protected information could cause costly and time-consuming interoperability issues. National standards and guidelines would provide states with a platform to begin exchange discussions, which they could alter if necessary, but maintain a similar core of information from state to state.

6.1.2 National Standard for Health Information Exchange-Related Business Associate Agreements¹⁷

Similar arguments were proposed for the development and publication of a national standard for data sharing agreements, such as a business associate agreement (BAA).¹⁸ Eight state teams proposed that a standard BAA be established at the national level, even though a national standard for BAAs and data use agreements is included in the HIPAA Privacy Rule. These state teams pointed to BAAs as potential catalysts for encouraging electronic health information exchange. The state teams also emphasized the increased burden that would come from creating a BAA from scratch for every type of exchange. Therefore, they called for a national standard or template to encourage the discussion of data sharing among entities. None of the states mentioned using national standard templates such as those that have been developed by American Medical Association, the American Hospital Association, or the Blue Cross Blue Shield Association.

6.1.3 Standardized Model National Consent Form

Five state teams called for a standardized model national consent form or template that would guide the large number of providers who reported confusion about consent requirements, or continued to worry about liability concerns with transferring information without proper consent. The state teams making this recommendation indicated that a uniform or model consent form is an essential component to encourage data sharing among organizations and across states. Many state teams have proposed solutions to develop statewide uniform consent models. State teams recommending a model national consent form recognize that each state must be concerned with the unique laws that might affect their consent process, but also that using a common template decreased the likelihood that the consent process in one state is fundamentally incompatible with the consent process in another state.

One suggestion concerning the items that should be considered for such a form included: general consent requirements; consent principles relative to condition-specific consent requirements; interstate information exchange; information exchange with payers and

¹⁷ Five of the 8 states making this recommendation referred specifically to a national standardized business associate agreement, and 3 state teams referred to contractual or participant agreements. None of the states used the more specific term *business associate contract*. The HIPAA Rules require covered entities to document they have obtained satisfactory assurance that their business associate will safeguard health information through a written contract or other written agreement or arrangement. The Rules have specific provisions for business associate contracts and other arrangements. The other arrangements category includes, for example, memos of understanding between agencies. Thus, the term *business associate agreement* encompasses both contracts and other arrangements so this term is used in the summary above.

¹⁸ These types of agreements are common and required by the HIPAA Privacy and the Security Rules. BAAs are executed whenever a third party performs for a covered entity certain services that include access to PHI. For example, organizations receiving PHI and serving as a platform for many regional or local data exchange systems on behalf of covered entities would be a business associate of all covered entities that use the organization's services.

employers; use of information for marketing; compliance with the HIPAA Rules, 42 C.F.R. pt. 2, and other statutes that are relatively common across states (e.g., those that protect mental health, HIV/AIDS, minors, genetics data); and waivers of consent when the patient's life is at risk and in public health emergencies.

6.1.4 Centralized Model Regulation Process

To develop a centralized model regulation development process, 4 state teams suggested a range of options: a national effort to provide structured guidance to the current national standard setting bodies, a centralized national process to examine the role of emerging standard setting organizations, and working with the National Conference of Commissioners on Uniform State Laws (NCCUSL) to broker a set of model legislation. Although many of these solutions would require significant input from the states, all states proposing this recommendation felt that some federal oversight was needed to ensure that resources were provided to pursue the production of model standards or model legislation.

6.1.5 National Oversight Body

Three state teams proposed that an organized authority or oversight body guide the standardization of privacy and security implementations among states. Although all 3 states provided different alternatives, the overwhelming sentiment was that such efforts could accelerate the adoption of recognized model laws, contracts, policies, and procedures among HIE entities. One state team also recommended that the national oversight body oversee a consistent national educational campaign to consumers that will lead to greater public understanding and HIE participation.

At least 6 other states indicated that the state governing bodies that oversee privacy and security operations for HIE should try to follow or adopt any federal standards or guidance. Other states pointed to existing bodies as possible entities for oversight and guidance.

6.2 Clarifications/Revisions to Federal Regulations

The second most frequent set of issues raised by the state teams that offered national-level recommendations included recommended revisions and clarifications to federal regulations, including the HIPAA Rules, 42 C.F.R. pt. 2, Clinical Laboratory Improvement Amendments (CLIA), and Medicaid data disclosure regulations.

6.2.1 HIPAA Privacy Rule Revisions/Clarifications

Six state teams commented about clarifications or revisions to the HIPAA Privacy Rule. One state team stated that clarification and perhaps revision of the Privacy Rule is necessary to reduce the variation in understanding and application of Privacy Rule provisions across organizations and states. Three states commented that many of their state-level solutions could readily be shared with other states and, therefore, are relevant at a national level.

One state team proposed that the federal government amend or update the HIPAA Privacy Rule to address whether patients need to provide separate consent or authorization to allow their protected health information (PHI) to be accessible through the HIE network. In addition, the state team proposed that the amendment address whether a patient must take affirmative action to opt in to the network or will be allowed to opt out of the network. A second state recommended a change to the Privacy Rule that would require the provider to obtain authorization for downstream disclosures at the point of service to facilitate future requests for disclosure of health information held by that provider.

One state team provided recommendations along with a detailed rationale, which is presented below. The state team noted that, although the HIPAA Privacy Rule introduced requirements intended to protect patient privacy, the analysis of business practices revealed that, in some cases, the requirements increased administrative burdens that may impede electronic health information exchange without commensurate improvements in patient privacy protections. The state team further explained that in other cases, the HIPAA Privacy Rule requirements provide important protections to patient privacy but are broadly interpreted and implemented with wide variation. The state team recommended 3 changes to the Privacy Rule:

1. **BAAs:** Remove the requirement to have a BAA, but hold business associates directly accountable and liable for adhering to the HIPAA Rules.

The rationale is that determining the requirement for a BAA is administratively burdensome. Drafting BAAs is similarly time- and resource-intensive because separate, unique BAAs are required for almost every business associate. Although a national standard for BAA language exists, it is not uniformly applied. BAAs can also be confused with trading partner agreements. On balance, work group members consider BAAs to be burdensome and costly undertakings with little gain to operational efficiency or patient privacy.

2. **Minimum necessary:** Develop model policies and procedures to clarify and promote consistent application of the *minimum necessary* standard.

The *minimum necessary* standard, a specific protection of the Privacy Rule, is derived from confidentiality codes and practices commonly used today.¹⁹ It is based on sound current practice that the use and disclosure of PHI should be limited to what is necessary to satisfy a particular purpose or carry out a function. The *minimum necessary* standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI. The Privacy Rule's requirements for the *minimum necessary* standard are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.²⁰

¹⁹ 45 C.F.R. §§ 164.502(b), 164.514(d).

²⁰ OCR HIPAA Privacy Rule, December 3, 2002; revised April 4, 2003.

The Privacy Rule requires that the *minimum necessary* standard be applied unless the regulations specifically states otherwise. The application of the standard is distinctly different for uses other than disclosures and is applied differently for routine and nonroutine disclosures. The Privacy Rule generally refers to uses as internal *sharing* of information and disclosures as a *release* of information made outside the covered entity. The Privacy Rule is written so that each covered entity interprets the *minimum necessary* standard in its own policies and procedures.

The state reports that application of the *minimum necessary* standard creates a significant barrier to electronic health information exchange. The standard makes it difficult to determine what is to be disclosed and allows for subjective decision-making on the amount of information that is disclosed. Moreover, it is difficult to know what information will be received.

The state team noted that it may not be feasible to adhere to the *minimum necessary* standard in many HIE systems. In an electronic exchange, *minimum necessary* may require limitation of access or other technology that allows for layered access. In organizations with paper records, for exchanges subject to the *minimum necessary* standard, an individual must sort through the chart and copy only the relevant pieces of information before releasing the information. The standard, therefore, may require specific technology requirements, specially trained staff to evaluate records, or both, which may increase costs and administration of the disclosure process.

In addition to the requirements of the law, variations in business practice as a result of varying applications of the standard of the loosely defined law create further barriers to information exchange. For example, if one organization limits information in one way while the organization it is exchanging with limits it another way, it is difficult to obtain the information required for the intended purpose. The inconsistency in application may also result in insufficient information being provided when necessary for patient health care processes. Thus, the state project team recommended both rewriting a section of state code, so that it mirrors the Privacy Rule and developing state and national model policies and procedures for defining and applying the *minimum necessary* standard.

Almost all of the states recognized the need for each state to clarify and standardize the *minimum necessary* requirements to reduce the variation in business practice and policy that will impede electronic health information exchange, and the majority felt that a national standard or uniform agreement for defining and applying the *minimum necessary* standard was necessary. One state proposed a change to the HIPAA Privacy Rule to allow full sharing of patient information for treatment, payment and health care operations, minus the *minimum necessary* requirement.

6.2.2 Clarify Legal Status Under HIPAA of Entities Participating in a Health Information Exchange

Two states noted the need to clarify the legal status of certain entities participating in centralized, state-level HIEs, including regional health information organizations (RHIOs), under the terms of the HIPAA Rules and to clarify whether these entities should be considered covered entities, business associates, or another as yet undefined category. The state teams also agree that a framework needs to be developed at a national level for liability that addresses the role of the state-level HIE organizations (such as a RHIO) and the interaction of federal and state regulatory frameworks. The state teams noted a need to adopt a nationally accepted common definition of terms when referring to these organizations, their organizational and structural models and core components, their operational frameworks, and their legal standing in terms of liability.

6.2.3 Confidentiality of Alcohol and Drug Abuse Patient Records (42 C.F.R. pt. 2)

Seven states expressed concerns about the current constraints to exchanging alcohol and drug abuse patient record information under 42 C.F.R. pt. 2.²¹ This regulation generally requires information from an alcohol or substance abuse treatment program to be treated confidentially. The rule generally requires the patient's consent for disclosure of information, including for treatment (except in emergency circumstances) and prohibits a health care provider or plan that receives such information from redisclosing that information without patient consent.²² In contrast, the HIPAA Privacy Rule does not require consent or authorization to disclose or redisclose health information for treatment. Because 42 C.F.R. pt. 2 is more protective of patient privacy in this circumstance than the Privacy Rule, a number of states believe this creates a barrier to electronic health information exchange and may interfere with the quality of care.

Three states proposed legislative or regulatory solutions including:

- Work with the Substance Abuse and Mental Health Services Administration (SAMHSA), the federal organization in charge of 42 C.F.R. pt. 2, on how best to approach substance abuse information disclosure in HIE.
- Amend 42 C.F.R. pt. 2 to provide that patient consent is not required to exchange the data for treatment purposes and impose strict monetary penalties for misuse or inappropriate disclosure of identifiable alcohol or chemical dependency data (that would require appropriate and consistent enforcement activity).

²¹ 42 C.F.R. pt. 2 uses the term *alcohol and drug abuse*. Most of the states used the term *substance abuse*. This summary has adopted the terminology from the federal regulation for consistency.

²² Although 42 C.F.R. pt. 2 applies only to *federally funded* programs, that term is broadly defined and most alcohol or chemical dependency providers must comply with the regulation. In addition, most other providers in this field require a patient's consent before disclosing clinical data either due to ethical obligations or liability concerns.

- Consider an exception in the 42 C.F.R. pt. 2 regulations so that when people consent to disclose their information to a provider for treatment purposes, this consent includes disclosure of any and all information deemed necessary for the treating provider accessing the HIE.
- Explore HHS's authority to define the contours of the consent without the need for legislative action, recognizing that it may not be permitted without Congressional action. That is, the consent provisions should be clarified so that a single consent would allow for unlimited downstream releases for certain purposes (e.g., treatment), clarify that consents can describe generally the entities to which pt. 2 records may be disclosed (e.g., health care providers), and also allow consent to be effective indefinitely—at least until explicitly revoked.
- 42 C.F.R. pt. 2 was established before electronic health information exchange and electronic records. Although efforts to add protection to substance abuse and mental health data are no less important, the stakeholders found no consensus about what class of information requires extra protection. In the end, states recommended federal legislation that would protect all personal health information equally.
- Amend 42 C.F.R. pt. 2 to allow for re-release of substance abuse and mental health information without limitation for treatment.

6.2.4 Revision or Amendment to CLIA Regulations

One state suggested a revision to the federal CLIA regulations. The federal CLIA regulations, 42 C.F.R. § 1291(f), currently provide that “Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test.” The term *authorized person* is defined in 42 C.F.R. § 493.2 as “an individual authorized under State law to order tests or receive test results, or both.” The term *individual responsible for using the test results* is not defined in the CLIA regulations, and the team found considerable uncertainty about its meaning. The state team proposed that the federal CLIA provisions may pose a barrier to laboratories’ exchanging test results directly with the non-ordering providers to whom patients are referred, RHIOs, and other stakeholders who may participate in electronic health information exchange for legitimate purposes otherwise permitted by the HIPAA Privacy Rule but are not identified as *authorized persons* for receipt of test results under state law. The state team’s proposals include changes to both state and federal statutes to clarify the terms believed to be causing the confusion. Such changes may not be feasible at the federal level, and any effort to make these changes to state law should be thoroughly researched to ensure consistency with the purposes of the intended privacy permissions under CLIA.

6.2.5 Clarification of Medicaid Data Disclosure

Many states noted that federal guidelines related to Medicaid data release were a barrier to electronic health information exchange. To facilitate this exchange, 2 states felt that the Medicaid guidelines needed to be reviewed at a federal level and that guidelines/rules should be established to facilitate the flow of health information between Medicaid programs and non-Medicaid providers. Federal statute and regulations require that disclosure or use

of Medicaid data concerning applicants or recipients must be limited to “purposes directly concerned with administration of the plan.”²³ Medicaid plan administration is narrowly defined and only includes determining eligibility and amount of assistance, providing services to recipients, and conducting or assisting with investigations, prosecutions, and civil and criminal proceedings related to administration.²⁴ In addition, information concerning Medicaid applicants or recipients may be shared only with persons who are subject to standards of confidentiality that are comparable to the Medicaid confidentiality standards. These restrictions apply to all requests for information from outside sources, including other governmental bodies. These restrictions make it difficult for Medicaid and non-Medicaid providers to share information, and also inhibit the sharing of information between states’ Medicaid agencies and other state agencies.

State teams have proposed a number of approaches to this issue. One state team has proposed establishing guidelines/rules that will facilitate the flow of health information between the state Medicaid program and non-Medicaid providers. In general, the state’s Medicaid program does not share patient-level data with non-Medicaid providers. For Medicaid to serve as a participant in a RHIO, new rules and guidelines must be established authorizing the sharing of health information between Medicaid and non-Medicaid providers. Federal regulations may limit what can be accomplished through the establishment of state guidelines. Guidelines from Centers for Medicare and Medicaid Services may be more effective. The same state team proposed the establishment of a task force to research opportunities to make electronic health information exchange reimbursable by Medicaid and under the state employee group health plan. Two additional states called for federal clarification of the laws governing access to Medicaid data.

6.3 Funding

6.3.1 Funding for More Widespread Adoption of Technology

Although this project focuses on issues related to private and secure electronic health information exchange, nearly all states raised the issue of low levels of technology adoption and the absence of a technical infrastructure as key barriers to their progress with the privacy and security work. Many state teams that represent stakeholders with low EHR use and no electronic health information exchange among organizations have difficulty gathering support for privacy and security discussions. Two state teams reported that until incentives for adopting EHR systems and HIE become organized and systematic, preferably at the national level, the discussions that have begun may stagnate.

²³ The federal regulations require that state Medicaid programs implement safeguards to protect Medicaid data. Thus, state standards actually restrict exchange, although federal statute and regulations mandate those standards.

²⁴ The federal law can be found in the Social Security Act, 42 U.S.C. §§ 1396a(a)(7), 1902(a)(7). The regulations can be found in 42 C.F.R. § 431.300 *et seq.* The definition of plan *administration* is found in § 431.302.

6.3.2 Funding for Educating Patients and Consumers

Although most states noted that various education campaigns were a fundamental way to reduce variation in practice, 2 states reported that this process would best be undertaken at the national level. One state called for a national HHS public relations effort to provide a consistent, centralized, and visible source of education to the public. The focus of the campaign would be to allay the general public's fears about data security, and reveal the many positive outcomes from a secure interoperable electronic network that assures the greatest level of privacy possible.

7. MOVING STATES FORWARD COLLECTIVELY

The primary goal of each state team was to work toward solutions that would enable secure and private transfer of electronic health information between entities. However, the importance of collaboration in this project should not be ignored. Perhaps the greatest long-term effect of these activities will be the concurrent momentum built within each of the subcontracting states, the enthusiasm of which was not confined to state lines. Although the timeframe required under the original project made it difficult for states to construct agreed-upon solutions for transmittal of data across state lines, a number of possibilities were proposed for the future.

7.1 Coordinating Standards and Policy

One state, although focusing on developing successful implementation of their state-level plans prior to widening their focus to cross-state exchange, proposed a strategy to engage in more substantive discussions with other states about planning and implementation. Preliminary discussions have been held with a neighboring state, and the states have agreed to focus on

- quantitative and qualitative assessment of the value of cross-state health care business to articulate the need for interoperable health information exchange (HIE);
- comprehensive policy assessment of consent requirements in both states' HIE environments and determination of an acceptable approach to consent management in cross-state exchanges; and
- assessment of information infrastructure and consideration of using applicable IHE interoperability profiles to establish the framework for seamless electronic health information exchange for patient care coordination.

One state proposing to produce a privacy and security core solutions set mentioned that research and input from multistate stakeholders would help ensure that the final solutions are appropriate for regional and national use.

Policy mapping and exchange agreements among Health Information Security and Privacy Collaboration (HISPC) states were noted as important to achieving the interoperable solutions. Specific exchange analysis and agreements will be needed, along with identification of specific consent/authorizations and standards for exchange. Specifically, the intent is to use the IHE Cross-Community Information Exchange (XCS) profile development, currently underway and under consideration by the Health Information Technology and Standards Panel, to establish a standards-based interstate exchange among states.

The same state urged a process to share and discuss cross-state solutions through an entity, preferably one supported by Office of the National Coordinator for Health Information Technology, such as the State Alliance for e-Health, that can identify solutions affecting interstate HIE. Suggestions for focus areas included patient identification, authorizations for

release, and standards. Patient and provider identification were noted as the most fundamental issues, with a secondary focus on information and interface standards.

7.2 Coordinating HIEs Between States

Several states identified opportunities to work with bordering states to coordinate interstate HIEs, particularly those involving emergency situations, public health conditions, or special population groups, such as Medicaid.

7.3 Coordinating Legislation

At least 6 states identified model state law as a pursuit that would save time for each state. The National Conference of Commissioners on Uniform State Laws (NCCUSL) is the logical vehicle to develop common privacy and security solutions across states. NCCUSL will need input both from the HISPC projects and the State Alliance for e-Health to accomplish this goal.

Another recommendation is to establish an interstate task force to collectively develop electronic health information exchange procedures and review laws for HIE among states. An evaluation should be done to determine what laws, if any, should be harmonized at the national level and what laws should stay in place to reflect the values of local communities across the country.

8. CONCLUSIONS AND NEXT STEPS

While the national-level recommendations summarized in Section 7 are an important outcome of the project, the final effort will focus on developing implementation plans for the state/territory level solutions summarized in Section 6. These have been classified into 6 types of solutions—business policy, legal/regulatory, technology/data standards, education, governance, and collateral issues (related to funding, encouraging electronic health record adoption, and stakeholder engagement).

The implementation plans for each member of the Health Information Security and Privacy Collaboration (HISPC) have been emphasized since the project's initiation. Project teams in each state and territory have been reminded that the government's purpose in funding this project has been not only to identify the variation in business practices, policies, and laws that present challenges to electronic health information exchange, but also to develop solutions that protect the privacy and security of health information. The project has generated a great deal of discussion among stakeholders in steering committees, work group sessions, and stakeholder meetings, as well as at the regional and national meetings. These discussions have, in turn, resulted in stakeholders' commitments to fulfill the promises of improved health information exchange. In addition to a better understanding of challenges and solutions, the perpetuation of this commitment is a major goal of the collaboration.

In developing their implementation plans, the state teams have been encouraged to focus on the practical and efficacious. As noted previously, conditions relevant to health information exchange vary on a number of dimensions both within and between states. What works in one state may not in another. The project teams have been encouraged to vet implementation plans with stakeholder groups in the same iterative process used in identifying variations in business practices and barriers and developing solutions.

Draft implementation plans provided by the teams in each state/territory have included specific objectives in

- governance and leadership;
- business practices and policies;
- legal and regulatory solutions;
- technological and data standards solutions; and
- education and outreach.

In addition to these concrete objectives, the project teams in each state/territory have provided practical considerations related to accountability, funding, and scheduling.