

June 30, 2007

Privacy and Security Solutions for Interoperable Health Information Exchange

Final Implementation Plans

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 0209825.000.008

Contract Number 290-05-0015
RTI Project Number 0209825.000.008

Privacy and Security Solutions for Interoperable Health Information Exchange

Final Implementation Plans

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 | 1-1 |
| 1.1 Scope, Limitations, and Assumptions of the IPs | 1-2 |
| 1.1.1 Scope of State IPs | 1-3 |
| 1.1.2 Limitations of State IPs | 1-3 |
| 1.1.3 Assumptions of State IPs..... | 1-4 |
| 2. Summary of Proposed Solutions | 2-1 |
| 2.1 Leadership and Governance Solutions | 2-3 |
| 2.2 Practice and Policy Solutions..... | 2-4 |
| 2.3 Legal and Regulatory Solutions | 2-5 |
| 2.4 Technology and Standards Solutions | 2-6 |
| 2.5 Education and Outreach Solutions..... | 2-10 |
| 3. Review of State Implementation Planning Process | 3-1 |
| 3.1 Formation of Implementation Planning Work Groups | 3-1 |
| 3.2 Process Used to Identify, Prioritize, and Develop Implementation Plans..... | 3-2 |
| 3.3 Stakeholder Engagement and Involvement | 3-4 |
| 4. Implementing State-Level Solutions | 4-1 |
| 4.1 Implementing Leadership and Governance Solutions | 4-1 |
| 4.1.1 Creation of New Oversight Bodies | 4-1 |
| 4.1.2 Leveraging Existing Leadership Efforts to Implement Solutions | 4-2 |
| 4.1.3 Creation of New Governance Structures..... | 4-2 |
| 4.1.4 Analysis of Feasibility and Barriers to Implementation of Leadership and Governance Solutions | 4-3 |
| 4.2 Implementing Practice and Policy Solutions..... | 4-4 |
| 4.2.1 Consent and Authorization | 4-4 |
| 4.2.2 Interpretation and Application of Federal Regulations | 4-5 |
| 4.2.3 Exchanging Sensitive Health Information | 4-5 |
| 4.2.4 Standardized/Model Documents..... | 4-6 |
| 4.2.5 Exchange of Medicaid Data | 4-6 |

| | | |
|-----------|--|------------|
| 4.2.6 | Data Exchanges with Public Health..... | 4-7 |
| 4.2.7 | Data Exchanges with Law Enforcement..... | 4-7 |
| 4.2.8 | Other Practice or Policy Solutions..... | 4-8 |
| 4.2.9 | Analysis of Feasibility and Barriers to Implementation of Practice and Policy Solutions..... | 4-8 |
| 4.3 | Implementing Legal and Regulatory Solutions | 4-8 |
| 4.3.1 | Amending State Law | 4-8 |
| 4.3.2 | Introducing New State Law | 4-11 |
| 4.3.3 | Implementing Other Legal and Regulatory Solutions..... | 4-11 |
| 4.3.4 | Analysis of Feasibility and Barriers to Implementation of Legal and Regulatory Solutions..... | 4-12 |
| 4.4 | Implementing Technology Solutions..... | 4-13 |
| 4.4.1 | Patient and Provider Identification | 4-13 |
| 4.4.2 | User and Entity Authentication | 4-14 |
| 4.4.3 | Information Authorization and Access Controls | 4-14 |
| 4.4.4 | Information Audits..... | 4-17 |
| 4.4.5 | Information Transmission Security, Data Integrity, and Remote Access | 4-18 |
| 4.4.6 | Information Standards and Best Practices | 4-18 |
| 4.4.7 | Analysis of Feasibility and Barriers to Implementation of Technical Solutions..... | 4-19 |
| 4.5 | Implementing Education and Outreach Plans | 4-21 |
| 4.5.1 | Consumer Engagement and Education..... | 4-21 |
| 4.5.2 | Provider Education and Outreach | 4-22 |
| 4.5.3 | Other Education and Outreach (To Health Plans, Policy Makers, and Others) | 4-23 |
| 4.5.4 | Implementation Plans Addressing Other State Solutions..... | 4-23 |
| 4.5.5 | Analysis of Feasibility and Barriers to Implementation of Education and Outreach Plans..... | 4-23 |
| 5. | Implementing Multistate Solutions | 5-1 |
| 5.1 | Multistate Leadership and Governance Solutions..... | 5-1 |
| 5.2 | Multistate Practice and Policy Solutions | 5-2 |
| 5.3 | Multistate Legal and Regulatory Solutions..... | 5-3 |
| 5.4 | Multistate Technology and Data Standards Solutions | 5-4 |
| 5.5 | Multistate Education and Outreach Solutions | 5-4 |
| 5.6 | Analysis of Feasibility and Barriers to Implementation | 5-4 |

| | |
|---|------------|
| 6. Implementing National Solutions/Recommendations | 6-1 |
| 6.1 National Governance: Identification of Responsible Bodies | 6-1 |
| 6.2 National Practice and Policy Recommendations | 6-2 |
| 6.3 National Legal and Regulatory Recommendations..... | 6-3 |
| 6.4 National Technology and Data Standards Recommendations..... | 6-4 |
| 6.5 National Education and Outreach Recommendations..... | 6-6 |
| 6.6 Analysis of Feasibility and Barriers to Implementation | 6-6 |

Appendixes

| | |
|-------------------------------|-----|
| A: Glossary of Acronyms | A-1 |
|-------------------------------|-----|

Tables

| Number | Page |
|---|------|
| 2-1. Stakeholder Group Participation in the Solutions Work Group..... | 2-2 |
| 3-1. Stakeholder Group Membership in Implementation Planning Work Groups | 3-3 |
| 3-2. Stakeholder Groups Engaged in Implementation Planning Through Community Outreach..... | 3-6 |

EXECUTIVE SUMMARY

This report is a summary of the 34 final Implementation Plans (IPs) that were drafted by the state project teams¹ 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 jointly managed by AHRQ and the Office of the National Coordinator for Health Information Technology. The following summary report provides a glimpse into the activities that the 33 states and 1 territory that form the Health Information Security and Privacy Collaboration plan to implement in their states over the next 12 to 18 months.

Background

The IPs serve as both the culmination of prior work on the project and as practical tools for sustaining the development of privacy and security solutions that enable the electronic exchange of health information. To produce these plans, the state project teams followed a process that encouraged sharing observations, ideas, and concerns among an array of stakeholders including consumers, providers, insurers, state agencies, and others involved in health information exchange. The process began with the assessment of variations in business practices related to interorganizational exchange, the identification of barriers to electronic exchange, and the proposal of solutions to barriers that both enable the electronic exchange and maintain the privacy and security of health information.

The IPs summarized in this report are intended to be actionable documents that will guide the development and adoption of a framework for privacy and security for electronic health information exchange. The project teams in each state prepared both short- and long-term plans to protect privacy and security. Many of the plans mention uncertainty about funding for the implementation plans as a constraint in considering scope and schedule of the plans. Some plans included securing funding as a critical part of the plan.

Many of the IPs noted difficulty in considering privacy and security solutions in the absence of a practical model of how exchange might occur and where in the process safeguards can be put into place. Limitations also included interdependencies with national-level issues that remain to be resolved or addressed, and state and regional uncertainties with the legislative process needed to make changes or modifications to existing laws.

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

Implementing State-level Solutions

Implementing Leadership and Governance Solutions

In Section 4.1 we describe the state project teams' proposed approaches to leadership and governance of privacy and security activities moving forward. Fourteen of the 34 state project teams proposed the need for an oversight body. Eleven state teams proposed creating a new oversight body to lead and promote electronic health information exchange activities within the state, including implementing solutions and carrying on work done by the state project teams; issuing policy, technical, and/or legal guidance; and promoting interoperability. Teams proposed that this body could derive from a legislative or executive mandate.

In addition to the need for oversight, state project teams also planned to implement governance structures that include stakeholder work groups including legal and technical groups that would offer leadership and guidance as solutions are vetted and implemented. In addition to providing leadership and guidance, tasks assigned to the governing committees also included promoting the adoption and use of electronic health records (EHRs) and best practices to small and rural providers within the state.

The majority of state project teams proposing leadership and governance structures thought that this was feasible. Although the state teams were generally optimistic with respect to implementation, 13 state teams raised funding as the most likely barrier to success. Staffing and government support were the next most frequently cited barriers to implementation. State project teams where electronic health information exchange efforts were just beginning noted that they were eager to access the expertise available from states that are more advanced in setting up their efforts.

Implementing Practice and Policy Solutions

A majority of solutions state project teams put forward were multifaceted and most had a policy or practice component. For example, although approaches to obtaining and documenting patient consent and authorization included technology and legal components, there was widespread agreement about the need for common understanding on the critical elements that comprise patient consent and the need for a universal consent form. A number of states also noted that those policies will need to address consent management in emergency situations and for specially protected information.

Policy development was also proposed to reduce variation associated with the interpretation and application of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. Many state project teams proposed plans to draft policy manuals and to provide training and policy guidance and education. One state proposed working with professional associations within the state to help develop consistent definitions and interpretations of terms and concepts related to the HIPAA Rules.

Several states proposed addressing the variation related to exchange of specially protected health information, which generally includes alcohol and drug abuse, mental health information, and human immunodeficiency virus/acquired immunodeficiency syndrome (HIV/AIDS) status, with policy solutions rather than making recommendations for federal action. Ten state project teams included policy solutions for exchanging specially protected health information.

Six state teams proposed the use of some type of model documents. Three state project teams planned to draft language for business associate agreements (BAAs),² to be used by HIPAA-covered entities within the state. One of these 3 state project teams intended to include education regarding model BAAs. Two additional state project teams made general reference to drafting standardized forms or policies, but did not develop these plans in greater detail.

Three state project teams addressed the issue of exchanging Medicaid data, with 2 state teams outlining implementation plans to do so. One state intended to establish policies to facilitate the flow of information between Medicaid and non-Medicaid providers. Another state proposed creating minimum security standards for sharing Medicaid data, implemented through contractual agreements.

Two state project teams raised the issue of exchanging information with public health authorities, although the plans were not fully developed. One state project team noted the value of law enforcement officials in emergency situations and raised the issue of data exchange with law enforcement. The team planned to offer targeted training programs for law enforcement officials including judges and to develop model protocols for information exchange by conferring with state agencies, the attorney general's office, and police on the design of the protocol. The state project teams noted that funding and stakeholder and consumer engagement were likely to be the biggest barriers to implementing policy solutions. Other potential barriers included resistance to change among health care staff and lack of political support.

Implementing Legal and Regulatory Solutions

Three state project teams included plans for updating state law to apply to electronic health information exchange. These ranged from broad unspecified plans to plans with a narrow

² The states generally used the term *business associate agreement* instead of the regulatory term *business associate contract or arrangement*. Either term is acceptable, but the agreement must be in some form of legally enforceable vehicle, such as a contract, or in the intra-governmental context, a memorandum of understanding. The HIPAA Privacy and Security Rules require covered entities to document 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, memorandums of understanding between agencies. Thus, the term *business associate agreement (BAA)* encompasses both contracts and other arrangements and this term is used in the summary above.

focus such as planning to update a law that requires wet signatures to accommodate electronic signatures when prescribing medications.

Proposed amendments to state law fell into 3 broad categories: amending state law to mirror federal law, amending state law to remedy state-specific concerns, and amending or drafting new state law to address consistency issues more broadly. Five state project teams drafted plans to align state law with federal law, usually HIPAA. Two teams made general reference to federal law, 1 explicitly referenced HIPAA, and the other 2 planned to incorporate the HIPAA Privacy Rule treatment, payment, and health care operations exemption from patient authorization into state law. State-specific concerns were related to specific language (or lack thereof) in state law. Four state project teams drafted language that could be used to amend state law related to consent, interactions between Medicaid and non-Medicaid providers, treatment, electronic health information exchange and minors, and specially protected information, including genetic testing results. Three project teams planned to amend state law to correct inconsistencies in definitions of terms and between state regulations governing the exchange of general health information and specially protected information.

Eleven teams' plans included recommendations for new legislation and 3 teams planned to draft new legislation, but were still in the process of examining the need for legislation in a number of areas. One team was unable to locate any state law that applied to electronic exchange and planned to form a committee to draft foundational laws and regulations.

The remaining legal and regulatory solutions fell into 2 general categories: consolidating or centralizing state laws and regulations, and considerations of the Physician Self-Referral Law and the Healthcare Antikickback Law (commonly referred to as the Stark and Antikickback Laws). Three state project teams planned to consolidate their state laws and regulations governing privacy and security. It was thought that collocating the various pieces of applicable legislation would facilitate legal analyses and reduce variation in business practices.

Two state project teams planned to resolve issues related to the Stark and Antikickback Laws. The Stark and Antikickback Laws prohibit physicians from receiving compensation, including nonmonetary compensation, for referrals of Medicare and Medicaid patients. In 2006, the Department of Health and Human Services (HHS) announced new regulations allowing exceptions for the donation of health information technology (HIT) equipment to facilitate adoption of HIT and EHRs. Although the state project teams did not fully develop their IPs for addressing these issues, they planned to do so in subsequent work.

State project teams identified a number of potential barriers to implementing regulatory solutions; the most frequently cited was lack of stakeholder support. The need to have full stakeholder support for any legislative change was recognized, although plans to gain that support were not fully formulated. One state anticipated resistance to their proposed

legislative amendment and included other options for amending state law, as well as an analysis of the risks and benefits of choosing other solutions.

Other commonly cited barriers included those related to the legislative process. Three states have legislatures that meet infrequently and/or for short periods of time. The compressed time frame of these legislative sessions makes it difficult to pass legislation that does not have substantial support from the outset. While some states were confident that they would receive support from legislators, 2 state teams expressed doubts about their ability to find sponsors for their legislation or to achieve consensus with those sponsors.

Implementing Technology and Standards Solutions

The majority of technology solutions focused on methods for patient and provider identification, user and entity authentication, authorization, and access controls. Several state project teams focused on developing a centralized provider directory to authenticate and authorize providers. State project teams also proposed using a master patient index and a provider identification management system to function within their HIE or regional health information organization. Other state project teams proposed probabilistic matching algorithms to match patients with their records. Ten of the state project teams included IPs related to user and entity authentication. Several state project teams studied biometrics and other authentication tools. One state planned to develop a personalized health smart card that individuals can carry. Another state was undertaking a pilot project to automate the flow of laboratory orders and results among the major laboratories servicing the state and health care providers. This was chosen as the vehicle for centralizing and sharing authentication services as well as implementing interorganizational secure messaging.

Eighteen of the state project teams planned to implement solutions related to information authorization and access controls to ensure access to data, people, or software programs that have been granted access rights. The plans ranged from developing role-based access standards that account for physicians' on-call coverage and emergency roles to implementing various authentication technologies. Many of the state project teams tackled the issues related to authentication, authorization, access, and audit as a group (i.e., the 4 A's). The state project teams formed subgroups to research specific technology and process solutions using various exchange models including centralized, federated, and hybrid. Other states defined procedures and processes. One state project team is developing a consensus model document of policies and procedures based on the provisions of the HIPAA Rules. Another state project team drafted 19 principles or best practices to guide their implementation. Specific technology solutions proposed for implementation included digital signatures, digital certificates, biometrics, and USB and card swipe technologies. Several state project teams were developing software tools to assist in specifying *minimum necessary* information and specially protected health information. Seven state project teams focused on information audits that record and monitor the

activity of health information systems; most of the teams were planning to adopt industry standards, but other teams planned to develop a framework for what standards need to be reviewed and how to identify best practices.

Five state project teams planned to implement or strengthen information transmission security or exchange protocols for information exchanged over an electronic communications network. All of these teams will focus on the design and implementation of technical solutions for expanded data exchange services, and several state project teams will draft rules to govern how personal health information can be transmitted. One state project team was specifically examining encryption as a technical solution and planned to use their newborn screening program as a test case for implementing the new rules. Another state project team will require that any patient information being transmitted on external networks go through a virtual private network connection between client and server or network to network.

Five of the state project teams planned to implement broad information security standards and best practices. State project teams in the early planning stages for electronic health information exchange were working to develop vocabulary, data, and messaging standards while other state project teams planned to examine security standards in all 9 domains. Typical of the more comprehensive approach was the plan to form an information technology security committee to identify and establish a wide range of security standards for entities participating in an HIE that will initially focus on established security protocols, organizational standards, and minimum standards for exchange. Later work will involve testing and recommending common standards and protocols in conjunction with privacy policies for all areas of security. Another state project team planning a comprehensive approach planned to establish data element standards and create a best practices repository.

Implementing Education and Outreach Solutions

The majority of the states proposed some form of informational group meeting to share information about electronic health information exchange with consumers. The goal of the sessions is twofold: to educate consumers on the secure exchange of electronic health information and to solicit input regarding the implementation plans and process. In addition to the informational meetings, some states proposed utilizing a secure website to keep consumers engaged and updated. Several states also planned to create consumer advisory committees as a way to maintain consumer engagement.

Consumer education and engagement aims to address to 3 major issues: First, consumers are often not aware of their rights and responsibilities with respect to their health care records. Second, consumers may not be aware of the benefits of electronic health information exchange and EHRs. Finally, because of the lack of information, consumers may

mistrust HIEs and EHRs. As one state noted, “The cumulative differences in knowledge among consumers and health care industry staff naturally leads to mistrust and negatively affects consumers’ confidence for participation in electronic health information exchange.” Another observed:

Patients and consumers are generally not aware of the privacy protections and rights they enjoy under the HIPAA Rules and state law. Because of this, many patients and consumers retain an unnecessarily high level of distrust regarding the storage and communication of their health care information when it is in electronic form. This high level of public distrust may threaten to delay or derail the transition of the health care delivery system into the information age.

Sixteen state teams included IPs for engaging with or educating consumers. These efforts included community forums, focus groups, pamphlets and other literature, and a website with frequently asked questions and other resources. Other options include television and radio campaigns and collaboration with consumer groups to raise awareness about the benefits of electronic health information exchange.

In addition to reaching out to consumers, state teams also planned outreach and educational efforts for providers. States identified different levels of knowledge among health care industry stakeholders about privacy and security requirements for electronic health information exchange. The purpose for the provider education plans is to reduce variations due to incorrect or incomplete understanding of relevant state and federal law. Provider education may also reduce liability concerns and facilitate exchange if providers are more confident in their compliance with state and federal law. Twelve state teams outlined education efforts for providers, with 5 of these functioning as components of broader educational efforts that include education and outreach for consumers and others, such as payers and employers. In addition to general awareness about electronic health information exchange and HIT, state teams also sought to raise awareness about specific issues. Three states proposed educational efforts relevant to newly passed or anticipated legislation that could change the way providers exchange information.

In addition to patients and providers, almost all of the state teams proposed plans for informational sessions tailored toward legislators and government leaders to garner support and funds for initiatives although the teams often did not include details on implementation with the exception of 1 state team that plans to hold a statewide health information network summit to share technological solutions to the privacy and security barriers identified in their state.

Two other groups that state teams identified as targets for educational efforts included public health and law enforcement officials. These individuals frequently need access to personal health information in order to conduct disease surveillance and investigation in the case of public health, and to assist in emergency care of a patient or to conduct criminal

investigations and prosecutions in the case of law enforcement. Three state teams planned educational programs for law enforcement officials. Two have already had success in working with the officers, and 1 includes relevant training for members of the service academy. One state planned to educate public health officials about their role in electronic health information exchange, but did not offer details. Finally, 1 state has included public health from the inception of their project, and has integrated a public health perspective into their entire planning process.

State teams felt that it was feasible to implement education and outreach programs. Although such programs may be costly, there are established frameworks for educating consumers and providers. In addition, the fact that many state teams feel that such education is critical to the success of electronic health information exchange and HIT makes these programs a priority.

Although the state teams believe that educational solutions are feasible, they do recognize that they will require special expertise in executing the education and outreach campaigns and therefore often listed the need to identify and hire a marketing or communication consultant to develop effective consumer messages. The state teams also proposed to identify subject matter experts to be used in the various education forums. Another state team reported that current events, such as those related to widely publicized breaches or other unapproved releases of personal information, will greatly influence receptivity of messages and acceptance of those messages.

Again, funding was a frequently cited barrier, as were stakeholder buy-in and political support.

Implementing Multistate Solutions

Nineteen state project teams discussed the importance of transcending state lines to provide quality and continuity of care for individuals traveling between states to receive their health care, but only a few state project teams proposed plans for multistate exchange. Four states proposed potential solutions that had specific tasks or time frames, while another 11 state teams articulated the desire to collaborate with other states on a particular issue and 5 additional state teams indicated a desire to pursue more organized plans but felt that additional time and continued networking support were needed in order to achieve a more structured collaborative environment for multistate solutions.

Few of the states proposed specific plans for the creation of a governance structure that would oversee the creation of common privacy policy and security solutions between multiple states, although a handful of states noted a willingness to join in such an effort if one were started. Three states mentioned the possibility of coordinating efforts in their own states with the efforts of a common coordinating body such as the State Alliance for e-Health. One state indicated that it planned to convene a "multistate work group" that

would track the direction in which neighboring states were going in a variety of different areas and feed that information to other state-level work groups (clinical, technical, legal/policy, etc).

State project teams noted a need to develop a plan for sharing data across state borders in the case of disaster or emergency and continuing to explore legal templates that could be shared between states. Three state project teams planned to pursue standard policies with other states concerning emergency or “break the glass” procedures. One state project team clearly outlined a plan to expand the state effort through its department of health and department of emergency management to pursue communications plans and strategies in the case of a bioterrorist attack or natural disaster into a regional plan. Three other state project teams proposed to standardize the criteria used to identify a patient within an electronic exchange. Three state project teams mentioned the need to standardize consent practices across state boundaries. However, no plan details were provided.

One state project team discussed working on a model state law to improve interstate communication and another state project team suggested working with the National Conference of Commissioners on Uniform State Laws as part of a general review on harmonizing federal and state law. Again, specific goals were not outlined in terms of formulating or utilizing model laws. Two state project teams proposed specific plans to pursue a compact between 3 states before the end of 2008 that would seek to clarify the legal interstate environments related to each state’s electronic health information exchange programs. Further, the state project teams proposed to standardize laws between neighboring states that protect genetic information and define *age of consent*.

Four states proposed plans to create regional standards for technical issues, including the development of a core set of privacy and security solutions. None of the state project teams proposed multistate outreach or education plans.

Implementing National Solutions/Recommendations

The state project teams were charged with solving issues at the state level rather than making recommendations for action at the national level, unless necessary to accomplish their state-level goals. The state teams that did include recommendations for actions to be taken at the national level indicated that it would simply be more expedient to implement some standards at the national level than to try to achieve consensus within and across states.

Most of the state project teams expressed a desire to see greater coordination of governance, policy, regulation, technology standards, and education at the national level rather than in scattered regional pockets. Twenty-one states made some type of recommendation regarding national-level intervention. A number of states offered to participate in leadership and the development of policy and technical standards, especially

when they felt they had already made significant headway through local initiatives. The theme, however, clearly indicated a strong feeling that these efforts should be centrally coordinated and not left completely to local efforts, which can be scattered and lack adequate resources. There is a shared understanding that central coordination will provide for efficient knowledge transfer between state project teams that will advance the initiative nationwide.

Seven states proposed recommendations for federal guidance on practice and policy. First, although the states recognize that the variation in the way approval policies such as consent and authorization are defined and implemented is largely driven by state laws, there is widespread confusion when organizations try to reconcile the requirements of state law with federal regulations that are more stringent with regard to specially protected data. Three states suggested that a basic or core set of practices and policies for consent and authorization could be defined and coordinated at the national level so states could choose to adopt those that best met the needs of the state.

Three states suggested that federal policy guidelines regarding certain data elements would greatly reduce the burden of developing technical standards. Two states suggested using the American Society for Testing and Materials (ATSM) continuity of care record (CCR) as a policy adoption target that would encourage the development of a data set that health care providers would feel comfortable using. It is important to note here that the Health Information Technology Standards Panel (HITSP) has endorsed the work done by ATSM and Health Level 7 (HL7) to harmonize their respective standards to create the continuity of care document (CCD). The CCD describes the use of the CCR standard data set so it could function within the broader capabilities of HL7's clinical document architecture (CDA).

Twelve states proposed the need for legislation or guidance at the federal level.

Three states suggested the need for new legislation or guidance concerning HIEs or other clearinghouse organizations to enable information sharing between state-level HIEs. The federal legislation would designate a federal privacy and security standard that preempts more stringent state legislation in connection with information that is sent from one state to another via a health information network. The state teams also recommended that the legal status of HIEs be addressed at the national level, as well as the process of developing a framework for liability that addresses the role of the state-level HIEs and the interaction of federal and state-level regulatory frameworks.

Medicaid: One state team suggested that federal guidelines related to Medicaid data release be reviewed and streamlined. The desired outcome would be changes to both federal and/or state guidelines related to sharing of Medicaid data. Another state asked both the Centers for Medicare & Medicaid Services and the Office of Inspector General for a favorable advisory opinion excepting some specific level of cooperation between physicians

and hospitals with respect to sharing money for technology or participating in demonstration projects.

Stark and Antikickback Laws: Two states suggested expanding the scope of these regulations to target providers who serve the historically underserved, and to amend these regulations such that hospitals are allowed and possibly induced to provide physician practices that are serving economically disadvantaged populations with not only hardware, software, and training, but also additional technical resources to implement and support the technology.

Clarification of HIPAA Privacy Rule: Three states suggested clarification or changes to the HIPAA Privacy Rule. One recommendation was to change the HIPAA Privacy Rule so that it would require the provider to obtain a patient's legal permission once at the initial point of service that would permit the provider to release the information for specific purposes and to specified entities in the future. The suggestion to make patient permission mandatory for current exchanges for treatment, payment, and health care operations was thought to facilitate future requests for the release of the information held by that specific provider. The state team believed that making this a federal recommendation or standard would facilitate the interstate exchange of information.

42 C.F.R. pt. 2: One state suggested that HHS explore the contours of consent/approval without the need for legislative action although they also recognized that their suggestion may require congressional action. The team is recommending that HHS more clearly define 42 C.F.R. pt. 2 so that a single consent would allow for unlimited downstream releases for certain purposes and clarify that authorization can describe generally the entities to which Part 2 records may be disclosed. As an alternative, 42 C.F.R. pt. 2 could be amended to provide that patient authorization is not required to exchange the data for treatment purposes only.

CLIA: One state discussed the Clinical Laboratory Improvement Amendments, detailing specific conflicts that it imposes in their state due to ambiguity about the terms utilized. One other state proposed to review the CLIA regulations in light of HIE organizations that endeavor to provide electronic laboratory reporting services.

FERPA: Two states called for general clarification and/or revision of the Family Educational Rights and Privacy Act and educational institutions' rights to deny medical record release. It is important to note here that FERPA falls under the authority of the Department of Education.

Three state teams outlined recommendations to provide education and outreach at the national level, citing the need for a national information campaign that provides consistent and uniform messaging in the form of federally recommended education materials to include patient-consumer advocacy components and promote the idea of patient rights.

Overall the state teams are looking for a centrally coordinated effort because although the decisions need to be made at the local level, the teams do need to provide some assurance to their stakeholders that they are not operating in a vacuum and that the work they are doing will not only advance the work in their state but will also be compatible with the broader nationwide effort. It is clear that many of the teams are not fully aware of the breadth and scope of activities that are already occurring at the national level and that will serve as resources for the state teams as they move forward into implementation.

1. BACKGROUND

The final Implementation Plans (IPs) serve as the culmination of prior work on the project and as practical tools for sustaining the development of privacy and security solutions that enable electronic health information exchange. To produce these plans, the state project teams³ followed a process that encouraged sharing observations, ideas, and concerns among an array of stakeholders including providers, insurers, state agencies, consumers, and others involved in health information exchange. The process began with the assessment of variation in business practices related to interorganizational exchange of personal health information, the identification of barriers to the exchange of health information, and the proposal of solutions to barriers that both enable the electronic exchange and maintain the privacy and security of health information.

It should be noted here that the business practices under consideration are not limited to the context of electronic exchange. Exchange of health information is predominately paper-based. Even in areas where interoperable electronic medical records are common, exchange of health information is best characterized as a mixture of electronic and paper-based. In order to understand how current business practices relate to the privacy and security of health information, it is necessary to draw on examples of both modes.

The IPs summarized in this report are intended to be actionable documents that will guide and sustain adoption or expansion of electronic health information exchange. The project teams in each state were encouraged to prepare short- and long-term plans for a movement from today's hybrid environment (paper and electronic) toward an electronic health information exchange environment that is interoperable and based on common standards (privacy, security, and technical).

IPs have been developed in response to a broad array of circumstances in each state. Health information and the purposes for sharing these data are myriad, as are the types of entities involved in the exchange relationships. The many forms of health information include medical histories, diagnoses, treatments, prescriptions, laboratory orders and results, personal health records, and billing data. A good deal of the sharing of this information is related to direct care of patients, but other purposes include public health, research, and law enforcement. Exchange partners include hospitals, physicians and other health care providers, pharmacies, laboratories, and health insurance companies that are involved in direct treatment of patients. Other entities that use health information are public health agencies, educational facilities, law enforcement agencies, and research institutions. Consumers—patients and their families—themselves rely on information about their health and health care. All of these individuals and entities have legitimate concerns about access

³ Throughout this report the 33 states and 1 territory are referred to as the *state project teams* or *state teams*.

to and exchange of this specially protected information. These elements—the type of health information, the purposes of exchange, and the exchange partners—form the basis for myriad relationships that vary in nature across and within the states and territories.

With this complexity in potential and actual exchange relationships, it is not surprising that the IPs vary on a number of key dimensions, including the following:

- **Degree of adoption of electronic health information exchange**—Several states can point to functioning and sophisticated systems of HIE as models for expanding scale and coverage. However, many states lack working models and, consequently, have to imagine issues and consequences of electronic health information exchange based only on experience with paper-based systems. And it should be noted that even in states where working models exist, coverage is far from universal. Many stakeholders in each state and across the country lack practical experience with electronic health records (EHRs) and are unfamiliar with the concept.
- **Health care market forces in the state**—The business and organizational dynamics and relationships between health care entities differ across regions and states and within states and specific markets, which affect the ways in which exchange practices are adopted and implemented.
- **Legal and regulatory conditions related to health information**—Relevant laws and regulations have developed and evolved largely in response to the paper-based exchange of health information and specific concerns generally raised by advocacy groups (called specially protected health information). Legal restrictions addressing electronic health information exchange are often dispersed across many different statutes and regulations and are sometimes inconsistent with one another. Several states reported that antiquated laws written for paper-only environments created significant barriers to electronic health information exchange. Other states noted that laws are silent with respect to certain aspects of electronic health information exchange, leading to varied business practices and customs. In addition, there are differing federal regulations governing privacy and security that can affect practices related to electronic health information exchange.
- **Demographic composition of the state**—Factors within each state such as population size, cultural and ethnic diversity, and population density have been considered in the development of implementation plans. In addition, several states have considered interstate health information exchange in their plans.
- **Financial status of the state**—The plans of several states noted that funding of implementation plans would be uncertain and some states clearly indicated that the poor financial status of the state made it unlikely that scarce resources would be devoted to electronic health information exchange.

These points underscore diversity in the IPs that challenge summary. The plans were developed in response to unique situations; nonetheless, there are common elements that are discussed in this report.

1.1 Scope, Limitations, and Assumptions of the IPs

Following review of the IPs, RTI classified the proposed solutions and plans into the following 5 areas:

- **Governance**—A number of the state plans called for the establishment of a permanent body to provide oversight and guidance for the implementation of privacy and security solutions in the context of intrastate health information exchange, and, in a larger scope, implementation of regional health information exchange initiatives.
- **Business policies and practices**—Most plans called for modifications in business policies and practices related to consent and authorization, application of federal and state law, exchange of specially protected health information, standard/model documents, secondary use of data, and exchange of data related to Medicaid, public health, emergency management, and law enforcement agencies.
- **Legal and regulatory solutions**—Plans called for amending state law, introducing new legislation where required, and partnering between states and nationally to develop model legislation that will assist in conforming state privacy laws without necessarily removing special protections for certain types of health information.
- **Technological solutions**—Plans called for standardized approaches to authorization, authentication (consumer, provider, health plan, etc), access, and audit; patient identification systems; segmenting data within EHRs; terminology standards; transmissions security standards; and securing data at rest.
- **Education and outreach**—All of the plans called for education and outreach programs directed to consumers, providers, health plans, and other potential exchange partners.

1.1.1 Scope of State IPs

The scope of the final IP in each state report is to identify and prioritize state and regional implementation plans for solutions that address barriers to electronic health information exchange. The content of the plans and the priority assigned to solutions vary across the states depending on the factors described above. Plans include a statement of purpose, key milestones, tasks, timelines, and a budget. Also, the plans include a discussion of lead responsible parties, feasibility, and limitations. The intent of the planning task is the creation of a practical tool that will facilitate taking the next step on the path toward incorporating privacy and security protections into the adoption of electronic health information exchange in each state and territory.

This summary of the final IPs will provide an overview of plans submitted by the state project teams, identify common approaches to resolving similar problems, and point to ways in which the continued activities in each state can be supported at an interstate or national level.

1.1.2 Limitations of State IPs

Several of the IPs mention uncertainty about funding for the implementation plans as a constraint in considering scope and schedule of the plans. Some plans included securing funding as a critical part of the plan.

Many of the IPs noted difficulty in considering privacy and security solutions in the absence of a practical model of how exchange might occur and identifying where in the process

safeguards can be put into place. The completion of Nationwide Health Information Network (NHIN) prototypes, published interoperability specifications from HITSP, and the development of technical standards may help states understand the functional requirements for electronic health information exchange.

Limitations also included interdependencies with national-level issues that remain to be resolved or addressed, and state and regional uncertainties with the legislative process needed to make changes or modifications to existing laws.

It is important that implementation continue to be a grassroots effort driven by state and local participants so that it continues to develop as a community-based effort rather than an effort that has been imposed upon the states. An important outcome of this project has been the creation of groups nationwide that now embrace the concept of electronic health information exchange and have developed a basic understanding of how it can be implemented in their own circumstances.

1.1.3 Assumptions of State IPs

A critical assumption of the IPs is that they are state-level plans. Key aspects of the plans may be supported, but not driven, by federal initiatives. The plans themselves are developed, initiated, and sustained by key actors in each state. While federal action may simplify some of the states' implementation plans or make some implementation plans easier, most of the plans do not contemplate or anticipate speedy federal action.

An element of this assumption is that consensus can be reached within each state/territory on such topics as model forms and procedures, terminology, and technical standards. It is recognized that some effort must be made to achieve consensus across the states and territories in order to enable interstate exchange.

2. SUMMARY OF PROPOSED SOLUTIONS

The Assessment of Variations and Analysis of Solutions (AVAS) report was the first of 2 final reports produced by the 34 state teams. The solutions presented in the AVAS report expanded on solutions presented in the Interim Analysis of Solutions (IAS) reports produced by the state teams. Implementation plans were created for some of the solutions identified in the AVAS report and were included in this, the second of 2 final reports.

After completing the Interim Assessment of Variations (IAV) report, states continued to collect information from their stakeholders and work group members relating to the 18 scenarios presented in the IAV report. States used this new information to produce their final assessment of variations presented in the AVAS report. As with the interim reports, these final variations were the basis for final solutions reported in the AVAS report, and represented a shift away from the scenarios toward a broader discussion of privacy and security issues organized by topic areas. Additionally, states received feedback on their IAS report from stakeholders, work group members, steering committee members, RTI, and the technical advisory panel, and incorporated those comments into their final solutions.

To ensure continuity between the assessment stage and the solutions stage, nearly all of the state teams included members of their variations work group and legal work group in their solutions work group. Additionally, states added key members to their solutions work group through targeted recruitment of stakeholders with specific subject matter expertise. The composition of the solutions work group often evolved through time, depending on the knowledge and experience required to address particular issues and solutions. During the solutions process, several states merged their solutions work group with their implementation planning work group, making for a fluid transition from solutions to implementation. Table 2-1 illustrates the variety of stakeholder groups that participated in the solutions work group.

In their IAS and AVAS reports, the state teams described an iterative process of solution development, review, validation, and refinement as the method used to identify and propose solutions. Additionally, the states described a vetting process for the proposed solutions that included review by 1 or more of the following: the solutions work group, the legal work group, the steering committee, the broader stakeholder community, consumers/consumer advocacy groups, and key government officials. To prioritize solutions, many states reported using a number of ranking, scoring, and weighting methods for seeking consensus during the priority-setting period.

In most states, preliminary determination of the feasibility of solutions was based on an evaluation of cost, ease of implementation, stakeholder support for the solutions, and time required for implementation. States were asked to make plans for solutions that could be implemented in the short term (12 to 18 months); therefore not all solutions presented in

Table 2-1. Stakeholder Group Participation in the Solutions Work Group

| Stakeholder Group | Number (N = 34) | Percentage (%) |
|--|----------------------------|---------------------------|
| Technology and Health Information Experts | 33 | 97% |
| Privacy and security experts/compliance officers | 28 | 82% |
| Health information technology 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 ^(a) | 5 | 15% |
| Public Health Agencies or Departments | 32 | 94% |
| Providers | 32 | 94% |
| Hospitals/health systems | 31 | 91% |
| Physicians and physician 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% |
| Pharmacists/pharmacy benefits 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 ^(b) | 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/advocates | 21 | 62% |
| Individual consumers | 19 | 56% |
| Medical and Public Health Schools that Perform Research | 25 | 74% |
| Payers | 25 | 74% |
| Employers | 12 | 35% |
| Law Enforcement and Correctional Facilities | 7 | 21% |
| Other^(c) | 5 | 15% |
| Foundations/Other Policy Consultants | 1 | 3% |

^a Examples include "health information directors," "information technology directors," "wireless communications services," and "transcription service."

^b Examples include "radiology," "dental," "chiropractic," "osteopathic," and "nursing."

^c Examples include "state law reform specialist," "regional representation," "medical ethicist," and "school health."

the AVAS report were included as implementation plans in this report. For the most part, states only created implementation plans for solutions that were deemed to be feasible within the allotted time frame and where they were able to identify key players and funding sources.

Section 4 of this report summarizes the state-level solutions that were identified by the state teams, Section 5 summarizes multistate implementation plans, and Section 6 summarizes national-level implementation plans.

2.1 Leadership and Governance Solutions

Twenty-two states identified solutions based on issues relating to leadership and governance. Leadership and governance policies usually varied according to the degree of electronic health information exchange within the state. States with limited electronic health information exchange were more likely to propose governance structures that would consider basic implementation issues, while states with more experience with electronic health information exchange proposed governance structures predicated on the assumption that the technical considerations had already been addressed.

Eight states suggested forming a permanent committee or organizational body to help oversee and guide the development of electronic health information exchange and health information technology (HIT) in their state, as well as assisting in the implementation of privacy and security solutions. These bodies would play a significant role, including developing and monitoring standards for the state, providing education on privacy and security laws, and addressing needs across jurisdictional lines. Many of these 8 states proposed solutions that involved interaction with their state legislature, such as providing recommendations to state legislators and policy makers, and working with the governor's office to draft and pass legislation.

In addition to the states proposing a centralized HIE organization, 10 states identified multiple ways in which increased coordination among those involved with electronic health information exchange—such as providers, payers, technology providers, and clinicians—could enhance the adoption of electronic health information exchange and provide increased privacy and security safeguards.

Although many states have working HIEs in place, the legal status of certain entities that participate in HIEs under the HIPAA Rules and state law is still unclear. Several states reported that they were working to form an HIE, while other states were reluctant to do so without clarification. Despite this uncertainty, many states have functioning exchanges and have developed a variety of solutions for the governance of existing exchanges.

2.2 Practice and Policy Solutions

The need for standardization of business practices, policies, and procedures was cited by most of the states. Suggested solutions to help reduce variation in business practices and procedures included the use of model forms, policies, and processes, as well as common interpretations and applications of the HIPAA Rules.

Variation in the interpretation and application of the HIPAA Rules, especially the definition of *minimum necessary*, emerged as a major theme in the AVAS report. HIPAA was frequently cited as limiting exchange, despite the fact that the HIPAA Privacy Rule allows for the exchange of information for the purposes of treatment, payment, and health care operations without the consent or authorization of the patient. Although some providers may genuinely misunderstand the law, other providers use the HIPAA Privacy Rule as a shield to limit the release of information out of fear of litigation for wrongful or inappropriate disclosure of personal health information.

State teams offered a variety of solutions aimed at reducing variation related to how organizations interpret and apply the HIPAA Rule requirements, especially for consistent application of the *minimum necessary* standard, including educational programs aimed at clarifying the requirements of the HIPAA Rules. The state teams also proposed developing uniform consent and authorization forms, and standard policies, procedures, and training materials regarding use and disclosure of health information in accordance with state privacy laws. State teams also requested national policies, standards, and uniform codes as solutions, as well as additional federal guidance from the US Department of Health and Human Services (HHS) regarding the HIPAA Privacy Rule that would help them come to agreement on a narrower range of interpretations of the *minimum necessary* standard.

Several states noted that the standardization of business associate agreements (BAAs),⁴ as well as other types of agreements, may help reduce or eliminate major obstacles to sharing data between entities. Supplemental provisions in BAAs may be used to define standards for data confidentiality and integrity during end-to-end electronic exchanges and also serve to outline parameters for the interoperable mechanisms used to uniquely identify patients and health care providers between systems. In situations where BAAs are not required, such as for most exchanges between providers, health care plans, and health care clearinghouses, the same kind of provisions may be implemented through other kinds of agreements.

⁴ The states generally used the term *business associate agreement* instead of the regulatory term *business associate contract or arrangement*. Either term is acceptable, but the agreement must be in some form of legally enforceable vehicle, such as a contract, or in the intragovernmental context, a memorandum of understanding. The HIPAA Privacy and Security Rules require covered entities to document 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, memorandums of understanding between agencies. Thus, the term *business associate agreement (BAA)* encompasses both contracts and other arrangements and this term is used in the summary above.

Thirteen of the state teams proposed uniform consent and authorization forms as a means to address when consent or authorization is needed and how it is collected. State teams proposed 3 general designs for consent or authorization documents. The first option would be a uniform consent or authorization form used by all health care entities within the state. The second option would be to offer standardized forms that include certain elements, but may be modified based on institutional preferences. The third option would be to provide model forms and allow institutions to draft their own forms.

2.3 Legal and Regulatory Solutions

Most states cited a need to either amend current state laws or develop and enact new laws to address problematic issues surrounding the privacy and security of electronic health information exchange. States are at various stages in this process. Some states have already introduced bills to their legislatures, while other states are proposing to review, classify, and clarify the interpretation of existing state laws, including identifying laws that apply only to paper records.

Finding and interpreting state laws relating to privacy and security can pose a challenge. In many states, these laws are spread throughout several chapters of state codes. One suggestion was to consolidate these scattered privacy and security laws into a single chapter. Other issues include nonexistent state laws pertaining to privacy and security, laws that apply only to paper records, and laws that are inconsistent with other state laws. Suggested solutions to these issues were to propose specific language to address gaps in state law, offer definitions for terms currently undefined in state law, and update existing legislation to include electronic health information exchange.

In addition to the more general modifications to state law mentioned above, many states proposed amending state law in a more specific fashion. Amendments to state law, as well as proposed new legislation, often dealt with specially protected information or the status of HIEs. Sensitive information generally includes human immunodeficiency virus/acquired immunodeficiency syndrome (HIV/AIDS), mental health, alcohol and substance abuse treatment, sexually transmitted diseases, reproductive services, some services provided to minors, and genetic testing information.

The intersection of federal and state law presented a significant challenge for the states. In addition to the HIPAA Rules, states must also comply with 42 C.F.R. pt. 2, which addresses the confidentiality of alcohol and substance abuse treatment, Medicare and Medicaid regulations, the Clinical Laboratory Improvement Amendments (CLIA), and the Family Educational Rights and Privacy Act (FERPA). While many states referred to 42 C.F.R. pt. 2 as an issue in their variations sections, only a couple of states addressed it in the solutions section. One solution included amending 42 C.F.R. pt. 2 to allow for freer use of secondary data, while another solution included it as a consideration for a law relating to specially

protected information. CLIA and FERPA were not widely addressed, although 1 state developed possible amendments to CLIA to expand the list of permissible recipients of laboratory testing results, while another state recommended aligning FERPA with other federal privacy laws.

Another issue raised by the states was the relationship between Medicaid and non-Medicaid entities within the state. Federal regulations require that disclosure or use of Medicaid data must be limited to “purposes directly concerned with the administration of the Medicaid plan.” While several states proposed legislation to govern the exchange of information between these entities, other states felt the federal government should recommend a solution to resolve this issue.

2.4 Technology and Standards Solutions

In their reports, states described the confusion and misunderstanding among stakeholders regarding appropriate security policies, procedures, and technical solutions, as well as broad misunderstanding regarding what technology was currently available and scalable to the health care industry and consumers. States found that legal standards regarding security are generally not perceived to be adequate or specific enough, and are lacking at the state level. Much of the concern regarding security came from providers who were worried that the entities receiving their data might not have security measures as robust as those of their own organization, and that this might expose them to liability in case of a security breach. Related to this concern was a lack of understanding that security in health care is far more complex than just the adoption of appropriate technical standards.

Thirty-one of the state teams offered solutions to technology-related issues identified in their states. The level of specificity in the solutions varied widely, from general statements that certain technological issues would need to be resolved to very specific and detailed discussions of how to resolve specific issues. For example, 1 report provided 173 specific solutions to 20 technical issues encountered during the creation of an electronic health information exchange program in their state. Another state team developed a set of 19 principles regarding the “4 A’s” associated with electronic health information exchange—authorization, authentication, access control, and auditing—which are specific enough to assist organizations in making decisions regarding electronic exchanges, yet flexible enough to adapt to future changes in the implementation of electronic exchange. The variation in the level of specificity in the solutions reflects the level of technology adoption and use by stakeholders within a given state, as well as the level of advancement of electronic health information exchange initiatives within the state.

Data security emerged as an important issue in almost every discussion regarding the technical issues surrounding electronic health information exchange. Twenty-three of the

state teams addressed issues related to the 4 A's. While some discussions were fairly general, others outlined very specific solutions to these issues.

For the purposes of this project, authentication was defined as *the ability to verify that a person or entity seeking access to personal health information is who he or she claims to be*. Nineteen states included a discussion of authentication issues when referring to data security. One of the issues raised was the lack of standards for authentication between all entities involved in a data exchange. In the absence of generally accepted authentication standards, stakeholders were unable to trust that personal information would only be provided to, or accessed by, the correctly identified users. A solution often proposed was the creation of standard policies and procedures to be used by all participating organizations. Other solutions included the use of technology such as digital certificates, biometric authorization, and role-based access control to ensure an appropriate level of security during the transfer of personal health information.

Information authorization and access control issues were often raised in tandem. Appropriate authorization policies and procedures are necessary to ensure that information access rights are only granted to approved individuals, entities, or software programs, and only for purposes permitted by law and organizational policy. Consumers, as well as the individuals responsible for maintaining their data, are concerned that the level of information shared between individuals or entities is appropriate, and also that the individuals receiving the information are appropriately authorized to view the data. Many states looked to technology, as well as standard procedures and policies, as potential solutions with regards to these issues. One solution to address access control was to use a role-based access scheme, with standard definitions for job titles and roles among those authorized to access the data—including providers, and in some cases, health plans. Individuals would only be able to view certain parts of the data based on their job title or description, allowing for the separation of employees requiring access to clinical data from those requiring only administrative data access.

Information audits refer to policies, procedures, and system functions for recording and monitoring the activity of health information systems. The ability to create review audit trail events related to the transfer of personal health information is a core building block for HIE systems, as well as a requirement of the HIPAA Security Rule. States reported that it was important to ensure that all organizations were monitoring the access of data by users as a safeguard against improper use, disclosure, or modification of personal health data. Suggested solutions to auditing issues include: the creation of guidelines for audit control and proactive monitoring; the use of a time/date stamp when a record is accessed, created, modified, destroyed, or transmitted; periodic tests of system controls that protect against breaches, viruses, or spyware infection; and audit capability for e-mail and other methods of transmitting health information. A few states mentioned that if stringent audit requirements were imposed, additional support staff would need to be hired in order to

maintain, monitor, and analyze the large quantities of data captured by the audit process. Many small providers may not have the funding to hire additional staff, resulting in a barrier to implementation. Although minimum audit requirements are needed to ensure the privacy and security of the data and are required by the HIPAA Security Rule where covered entities are involved, the cost issue must be taken into consideration when determining the appropriate level of audit requirements. The creation of cost-effective, efficient, and automated proactive mechanisms to assist with audit control could help with this issue.

The standardization of data transmission requirements is another issue associated with technology, data security, and privacy. The states found that while the technology exists to ensure the private and secure transmission of data, too often there is little or no communication between organizations regarding standards for electronic transmission or available technical solutions to assist with secure data exchange. Seven of the state teams offered specific technical solutions to encourage electronic health information exchange. Solutions regarding secure transmission included the development of standard policies and procedures for the encryption and transmission of electronic data, including the development of a single set of regulations governing the parameters for electronic health information exchange; the clarification of rules governing the use of electronic signatures and public key infrastructure; and the development of a secure web portal for health data exchange. Solutions related to secure electronic messaging between entities include enforcing the use of encryption when e-mailing personally identifying information, adoption of scalable technology to accommodate secure transmission of data, and the creation of a consensus framework for a shared secured messaging platform, including technical and functional requirements.

The ability to accurately identify patients across systems was an issue in many of the states, with 16 state teams suggesting technical solutions to this issue. 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 matching criteria to ensure that patient records remain confidential. States suggested creating standards for matching that included minimum, as well as optional, data elements. Specific solutions included establishing biometrics as the preferred method of verifying the identity of patients, creating model policies and procedures to ensure appropriate capture of patient identifiers, and developing a master patient index with patient identification algorithms to facilitate the accurate exchange of information.

The segmenting of specially protected data was another technology issue raised by the states. Currently, because state and federal laws require additional consent, authorization, or other considerations when transmitting specially protected data, many states simply do not send any of the information associated with these cases. 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. One solution was to

require opt-in/opt-out procedures for patients and methods for capturing and transmitting that information within and between systems. Technology-based solutions to segmenting the data included the use of filters to suppress data access to end users, increasing layers of computer security, using flags within databases to identify specially protected information, and notifying end users that some specially protected information has been blocked. However, technology solutions tend to require extensive planning and programming and have the potential to increase workflow burden on providers.

Although the use of BAAs and the process for managing and obtaining appropriate authorization were raised primarily as policy issues, there are important technology implications. Seven states noted that the policy discussions about the standardization of BAAs and other data use agreements to share data between entities must include discussion of the implications of policy decisions for the technology requirements necessary to implement and manage the dictates of the policies in an electronic environment. BAAs define standards for data confidentiality and integrity during electronic exchanges and also serve to outline parameters for the interoperable mechanisms used to uniquely identify patients and health care providers between systems. Six state teams identified the need to discuss the technological implications of obtaining and managing consent and authorization requirements in EHRs and/or in HIEs. With the move toward electronic health information exchange, the patient's consent or authorization to participate in an HIE must be captured in the electronic record. The ability to capture consent or authorization uniformly within an electronic system also enables the transmission of that data between entities.

Advances in technology have allowed consumers to be more directly involved in their care. For instance, 3 state teams are considering systems that would allow consumers to direct where and how much of their health record data is sent. This concept draws the consumer 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 consumer's care back to a dialogue between the consumer and his/her health care provider or organization.

Individual consumer involvement in the health care information exchange may result in an increased awareness of privacy and security issues in the general population. Although this model would address many of the current issues related to electronic health information exchange, it raises other issues that are just as complex. For instance, what happens if patients block access to data that could save their life? And, how do you involve consumers who do not have access to computers or do not understand the complexity of issues that would need to be considered when making these decisions? These questions and others must be taken into consideration when creating a consumer-oriented model. There are resources, such as the guidelines for personal health records described by the Markle Foundation's Connecting for Health report and person-centered regional health information

organizations such as the Louisville Health Information Exchange, which can be utilized when considering these issues.

2.5 Education and Outreach Solutions

Twenty-nine state teams recommended some form of education program or training materials to increase knowledge within stakeholder groups. The education and training would be aimed not only at consumers, but also at providers, health plans, administrative staff, first responders, and law enforcement.

Many consumers lack knowledge of their existing health information privacy rights, as well as current security obligations and practices of health care organizations. Consumers not only need to be educated about their rights, but also need to understand who can access their information and for what reasons. This lack of knowledge is likely to create a significant trust issue as electronic health information exchange is implemented, since privacy and security rights and obligations are not yet well defined for electronic health information exchange.

Educational programs could not only be used to increase consumer involvement in the management of their own health data, but also to inform them about their rights, advantages of electronic health records, authorization/consent issues, and recent developments in technology and security. Many states recommended methods such as leveraging existing consumer education venues such as doctor's offices, clinics, and established websites, hosting focus groups, creating educational packages, and producing frequently asked questions documents as ways of educating the public.

Another suggested solution calls for the establishment of a centralized method to develop and distribute educational materials concerning patient rights and responsibilities, as well as enabling consumers to protect and monitor their own health care information. Educational materials should include information regarding the technology used in an HIE to help consumers understand the technology as well as their ability to interact with it.

While consumer education is a major concern, many states reported misunderstanding and distrust of electronic health information exchange within the provider community as well. States found that many health care professionals do not have an accurate or complete understanding of HIPAA regulations or relevant state laws. States reported that educating and training providers was essential, including educating providers on state and federal privacy and security laws and regulations and the types and benefits of HIE systems. Additionally, states suggested providing continuing education for all professional health care staff in organizations that use an HIE system to ensure that proper privacy and security procedures are followed.

Although education of health care providers and the general public dominated states' 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 were either 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. States suggested creating education and outreach materials targeted to these groups. Specific solutions include conducting joint training events for law enforcement and public health, targeting training/educational programs for law enforcement and public officials (including judges) to clarify HIPAA requirements, and educating health plans and employers on the benefits and use of data for research purposes.

3. REVIEW OF STATE IMPLEMENTATION PLANNING PROCESS

The outline of the Interim Implementation Plan report, distributed in draft form in September 2006, provided guidance to state project teams regarding the process to follow when developing implementation plans. Additional guidance emphasizing the need for detailed, actionable plans was provided during regional meetings and WebEx conferences held in October and November of 2006. The process of developing state-level implementation plans as distilled from this guidance was to assemble a work group, review solutions reported in the Interim Analysis of Solutions (IAS) report, and select a subset of solutions to address based on an assessment of feasibility. Work groups or subgroups of relevant stakeholders were to subsequently meet and develop implementation plans, considering such factors as affected stakeholders, potential sources of funding, staffing, timelines, and barriers to implementation. Mirroring the recursive design of the variations assessment and solutions development stages of the project, relevant stakeholders were to be engaged to review and comment on draft implementation plans, providing insight from additional perspectives and ensuring that the plans were acceptable to affected stakeholders and the larger community.

3.1 Formation of Implementation Planning Work Groups

State teams employed a variety of approaches to ensure continuity between the earlier stages of the project and the implementation planning stage through the formation of their implementation planning work groups (IPWGs). State teams were keenly aware of time constraints, and many of them explicitly reported a desire to ensure efficiency by eliminating the learning curve that would be associated with bringing new members into the project at the implementation planning stage. All state teams included members from their other project work groups and committees on their IPWGs. Three state teams reported that their solutions work group simply continued on in the capacity of their IPWG. Six state teams reported that they had combined the solutions work group and the IPWG preemptively, during the earlier solutions development stage. Six state teams reported that their IPWG included their solutions work group in its entirety. Three state teams formed their IPWG by combining their variations work group with their solutions work group. One state team went so far as to include all members of their existing project teams on the IPWG, including their steering committee, variations work group, legal work group, solutions work group, and consumer advisory committee. One state team merged the IPWG with the steering committee. Few state teams reported adding members with no prior experience with the Health Information Security and Privacy Collaboration to their IPWGs. Those that did noted that they made a significant effort to familiarize these new members with project concepts and activities. All of these approaches effectively carried forward the knowledge and experience gained through the earlier stages of the project.

The number of IPWG members per state team varied considerably, from a low of 3 to a high of 119. The average IPWG consisted of 27 members. Six state teams reported IPWGs with fewer than 10 members, choosing to form small, nimble groups of highly knowledgeable people who could communicate easily and act quickly. Four teams reported IPWGs with more than 50 members.

All 34 state teams reported the stakeholder groups that these IPWG members represented (see Table 3-1). On average, IPWG membership represented 15 of the 34 stakeholder groups⁵ per project team. The most frequently represented stakeholder groups among IPWG members were technology and health information experts (97%), providers (91%), and legal counsel/attorneys (88%). Consumers (74%), medical and public health schools/research (71%), and other government (71%) were represented on a large majority of teams.

3.2 Process Used to Identify, Prioritize, and Develop Implementation Plans

All state project teams assembled an IPWG and narrowed the focus of implementation planning by reviewing the IAS report and identifying a suitable subset of solutions to pursue. During the initial assessment of feasibility, teams considered factors such as ease of implementation, cost, the availability of technology, compatibility with the current legal and regulatory environment, and the readiness of affected stakeholder communities to implement proposed solutions. Sequencing implementation plans so that work accomplished by earlier implementations would be available when needed by later implementations was occasionally cited. Many relied on ranking, scoring, and weighting methods to identify a small set of solutions to consider, building consensus among large groups with broad representation. A few state teams were guided by the decisions of the steering committee or core team to determine feasibility and narrow the focus of the IPWG.

State teams frequently reported circulating the IAS report prior to IPWG meetings, along with worksheets and document templates to capture information on priorities and implementation planning steps. Many state teams reported posting these documents, as well as preliminary implementation plans, on web portals to promote broader stakeholder involvement.

⁵ RTI initially defined 18 stakeholder groups. The number of group types increased in response to the reporting preferences of state teams. Tables 3-1 and 3-2 display 34 stakeholder groups and 4 additional summary categories.

Table 3-1. Stakeholder Group Membership in Implementation Planning Work Groups

| Stakeholder Group | Number (N = 34) | Percentage (%) |
|--|----------------------------|---------------------------|
| Technology and Health Information Experts | 33 | 97% |
| Health information technology consultants | 27 | 79% |
| Privacy and security experts/compliance officers | 25 | 74% |
| Technology organizations/vendors | 19 | 56% |
| Regional health information organizations | 17 | 50% |
| Electronic health records experts | 17 | 50% |
| Quality improvement organizations | 16 | 47% |
| Health information management organizations | 14 | 41% |
| Other health data and technology experts ^(a) | 5 | 15% |
| Providers | 31 | 91% |
| Hospitals/health systems | 30 | 88% |
| Physicians and physicians groups | 26 | 76% |
| Professional associations and societies | 22 | 65% |
| Clinicians | 20 | 59% |
| Community clinics and health centers | 18 | 53% |
| Mental health and behavioral health | 12 | 35% |
| Pharmacists/pharmacy benefit managers | 9 | 26% |
| Federal health facilities | 8 | 24% |
| Emergency medicine | 8 | 24% |
| Long-term care facilities and nursing homes | 8 | 24% |
| Homecare and hospice | 8 | 24% |
| Safety-net providers | 8 | 24% |
| Laboratories | 7 | 21% |
| Other health care providers ^(b) | 4 | 12% |
| Legal Counsel/Attorneys | 30 | 88% |
| Public Health Agencies or Departments | 28 | 82% |
| Consumers | 25 | 74% |
| Consumer organizations and advocates | 21 | 62% |
| Individual consumers | 17 | 50% |
| Medical and Public Health Schools that Perform Research | 24 | 71% |
| Other Government | 24 | 71% |
| Medicaid/state government except public health | 24 | 71% |
| County government | 7 | 21% |
| Payers | 21 | 62% |
| Employers | 13 | 38% |
| Other^(c) | 5 | 15% |
| Law Enforcement and Correctional Facilities | 4 | 12% |
| Foundations/Other Policy Consultants | 1 | 3% |

^a Examples include "health information directors," "information technology directors," "wireless communications services," and "transcription service."

^b Examples include "radiology," "dental," "chiropractic," "osteopathic," and "nursing."

^c Examples include "state law reform specialist," "regional representation," "medical ethicist," and "school health."

Implementation planning was usually conducted through a series of face-to-face meetings and conference calls. Typically, the first meeting established the smaller set of solutions for which implementation plans would be developed and a framework for brainstorming sessions to be conducted by smaller breakout groups. A number of teams sorted issues into topic areas for consideration by these smaller breakout groups. Some examples of the topics areas employed by the state teams include the following:

- Operational and legal
- Consent management and specially protected information management
- Consent and the 4 A's
- Technical, legal, and educational
- Financial, technical, logistical, and educational
- Legal, educational, and federal
- Consent, leadership, accreditation, patient engagement, and patient identification
- Legislation, education, and standards and best practices

These smaller subgroups met, developed implementation plans, and reported back to the larger group. Implementation planning usually required a series of meetings to complete the process of review, validation, and refinement. Typically, 2 or 3 face-to-face meetings were held but as many as 15 meetings were reported. A few state project teams reported that they conducted research between meetings. In most instances, the steering committee reviewed and approved the final IP report before it was submitted.

In addition to facilitated meetings, input was collected through online forums, threaded discussions, interviews with key informants, focus groups, questionnaires, WebEx meetings, and e-mail.

A small number of teams reported that they reassessed the feasibility of solutions after the national meeting, held in early March 2007. These teams reported that the selection of solutions to be implemented was further informed by discussion with other state teams, relevant Agency for Healthcare Research and Quality webcasts, and additional research.

While all state teams acknowledged the need for detailed, actionable plans that consider leadership, personnel, cost, and timelines, a few reported that their efforts were ongoing at the time the final IP report was due.

3.3 Stakeholder Engagement and Involvement

Thirty (88%) of the 34 state teams were able to involve the stakeholder community in vetting and evaluating their implementation plans. Teams typically reported distributing their Interim Implementation Plan reports as the basis for meetings held to capture additional insight, particularly from affected stakeholders. One state team reported the

participation of their stakeholder community of 60 volunteers. Another state team posted its draft implementation plans on its wiki website and reported receiving stakeholder input. Yet another named 119 members in their IPWG, and described it as including “HIE [health information exchange] stakeholders from across the state,” effectively including the broader community in the work group itself.

A few state teams noted incomplete stakeholder involvement as limiting their implementation plans. One state team reported meetings scheduled to be held in May 2007 to address this issue. Another state team noted a lack of consumer involvement in vetting and evaluating implementation plans. A third state team acknowledged the lack of involvement from the Veterans Administration, despite the team’s efforts to engage them in the process.

Table 3-2 shows the number and percentage of the 34 teams that engaged each stakeholder group in implementation planning through community outreach. Providers and technology and health information experts were engaged by 85% of the state teams. Legal counsel/attorneys and other government were engaged by 74% of the state teams. Public health agencies or departments and consumers were each engaged by 71% of the state teams. Payers (health plans) and medical and public health schools that perform research were engaged by approximately two-thirds of the state teams.

Table 3-2. Stakeholder Groups Engaged in Implementation Planning Through Community Outreach

| Stakeholder Group | Number (N = 34) | Percentage (%) |
|--|----------------------------|---------------------------|
| Providers | 29 | 85% |
| Hospitals/health systems | 28 | 82% |
| Physicians and physicians groups | 26 | 76% |
| Clinicians | 22 | 65% |
| Professional associations and societies | 19 | 56% |
| Community clinics and health centers | 15 | 44% |
| Mental health and behavioral health | 14 | 41% |
| Emergency medicine | 11 | 32% |
| Homecare and hospice | 10 | 29% |
| Pharmacists/pharmacy benefit managers | 10 | 29% |
| Long-term care facilities and nursing homes | 9 | 26% |
| Safety-net providers | 8 | 24% |
| Other health care providers ^(a) | 8 | 24% |
| Federal health facilities | 6 | 18% |
| Laboratories | 6 | 18% |
| Technology and Health Information Experts | 29 | 85% |
| Privacy and security experts/compliance officers | 22 | 65% |
| Health information technology consultants | 22 | 65% |
| Quality improvement organizations | 20 | 59% |
| Regional health information organizations | 16 | 47% |
| Electronic health records experts | 16 | 47% |
| Health information management organizations | 14 | 41% |
| Technology organizations/vendors | 14 | 41% |
| Other health data and technology experts ^(b) | 4 | 12% |
| Legal Counsel/Attorneys | 25 | 74% |
| Other Government | 25 | 74% |
| Medicaid/state government except public health | 25 | 74% |
| County government | 7 | 21% |
| Public Health Agencies or Departments | 24 | 71% |
| Consumers | 24 | 71% |
| Consumer organizations and advocates | 21 | 62% |
| Individual consumers | 16 | 47% |
| Payers | 23 | 68% |
| Medical and Public Health Schools that Perform Research | 22 | 65% |
| Employers | 16 | 47% |
| Law Enforcement and Correctional Facilities | 8 | 24% |
| Other^(c) | 3 | 9% |
| Foundations/Other Policy Consultants | 1 | 3% |

^a Examples include "radiology," "dental," "chiropractic," "osteopathic," and "nursing."

^b Examples include "health information directors," "information technology directors," "wireless communication services," and "transcription service."

^c Examples include "state law reform specialist," "regional representation," "medical ethicist," and "school health."

4. IMPLEMENTING STATE-LEVEL SOLUTIONS

For the final Implementation Plans (IPs), state teams narrowed their focus and increased the depth of their implementation plans. As the project has progressed, some states have already succeeded in accomplishing initial tasks. For example, 4 state teams have succeeded in getting legislation introduced and passed. Another state team has received responses to its request for proposals and plans to award a contract to establish a state health information exchange (HIE)/health information technology (HIT) resource center in April 2007. Others have received commitments for funding from private foundations or corporations. These early successes serve as the foundation for future progress and offer models for other states to emulate.

In reviewing the IPs, it should be noted that state teams made a variety of assumptions, including the availability of financing, the achievement of buy-in from other stakeholders, a favorable political climate, and the availability of suitable technology options. In some instances, these assumptions were very sweeping, envisioning the creation of a state health information network or major efforts by federal agencies. The IPs discussed in this section are categorized by the primary type of solution being addressed in the plan. For example, amending the language of the state code to mirror the HIPAA Privacy Rule can be found in Section 4.3, Implementing Legal and Regulatory Solutions, even though such a plan may include educational or policy components.

4.1 Implementing Leadership and Governance Solutions

4.1.1 Creation of New Oversight Bodies

In many instances, this project represents the first coordinated effort to examine HIE/HIT at the state level, although some states had structures in place prior to the initiation of this work. There is a need to build or create new oversight bodies in states that had previously been examining HIE/HIT, so that implementation plans will be executed, and so that there is a continuing leadership to support HIE and HIT initiatives.

One team clearly elaborated on the need for leadership:

Barriers due to variations in information technology development from organization to organization could be alleviated by a standardized approach for information exchange. Variations in the organizational culture of physical/paper records, the culture of actions based on risk aversion and/or comfort rather than standards, the culture of market competition, the culture of organization type such as clinics vs. hospitals, public vs. private, etc, and the culture of ownership of data and not sharing it all would be affected by the creation of a level playing field brought about by benchmarking.

Eleven state teams composed implementation plans to create new oversight bodies. Generally, the creation of a new body requires 3 steps. First, the body's authority must be

established, either through the governor or the legislature. Second, members are recruited and appointed, and the body establishes bylaws. Finally, the new members create a work plan, building from the executive/legislative mandate.

The new oversight bodies were assigned a wide range of tasks associated with facilitating electronic health information exchange, including issuing policy guidance, drafting technology requirements, offering interpretations of state law, and coordinating educational and outreach programs. Overall, the bodies are to provide support for HIE/HIT initiatives at the state level. Other specific tasks included the following:

- Coordinate and implement any emerging federal standards (3 states).
- Coordinate existing HIT initiatives to avoid duplication of effort.
- Utilize a systematic, comprehensive approach to promoting the benefits of electronic health information exchange.
- Resolve disputes between entities participating in an HIE.
- Communicate with tribal nations.
- Offer adoption incentives.
- Compile and promote best practices.

4.1.2 Leveraging Existing Leadership Efforts to Implement Solutions

There are 3 general categories of existing leadership efforts that may be leveraged to implement solutions. First, states may have had some sort of e-Health leadership entity prior to HISPC, usually a committee created by the governor to examine HIE/HIT. Second, there are state teams that are being led by a coalition of existing groups, such as the state department of health, a public health institute, or a not-for-profit group, that plan to select a leader. Finally, there are state teams that plan to pass off work to an existing state agency, usually the state department of health.

Five states outlined specific implementation plans to facilitate this transfer of responsibility. This is not to say that other state teams did not anticipate the need to transfer formal control for continuing efforts, but rather that they assumed the transfer of authority would occur, or that the existing body was leading the HISPC efforts and would continue with future efforts. In addition, state teams often assumed that the new leadership bodies described in Section 4.1.1 would oversee the implementation of other solutions. Indeed, the oversight bodies were frequently seen as a precursor to subsequent implementation work and are a high priority for states that planned for them.

4.1.3 Creation of New Governance Structures

In addition to the large oversight bodies described in Section 4.1.1, state teams also created plans for independent or subsidiary committees designed to oversee certain aspects of HIE/HIT, such as a technical committee, legal advisory committee, or education and

marketing team. As with the creation of new oversight bodies, the scope of the governance committees' authority must be established, the members recruited and appointed, and a work plan developed in accordance with the commissioning authority.

Two state teams planned their governance structures as part of their new oversight body. Each planned technology, education, and legal advisory committees, with the committees reporting to the oversight body's steering committee. Other state teams did not draft a specific implementation plan for subsidiary committees, but included technical, legal, and educational tasks when creating their oversight body.

One state team outlined responsibilities for a financial group and a clinical group. The financial group was tasked with developing sustainable business models, to ensure return on investment for providers participating in an HIE. The clinical group is to draft quality benchmarks to ensure that the electronic health information exchange initiatives are improving quality of care and reducing school and work absenteeism. Although the state team did not clearly identify a responsible party for these 2 committees, their creation demonstrates a commitment to building a foundation of support for electronic health information exchange and HIT.

4.1.4 Analysis of Feasibility and Barriers to Implementation of Leadership and Governance Solutions

State teams generally rated their implementation plans as quite feasible. In such instances, they pointed to past successes in fundraising and collaborating with providers on state standards, high levels of stakeholder engagement, and commitment from the executive and/or legislative branch. One state team expressed reservations about its ability to raise the funds necessary to implement HIE/HIT initiatives and 2 others noted that the cost of forming the leadership body was not insignificant, but felt they had the necessary political support.

Funding was the most frequently cited barrier to success, mentioned by 13 state teams. As mentioned previously, some state teams have secured funding for primary initiatives, but there is still uncertainty about return on investment. Four state teams indicated the need to demonstrate the financial sustainability of an HIE. If politicians and providers do not feel they will receive a return, either in increased efficiency, improved quality of care, or some other outcome, they will be reluctant to invest. One state team noted that there is a critical mass required to begin to see returns. However, it is not clear how large this critical mass might be.

Another major barrier to implementation was lack of stakeholder participation or lack of stakeholder buy-in, including consumers, payers, and providers. A collaborative process may take more time, but will likely yield more sustainable results. Similarly, 4 states cited resistance to change as a barrier to implementation.

Other barriers included

- lack of standards for HIT (3 states),
- lack of staff (4 states),
- competing priorities (2 states),
- lack of technology options,
- different levels of HIE development, and
- inability to reach small or rural providers.

Barriers were often presented in a bulleted list without further explanatory information. Also, barriers are not limited to those presented in the IPs; some barriers tend to apply to the entire plan even if not specifically referenced with respect to governing bodies. For example, 2 states have legislatures that meet every 2 years, limiting the team's ability to get legislation passed that might be required to sanction the oversight and governing bodies. Similarly, multiple states have biennial budgets, which may limit their ability to secure funding immediately.

4.2 Implementing Practice and Policy Solutions

Overall, implementation plans for policy and practice solutions were not developed independently. These solutions were often incorporated under other plans, such as governance and leadership or education. As these solutions were often subsidiary to others, they are often not well-explored in the final IPs. Despite this, policies represent a crucial component in facilitating electronic health information exchange, as they are more easily implemented than legislative changes, and are more readily changed in the event that they do not have the desired effect.

4.2.1 Consent and Authorization

Eight state teams generated an implementation plan related to consent and authorization.⁶ As 1 state team observed, "Broad variation in opinion exists among stakeholders as to what is required legally, what is appropriate for risk management purposes, what constitutes the best public policy and what is feasible from an implementation perspective." This array of considerations indicates a need for work and consensus around the issue of consent. One state team proposed a comprehensive consent management process, designed to build consensus and facilitate electronic health information exchange. This process involves creating a leadership body, securing funding, drafting use cases, assessing policies and legal requirements, and educating consumers and providers. This is by far the most ambitious of the implementation plans related to consent.

⁶ The terms *consent* and *authorization* may have different meanings in the context of various state and federal laws. Here, the terms are used to refer to a signed permission of the patient to use or disclose information. A full discussion of the subtleties of the distinctions between the 2 terms is beyond the scope of this report.

On a smaller scale, common consent forms have the potential to facilitate exchange because they can offer providers assurance that they are complying with state and federal laws, and that exchange partners are also following the same protocols. One state team planned to combine the creation of a common consent form with educational efforts to inform providers as to when consent is required. Model consent forms from a variety of sources already exist, and so states will not have to begin from scratch when drafting model or uniform consent forms. However, the state teams did not identify previous work that could be used as models for their forms, and did not indicate how long the process of drafting a form might take.

4.2.2 Interpretation and Application of Federal Regulations

State teams offered limited implementation plans related to the interpretation and application of federal regulations. One state proposed standard operating procedures to reduce variation caused by differing interpretations or applications of the HIPAA Privacy and Security Rules. Another state team proposed creating a state-mandated HIPAA Privacy Rule training course.⁷

State teams more frequently addressed the interpretation and application of federal regulations through a legislative solution, opting to amend state law to mirror the language of the HIPAA Privacy Rule and establish similar exceptions for using and disclosing information for the purposes of treatment, payment, and health care operations, without consent or authorization. See Section 4.3 for additional information on legal solutions.

Other federal laws, including 42 C.F.R. pt. 2, which governs alcohol and drug abuse treatment records, the Clinical Laboratory Improvement Amendments (CLIA), the Family Educational Rights and Privacy Act (FERPA), and the Employee Retirement Income Security Act (ERISA), were identified as potential barriers to exchange, but they were not addressed in the state-level implementation plans. See Section 6 for additional discussion of federal solutions.

4.2.3 Exchanging Sensitive Health Information

Sensitive health information generally includes alcohol and substance abuse, mental health information, and human immunodeficiency virus/acquired immunodeficiency syndrome (HIV/AIDS) status, although definitions vary from state to state. At the federal level, alcohol and substance abuse treatment information is governed by 42 C.F.R. pt. 2. The HIPAA Privacy Rule also provides additional protection for psychotherapy notes. (As noted in Section 4.2.2, none of the states addressed 42 C.F.R. pt. 2 in their implementation reports.) Many states have additional laws that similarly govern the exchange of specially protected information, although their definition of *specially protected information* may vary slightly.

⁷ Under the HIPAA Privacy Rule, a covered entity must train its workforce on the entity's privacy policies and procedures as necessary for employees to carry out their job responsibilities.

For example, 1 state includes developmental disabilities on the list of specially protected information, and another includes genetic testing results.

Four state teams drafted implementation plans related to specially protected health information. Three states mentioned mental health information, 2 mentioned HIV/AIDS information, and another referred to specially protected information more generally. One state team planned to use the continuity of care document⁸ as a standard for transferring specially protected health information. Another state team proposed an educational program for mental health providers to fully apprise them of current state law and the requirement of the HIPAA Privacy Rule to obtain patient authorization for the use or disclosure of psychotherapy notes.

4.2.4 Standardized/Model Documents

Six state teams proposed some sort of standardized or model document. The most frequently cited document was the business associate agreement (BAA), addressed by 4 state teams. One state team planned to include education to explain when and why a BAA is required.⁹ Two state teams planned to implement standardized contractual agreements to be used to facilitate exchange. Two other state teams stated that they would develop model documents, but did not elaborate as to what they might be. Overall, these plans did not include further discussion on this topic. As noted above in the discussion on common consent, standardized/model documents already exist, and state teams may build from these existing efforts rather than starting entirely anew.

4.2.5 Exchange of Medicaid Data

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.”¹⁰ 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.¹¹ 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

⁸ The continuity of care document emerged from the harmonization of the continuity of care record and the clinical document architecture. The two were harmonized to promote interoperability.

⁹ The HIPAA Rules specify who should sign a BAA and under what circumstances. The term *business associate* is defined in 45 C.F.R. § 160.103.

¹⁰ 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.

¹¹ 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.

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.

Four state teams mentioned exchange of data with Medicaid. Three of these solutions were included in the context of larger implementation plans and were not well-developed. The most developed of the plans included a proposal for a pilot program for Medicaid data exchange. The state team drafted technical standards for the physician's office and the network used for exchange purposes, and specified administrative safeguards. The state team also included Medicaid as a topic for inclusion in HIT initiatives moving forward, and as an issue for interstate collaboration.

One state team planned to establish rules and guidelines to facilitate the flow of information between the Medicaid program and non-Medicaid providers. A second state intended to use the continuity of care document as the standard for exchanging Medicaid data. The third state is in a unique situation because of a recent amendment to its state Medicaid plan that requires additional reporting of information by physicians. Beneficiaries can receive an enhanced benefits package if they meet certain requirements. The state team is working to fully understand the implications of these changes on privacy and security.

4.2.6 Data Exchanges with Public Health

Electronic transmission of data to public health authorities represents an opportunity to improve disease reporting and management. Four state teams mentioned public health in their implementation plan. In 1 state, public health has been included from the beginning and is a major part of the plans going forward. An additional 2 teams planned to include training for public health officials regarding the HIPAA Privacy Rule and state law, and to assess opportunities for future collaboration. Finally, 1 team included public health reporting as part of their foundation for interstate exchange.

4.2.7 Data Exchanges with Law Enforcement

In areas with limited numbers of health care providers, law enforcement can offer a valuable resource in providing care, especially in emergency situations. Two states proposed educational efforts for law enforcement officials, with 1 specifically planning to highlight communicable disease risks. Another 2 states included law enforcement in legal implementation plans, planning to modify or create new legislation that addressed law enforcement participation. Finally, 1 state sought to work through its new oversight body to improve communication with law enforcement, particularly with respect to disclosing records to law enforcement.

4.2.8 Other Practice or Policy Solutions

Three state teams proposed creating a committee or governance structure to oversee policy issues. These authorities would issue policy guidance, generate standard operating procedures, and standardize documents.

Other solutions included

- drafting standard operating procedures regarding general confidentiality of all information, including financial information and personal health information;
- developing new regulations and policies to govern electronic health information exchange in the event of a bioterrorism attack;
- creating a repository of best practices and technology solutions (2 states);
- setting standards for privacy and security expertise within organizations; and
- developing a predefined protocol or decision pathway for which elements of personal health information can be shared with certain entities.

4.2.9 Analysis of Feasibility and Barriers to Implementation of Practice and Policy Solutions

As these solutions were frequently part of larger plans, it is difficult to assess the feasibility of individual components. However, state teams felt their plans to be moderately feasible, but they recognized the challenge of achieving consensus on standardized forms, policies, or procedures.

As was often the case, funding was a commonly identified barrier to implementation. Other challenges included

- buy-in from providers (6 states),
- inconsistency between state and federal law,
- complexity of systems, and
- resistance to change (2 states).

4.3 Implementing Legal and Regulatory Solutions

4.3.1 Amending State Law

Amendments to state law fell into 3 broad categories: amending state law to mirror federal law, to remedy state-specific concerns, and to address consistency more broadly. Teams felt that these changes would reduce variation in business practices and facilitate electronic health information exchange.

Five state project teams drafted plans to align state law with federal law, usually the HIPAA Rules. Two teams made general reference to federal law, 1 explicitly referenced HIPAA, and the other 2 planned to incorporate the HIPAA Privacy Rule treatment, payment, and health care operations exemption from patient consent or authorization into state law.

State-specific concerns stemmed from language (or lack thereof) in state law. Ten state project teams created implementation plans to amend state law. In 4 instances, the teams composed language that could be used to amend the law. Issues addressed by the proposed amendments concerned consent/authorization; interactions between Medicaid and non-Medicaid providers; treatment; HIE and minors; medical record confidentiality; and specially protected information, including genetic testing results, communicable diseases, and mental health. Two states' privacy laws made no mention of electronic exchange and applied only to paper documents. Similarly, another state found that some laws did not sensibly apply to electronic exchange and planned to update the laws accordingly. A fourth state project team had a more narrow focus, planning to update a law to allow for electronic signatures when prescribing medications.

With regards to consent and authorization, some state project teams were heading in different directions. One team planned to amend its stringent consent law, but in such a way as to maintain protections. Another state planned to allow the sharing of more data, such as communicable disease information and pharmacy data, without patient consent or authorization, provided the HIPAA Privacy Rule was adhered to. A third state proposed legislation that would allow for research on health plan data without consent or authorization and for sharing of pharmacy data regarding medications without consent or authorization.

Three project teams planned to amend state law in order to correct inconsistencies. Two project teams observed that definitions were not consistent from one law or regulation to the next, resulting in confusion and variability in business practices. The third team's planned amendments were aimed at resolving inconsistent regulations for information exchange for general health information and specially protected information.

Listed below are 2 sample implementation plans for amending or drafting new legislation.

Example Implementation Plan 1:

- Identify a project leader.
- Identify and enlist the assistance of someone familiar with and experienced in introducing new legislation and successfully resulting in the passage of new law.
- Identify stakeholders who will support the draft legislation and be able to articulate the benefits of the proposed changes.
- Identify and enlist individuals or organizations to draft the legislative change.
- Draft legislative change.
- Review draft legislation with legal experts and stakeholders.
- Develop a roll-out plan for effecting change in state law (e.g., identify a state legislator who will sponsor the bill and help shepherd it through the legislative review process). Include key dates for being considered in a legislative session.
- Implement the roll-out plan.

Example Implementation Plan 2:

Preparing for Legislative Change

- Identify legislative sponsor(s), state health department sponsor, relevant advocacy groups, and content expert(s).
- Develop case for necessity of proposed changes.
- Hold listening sessions to discuss proposed changes.
- Refine proposed changes to reflect stakeholder input.
- Fine-tune specific legal changes identified (i.e., develop sample language).
- Request and review legislative draft.
- Obtain fiscal note.
- Identify support and opposition.
- Openly involve advocates representing individuals with specially protected health conditions.
- Develop plans to address concerns.
- Build support for proposed changes.
- Monitor, manage, and nurture proposed changes through the legislative process.

Building Stakeholder Involvement

- Identify stakeholder groups that can provide input.
- Identify areas where external input is most critical.
- Align stakeholders with areas requiring input.
- Invite input from a broad set of stakeholders.
- Seek endorsements from involved stakeholder and advocacy groups.

Communicating the Proposed Solution

- Identify all stakeholder groups impacted by the proposed changes.
- Determine communication needs of each group.
- Build communications plan for each impacted stakeholder.
- Develop communications pieces.
- Build website for project updates and all communication materials.
- Deliver communications throughout the legislative process.

Training and Education

- Determine how law changes will impact organizational policies and procedures.
- Develop training materials to communicate law changes to providers and health plans.
- Develop outreach materials to communicate changes to consumers.
- Build website with training materials and consumer information.

Next Steps

- Complete the legal reconciliation process.
- Develop administrative rules if necessary.
- Continue study of the amended statute and its impacts on electronic health information exchange.
- Maintain website with training and educational materials.

4.3.2 Introducing New State Law

State teams suggested a wide range of new state laws to protect the electronic transmission of health information. Eleven state teams' implementation plans include recommendations for new legislation. An additional 3 state teams plan draft recommendations to be provided to their legislatures, and are currently in the process of examining the need for legislation in a variety of arenas. Proposed recommendations included the following:

- Provide immunity or protection from liability (3 states).
- Establish the legal status of health information exchanges (HIEs) (2 states).
- Mandate operating procedures for a state health information network.
- Introduce a law regarding medical identity theft (protections and recourse).
- Introduce a mandatory reporting law (must notify all affected individuals in the event of a security breach).
- Implement an electronic health information exchange act to govern electronic health information exchange at the state level.
- Establish a law to support the use of digital signatures.
- Allow the display of name and basic demographic information for hospital patients during a catastrophic event.
- Put additional consumer protections for electronic health information exchange in place.

As mentioned previously, these implementation plans were usually not fully developed. The process for passing new laws is nearly identical to the process for amending existing law.

4.3.3 Implementing Other Legal and Regulatory Solutions

The remaining legal and regulatory solutions fell into 2 general categories: consolidating or centralizing state laws and regulations, and considerations of the Stark and Antikickback Laws. Three state project teams planned to consolidate their state laws and regulations governing privacy and security. It was thought that collocating the various pieces of applicable statute would facilitate legal analyses and reduce variation in business practices.

Two state project teams planned to resolve issues related to the Stark and Antikickback Laws. The Stark and Antikickback Laws prohibit physicians from receiving compensation, including nonmonetary compensation, for referrals of Medicare and Medicaid patients. In

2006, the US Department of Health and Human Services (HHS) announced new regulations allowing exceptions for certain arrangements in which (1) a physician receives compensation in the form of items or services (not including cash or cash equivalents) (“nonmonetary remuneration”) that is necessary and used solely to receive and transmit electronic prescription information; and (2) involving the provision of nonmonetary remuneration in the form of electronic health records software or information technology and training services necessary and used predominantly to create, maintain, transmit, or receive electronic health records to facilitate adoption of HIT and EHRs. Although the state project teams did not fully develop their implementation plans for addressing these issues, they planned to do so in subsequent work. Of course, these are federal laws, which cannot be revised by states. The states will have to seek federal action to make appropriate revisions.

4.3.4 Analysis of Feasibility and Barriers to Implementation of Legal and Regulatory Solutions

State project teams generally felt that their legal and regulatory solutions could be implemented, although they identified a number of potential barriers. The most frequently cited barrier was lack of stakeholder support. Nine teams mentioned the need for stakeholder support, although often in different contexts. Some teams felt that general consumer mistrust could hinder the ability to pass legislation, especially when the law concerned specially protected information. Another team observed that although they had developed their implementation plan, they had not assessed consumer buy-in. Finally, project teams were uncertain as to whether they would be able to achieve consensus across different stakeholder groups due to the lack of a common vision or purpose among different categories of stakeholders. One state anticipated resistance to their proposed legislative amendment and included other options for amending state law, as well as an analysis of the risks and benefits of choosing other solutions.

Other commonly cited barriers included those related to the legislative process. Three states have legislatures that meet infrequently and/or for short periods of time. The compressed time frame of these legislative sessions makes it difficult to pass legislation that does not have substantial support from the outset. While some states were confident that they would receive support from legislators, 2 others expressed doubts about their ability to find sponsors for their legislation or achieve consensus with those sponsors.

Several state project teams mentioned funding as a barrier. The legal work required to research and draft legislation related to electronic health information exchange can be expensive, and states may have to rely on discounted legal rates and/or volunteers. Other barriers and concerns considered by states included the following:

- States have different levels of electronic health information exchange development.
- Nonprofits may be prohibited from conducting lobbying activities.

- Legislation may end up inhibiting electronic health information exchange, rather than enhancing it, due to amendments and modifications.
- Special interest groups such as disease-specific advocates and privacy advocates may prefer the status quo and not support legislation aimed at facilitating electronic health information exchange.
- Staff lack experience in drafting legislation related to electronic health information exchange.

Legal solutions appear feasible if states are able to engage with legislators, the governor's office, and stakeholders and overcome the barriers listed above.

4.4 Implementing Technology Solutions

4.4.1 Patient and Provider Identification

Virtually all of the proposed efforts depend upon accurate identification of both users of the data (providers and health plans, for example), and of patients, either before an HIE takes place or before data are entered into a patient record. Accurate identification of the individual entering data into an EHR also is deemed essential to success. Many of the patient and provider identification implementations overlap with those aimed at achieving user and entity authentication, authorization, access controls, and appropriate audit practices. Several state project teams were examining the use of digital signatures and developing comprehensive definitions and requirements for all entities that would be engaged in an HIE. Many state project teams indicated that patient and provider identification is currently done in an ad hoc fashion, based on personal knowledge of an individual, or a combination of demographic and/or clinical information. Better algorithms, more advanced technologies, and efforts to develop health record identifiers will address these concerns. This would likely include the use of the national provider identifier (NPI) to clearly identify individual providers and provider organizations.

Several state project teams focused on developing a centralized provider directory that will function as the authoritative reference source of providers within the operational health care network. These directories would provide consistent identification of providers and may link with NPI adoption and implementation currently under way, and include developing methods for applying and incorporating providers without an NPI into the system. These registries will be used not only for provider identification, but also for authentication and to authorize access (i.e., multipurpose systems). One state specifically proposed to issue identification cards to providers that bear their NPI.

A number of states intended to implement solutions related to patient identity issues. One state project team proposed implementing an outreach and education effort related to using the patient's legal name as the patient identifier as an interim fix. Another state project team intended to develop a patient identity index and a provider identification management system to function within their HIE. Another intended to focus on policies and methods to

enable identification of patients and their corresponding health records to accomplish correct linking and matching of patient identifiers and merging of health records that originate from different sources. This integrated view of the patient's health information would then be accessible to authorized users through the HIE system. This will be accomplished through 3 steps: define the minimum demographic data required to optimize performance of the matching and de-duplication algorithm, define acceptable high and low thresholds for automated confirmation and rejection of patient matches in the HIE, and gain an understanding of the personnel resources required for the HIE to support highly accurate patient matching. Because provider acceptance of electronic health information exchange may be contingent upon liability for life or death decisions made on information in the patient's EHR, there exists a need for accurate patient identification.

4.4.2 User and Entity Authentication

Twelve of the state project teams included implementation plans related to user and entity authentication with the goal of verifying that individuals or entities seeking access to electronic personal health information are who they claim to be. One approach would be to develop an in-patient authentication process to confirm that a health care provider is currently providing services to the patient for whom information is requested. The goal is to achieve a process that will function across multiple facilities regardless of the existence of a defined relationship. Another approach would be to create a clearinghouse agency to authenticate participants in that particular HIE network. Several states were studying the role that biometrics and other authentication tools can play in their particular implementations. One state project team intended to develop a personalized health smart card that individuals can carry. State project teams with less advanced HIEs were working on simple authentication measures such as stronger password systems.

Most state project teams recognized the importance of considering the costs and benefits of various approaches to authentication and some were looking at setting minimum requirements. One state project team was undertaking a pilot project to automate the flow of laboratory orders and results among the major laboratories servicing the state and health care providers. This has been chosen as the vehicle for centralizing and sharing authentication services as well as implementing interorganizational secure messaging.

4.4.3 Information Authorization and Access Controls

Eighteen of the state project teams planned to implement solutions related to information authorization and access controls for electronic health information exchange. A variety of approaches were planned, ranging from developing role-based access standards that account for providers' on-call coverage and emergency (break the glass¹²) roles to

¹² Which allows an authorized professional to have access to previously unauthorized information, after verifying emergent need for the additional information.

implementation of various authentication technologies. The common thread running through all these strategies is the desire to allow access only to individuals, entities, or software programs that have been granted access rights to electronic personal health information.

Many of the state project teams examined practices of authentication, authorization, access and audit as a group—i.e., the 4 A's. They formed subgroups to focus on developing and implementing solutions in this area. These include research into specific technology and process solutions such as authorization access for health information handled by various exchange models including centralized, federated and hybrid models. Others were working on clearly defining procedures and processes. For example, participating entities might agree to take responsibility for authorizing a provider's access to patient information, maintaining the provider's account, and terminating the provider's account when he/she is no longer part of the organization. One state project team was developing a consensus model document related to policies and procedures in the EHR environment related to HIPAA standards for the 4 A's. Another was working to implement 19 principles or best practices determined by their 4 A subgroup. The principles are called "General Principles for Authorizing and Authenticating Individuals, Setting Access Controls, and Auditing in a Health Information Exchange" and are part of the state team's plan to implement solutions that address barriers to providing, limiting, and monitoring external access to patient data. The plan overall is to: (1) Assist organizations to incorporate a framework of 19 security principles into their planning and implementation efforts for electronically exchanging health information; and (2) Use an on-going work group with appropriate expertise to continue and further develop the framework created by the 19 security principles. The 19 principles include:

Authorization Principles

- P1.1** All persons having access to patients' health information through an HIE will be assigned a unique user ID. Consistent with the authentication principles, each ID for accessing the health information shall require at least single-factor authentication (e.g., password).
- P1.2** When a person is granted access to patients' health information through an HIE from a particular organization participating in an HIE, it should be that participating organization's responsibility to authorize, maintain, and terminate the individual's access to patients' health information.
- P1.3** The ability of persons to access patients' health information through an HIE should be set using role-based access control standards that are developed and accepted by all organizations participating in an HIE.
- P1.4** All organizations participating in an HIE should develop and accept security credentialing guidelines for authorizing persons to access patients' health information through an HIE. The security credentialing guidelines and process should be as streamlined as possible and minimally include: (a) verifying the identity of individuals authorized to access/exchange health information; (b) defining the appropriate role-based access for individuals authorized to

access/exchange health information; and (c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.

- P1.5** Medical credentialing of health care providers (distinct from security credentialing) should not be required by organizations participating in an HIE when the health care provider is only exchanging health information using standard-based messages or accessing health information in view-only access.

Authentication Principles

- P2.1** All organizations participating in an HIE should minimally require single-factor authentication for verifying the identity of all individuals authorized to access patients' health information within each organization.
- P2.2** All organizations participating in an HIE should minimally require 2-factor authentication for verifying the identity of all individuals accessing patients' health information through the HIE (i.e., across participating organizations).
- P2.3** Authentication of individuals accessing patients' health information through an HIE should be as seamless as possible when accessing information across participating organizations.
- P2.4** From the end user's perspective (i.e., health care providers), the authentication of individuals accessing patients' health information through an HIE should be the same process regardless of which participating organization's health information is being accessed.

Access Control Principles

- P3.1** Health care providers should only access information for patients with whom they have a treatment relationship and then only the health information relevant to the treatment being provided, except in the event of an emergency and, in this case, such access logged and the primary care provider notified of the access.
- P3.2** All organizations participating in an HIE should develop and accept written policies and procedures for accessing and exchanging patients' health information through the HIE.
- P3.3** All organizations participating in an HIE should develop and accept minimum standard training requirements for educating individuals about the policies and procedures for accessing and exchanging patients' health information through an HIE.
- P3.4** All organizations participating in an HIE should develop and accept common sanction policies for addressing situations when individuals violate the policies and procedures for accessing and exchanging patients' health information through the HIE.
- P3.5** HIEs should develop policies and procedures for disabling individuals' access to patients' health information through an HIE for inappropriately accessing patients' health information.
- P3.6** HIEs should have policies and procedures for terminating a logged-in individual's session accessing patients' health information due to inactivity within the session.

Auditing Principles

- P4.1** All organizations participating in an HIE should develop and accept minimum standards for routine auditing of individuals' access to or modification of patients' health information through the HIE, auditing established and related policies and procedures, auditing the results and action taken as the result of a risk analysis, etc.
- P4.2** All organizations participating in an HIE should maintain audit logs that document individuals accessing or modifying patients' health information. The audit logs should minimally identify: (a) the individual accessing the health information; (b) the health information being accessed; (c) the date and time of the access; (d) any action taken relating to the stored information (e.g., amendments, changes, deletions, and addition of new records); and (e) all failed log-in attempts.
- P4.3** All organizations participating in an HIE should develop and accept: (a) the data elements to be maintained and exchanged for auditing individuals' access to patients' health information; (b) the frequency with which the auditing data will be exchanged between organizations participating in the HIE; (c) the minimum retention time of audit logs maintained for auditing individuals' access to patients' health information; and (d) the development and management of a comprehensive audit program.
- P4.4** All organizations participating in an HIE should develop and accept procedures for: (a) alerting other participating organizations of situations where patients' health information may have been inappropriately accessed; (b) jointly investigating situations where patients' health information may have been inappropriately accessed; and (c) notifying the patient of any privacy breaches.

Several state project teams took creative approaches to these authorization and access challenges. One was developing software tools that assist in specifying *minimum necessary* information and specially protected information. Another was developing a mechanism for patients to specify whether and what information can be shared, whether they have opted out of sharing completely, or by information type. Additional technology solutions evaluated by some of the state project teams included digital signatures, digital certificates, biometrics, USB use, and card swipe technologies.

4.4.4 Information Audits

Seven of the state project teams included implementation plans focused on information audits that record and monitor the activity of health information systems. While some state project teams were confident in adopting industry standards, others will develop a framework for what standards need to be looked at and how to identify best practices. One state project team planned to build a cost-effective and efficient automated proactive audit mechanism. Another was establishing a sophisticated tracking methodology to be implemented in hospital information systems that would alert users to suspicious system activity. Others planned to conduct regular audits with deterministic methodology, while some will take a more passive approach and rely on industry standard practices defined in

their business associate contracts. Several states were looking at minimum standards for routine auditing of persons' access to patients' health information through their HIE.

4.4.5 Information Transmission Security, Data Integrity, and Remote Access

Six of the state project teams planned to examine ways to implement or strengthen information transmission security or exchange protocols for information exchanged over an electronic communications network. All will focus on design and implementation of technical solutions for expanded data exchange services, and several will craft regulations governing how personal health information can be transmitted. One state project team will specifically examine encryption as a technical solution and will use their newborn screening program as a test case for implementing the new regulations. Another will examine and establish procedures for pseudonymization, while a third will require that any patient information being transmitted on external networks go through virtual private network connections between client and server or network to network. State project teams in earlier phases of electronic health information exchange will work to define a common technical approach or adopt standard security protocols to clarify technical requirements for data-sharing partners. Another state team will assist facilities participating in electronic health information exchange by providing secure messaging functionality and the technology necessary to support it.

4.4.6 Information Standards and Best Practices

Nine of the state project teams took steps to implement broad information security standards and best practices. One project was forming an information technology security committee to identify and establish a wide range of security standards for their HIE participants. They will initially focus on convening workshops to examine established security protocols, organizational standards, and minimum standards for exchange. Later work will involve testing and recommending common standards and protocols in conjunction with privacy policies for all areas of security. One project will establish a collection of best practices and leverage those to provide technical assistance. States early in their HIE experience will limit their implementations to vocabulary, data, and messaging standards. One project aimed to establish data element standards and create a best practices repository available to help guide their HIE partners. Developing data standards will enable patient identification by ensuring that information necessary for matching algorithms is available, while messaging standards will help ensure that information transmitted electronically is done in a secure manner. Several states will be implementing HIE demonstration projects within specific geographic areas, or using specific types of personal health information.

4.4.7 Analysis of Feasibility and Barriers to Implementation of Technical Solutions

All state project teams rated the feasibility of the implementation of their proposed solutions to be *feasible*, or higher. Of the 23 individual efforts that received ratings, 9 were rated as *highly feasible* (39%); 4 were rated as *feasible-highly feasible* (17%); and 10 were rated as *feasible* (43%). Most state teams provided information on anticipated barriers to implementation. A quote from one stakeholder illustrates the complexity of progress in the HIE area:

While the work group acknowledged that some aspects of implementation will be inexpensive and have few impediments, they drew on their collective histories and knowledge to point out that [EHR] implementations in general were costly, have taken years to fully implement, if that implementation is ever complete, and require tremendous organizational resources in time, expertise and money.

Anticipated barriers clustered around 4 specific areas: funding and return on investment, people issues, technical challenges, and process issues.

The state project teams noted the following barriers related to the broad area of funding and return on investment:

- lack of overall funding to move projects ahead
- funding, not only for the shared services but also for the provider interface implementations of source and consumer applications and information conversions
- unknown costs to stakeholders for migrating to and implementing standards
- affordable advanced security controls may not be available
- lack of proven value of electronic health information exchange
- unidentified funding streams
- inability to articulate return on investment for electronic health information exchange to stakeholders
- lack of resources to implement a strong communication and public relations campaign

The state teams noted the following barriers related to the broad area of people issues:

- health care providers must cooperate and place a priority on this project
- fear of increased liability from standard policies and procedures
- inadequate buy-in from the medical community
- cultural resistance to changes incurred by proposed solutions
- lack of public awareness
- inadequate consumer buy-in

- lack of input from stakeholders in establishing the best practices for privacy and security of health information
- tracking and managing voluntary participation efforts—for consumers participating in an HIE
- change aversion
- requirement for long-term organizational commitment
- inappropriate governance structure of state health information network
- political roadblocks (not otherwise specified)

Specifically, some of the people issues are related to the availability of specific resources to fulfill needed roles on the projects:

- inability to identify the appropriate consultants
- limited qualified staff with specific expertise
- unidentified resource availability within the organization
- lack of personnel trained in encryption technology
- the burden to user entities of training and administration of delegated authentication functions for personnel who desire to use the HIE

The following barriers are related to the broad area of technical challenges:

- Rapid changes in security technology make purchasing decisions difficult.
- Outdated infrastructure makes integration of new products challenging.
- Lack of required standards that have been vetted and adopted (state and national).
- Resistance to adopt existing standards.
- Difficulty of integration with existing solutions.
- The potential inability to develop something that is both flexible and scalable.
- Lack of technology/technical infrastructure in rural communities, tribal nations, and smaller physicians offices.
- Different levels of development and resources among public and private entities.
- Existing security variations among entities.
- Risk that limited products are available that implement standard approaches not yet finalized.
- Providers lacking technical infrastructure.
- Reaching agreement on minimum data set and finding those data sources.
- Local standards are not yet available or appropriate.
- Limited connectivity and low adoption rates for EHRs.
- Integration with legacy systems will be technically challenging.

Finally, several process issues are significant and will require attention:

- Lack of process engineering in health care is a technological deficit that requires research.
- Benchmarks for evaluation of progress are not established.

4.5 Implementing Education and Outreach Plans

All of the state teams mentioned education and outreach efforts in their implementation plans, even if they did not include a specific implementation plan for their educational programs. Education and outreach are cross-cutting and are required when implementing nearly all of the plans described in this report. For example, passing new legislation should include an educational component to ensure that affected parties are aware of the change in regulations. Similarly, technology standards will not be adopted unless payers and providers are educated about their existence. State teams proposed a wide range of educational efforts aimed at consumers, providers, and other groups to facilitate and improve electronic health information exchange.

4.5.1 Consumer Engagement and Education

The majority of the states proposed some form of informational group meeting to share information about electronic health information exchange with consumers. The goal of the sessions is twofold: to educate consumers on the secure exchange of electronic health information and to solicit input regarding the implementation plans and process. In addition to the informational meetings, some states proposed utilizing a secure website to keep consumers engaged and updated on the process and progress. Several states also planned to create consumer advisory committees as a way to maintain consumer engagement.

Consumer education and engagement aims to address 3 major issues: First, consumers are often not aware of their rights and responsibilities with respect to their health care records. Second, consumers may not be aware of the benefits of electronic health information exchange and EHRs. Finally, because of the lack of information, consumers may mistrust HIEs and EHRs. As 1 state noted, “The cumulative differences in knowledge among consumers and health care industry staff naturally leads to mistrust and negatively affects consumers’ confidence for participation in an HIE.” Another observed:

Patients and consumers are generally not aware of the privacy protections and rights they enjoy under the HIPAA Regulations and state law. Because of this, many patients and consumers retain an unnecessarily high level of distrust regarding the storage and communication of their health care information when it is in electronic form. This high level of public distrust may threaten to delay or derail the transition of the health care delivery system into the information age.

Sixteen state teams included implementation plans for engaging with or educating consumers. These efforts included community forums, focus groups, pamphlets and other

literature, and a website with frequently asked questions and other resources. Other options include television and radio campaigns and collaboration with consumer groups to raise awareness about the benefits of electronic health information exchange. State teams have also been including consumers in their HISPC work, which may help ensure acceptance of electronic health information exchange initiatives emerging from this work.

Topics for consumer education included

- options regarding opting in or opting out of an HIE,
- existing and successful HIE efforts,
- benefits of electronic health information exchange,
- privacy and security rights related to sharing health information,
- how to access and manage one's own health information,
- personal health records, and
- the continuity of care document.¹³

4.5.2 Provider Education and Outreach

In addition to reaching out to consumers, state teams also planned outreach and educational efforts for providers. State teams identified different levels of knowledge among health care industry stakeholders about privacy and security requirements for electronic health information exchange. Educational efforts up until now have not always had the desired effect. As 1 team noted:

Despite many initiatives to educate health care providers and payers regarding federal and state privacy and security laws and regulations, it was clear many do not have an accurate or complete understanding of the HIPAA Regulations or relevant state privacy laws as they relate to electronic health information exchange.

Provider education seeks to reduce variations due to incorrect or incomplete understanding of relevant state and federal law. It may also reduce liability concerns and facilitate exchange if providers are more confident in their compliance with state and federal law.

Twelve state teams outlined education efforts for providers, with 5 of these functioning as components of broader educational efforts that include education and outreach for consumers and others, such as payers and employers. In addition to general awareness about electronic health information exchange, state teams also sought to raise awareness about specific issues. Three states proposed educational efforts relevant to newly passed or anticipated legislation that could change the way providers exchange information.

¹³ The continuity of care document emerged from the harmonization of the continuity of care record and the clinical document architecture. The two were harmonized to promote interoperability.

Other specific topics for provider education included

- clarification of state law,
- promotion of electronic medical record adoption,
- education about common consent forms, and
- technology options and standards.

Methods of education and outreach proposed were similar to those for consumers, such as literature and conferences, but also included options for working through professional organizations, and potentially offering continuing education credit for medical professionals.

4.5.3 Other Education and Outreach (To Health Plans, Policy Makers, and Others)

Almost all of the state teams saw the need for informational sessions tailored toward legislators and government leaders to garner support and funds for HIE initiatives although they often did not include a separate implementation plan for these efforts. One state team planned to hold a statewide health information network summit to share technological solutions to the barriers identified in their state.

Two other groups to be targeted for educational efforts included public health and law enforcement officials. These individuals frequently need access to personal health information in order to conduct disease surveillance and investigation in the case of public health, and to assist in emergency care of a patient or conduct criminal investigations and prosecutions in the case of law enforcement. Three state teams planned educational programs for law enforcement officials. Two have already had success in working with the officers, and 1 included relevant training for members of the service academy. One state planned to educate public health officials about their role in electronic health information exchange, but did not offer details. Finally, 1 state has included public health from the inception of their project, and has integrated a public health perspective into their entire planning process.

4.5.4 Implementation Plans Addressing Other State Solutions

In states where specific HIE initiatives have been identified as a method for advancing electronic health information exchange, the above methods of education and outreach will be utilized to build support for these efforts. That is, state teams intend to incorporate the overarching initiatives as a part of the larger presentation on electronic health information exchange in the state.

4.5.5 Analysis of Feasibility and Barriers to Implementation of Education and Outreach Plans

State teams felt that it was feasible to implement education and outreach programs. Although such programs may be costly, there are established frameworks for educating

consumers and providers. In addition, the fact that many state teams feel that such education is critical to the success of electronic health information exchange and HIT makes these programs a priority.

State teams also recognized that they may require special expertise in executing the education and outreach campaigns and therefore often listed the need to identify and hire a marketing or communication consultant to develop effective consumer messages. The teams also proposed to identify subject matter experts to be used in the various education forums.

Another state noted that emergent issues, such as those related to unapproved release of personal information, will greatly influence receptivity of messages and HIE acceptance.

As with many of the implementation plans described in this report, funding was a frequently cited barrier. State teams were concerned that they would not receive appropriations or be able to raise sufficient funds from other sources. Other barriers to implementation included

- lack of support and participation among stakeholders (5 states),
- nonparticipation among stakeholders (3 states),
- lack of staffing,
- inability to identify delivery mechanisms to reach the widest scope of consumers,
- inability to engage interested stakeholder groups to participate in the development of materials,
- lack of proven value of electronic health information exchange,
- complexity of systems and processes for implementation, and
- change aversion.

5. IMPLEMENTING MULTISTATE SOLUTIONS

In order to achieve the goal of interoperable electronic exchange of health information nationwide, states must begin to expand their discussions across their borders. Highlighted throughout the reports was the desire to build solutions that would facilitate exchange between states while preserving the privacy and security of the records. In some states, this issue is of more immediate importance due to relatively high numbers of patients traveling between states to receive their health care. States that have large border cities, high levels of tourism, or the ability to provide more comprehensive medical services than their neighbors all have a vested interest in being able to transmit data across their borders.

While this issue is clearly a fundamental necessity as electronic health information exchange continues to expand, it was difficult to create specific plans for coordination between states under the timeline required on this contract. Four states were able to propose potential solutions that had specific tasks or time frames, while another 11 were able to articulate the desire to collaborate with other states on a particular issue. Far from indicating that the teams were not interested in pursuing multistate solutions, 5 additional states indicated a desire to pursue more organized plans but felt that additional time and continued networking support were needed in order to achieve a more structured collaborative environment for multistate solutions. In fact, a number of states expressed the hope that continued initiatives would ensure that the collaborations invoked in this project were not forgotten.

An overview of the plans that were provided in the interim reports to implement multistate solutions is provided below. Specifically, these are the propositions that would create solutions owned by a group of states themselves, rather than solutions from the federal level that would affect a majority or all of the states.

5.1 Multistate Leadership and Governance Solutions

Few states proposed specific plans for the creation of a governance structure that would oversee the creation of common privacy policy and security solutions between multiple states, although a handful of states noted a willingness to join in such an effort if one were started. Three states mentioned the possibility of coordinating efforts in their own states with the efforts of a common coordinating body such as the State Alliance for e-Health. One state indicated that it planned to convene a “multistate work group” that would track the direction in which neighboring states were going in a variety of different areas and feed that information to other state-level work groups (clinical, technical, legal/policy, etc). Overall, the reports indicated an interest in becoming involved in initiatives that would seek to build consensus and harmonization, but most were unable to articulate, at this point, an

appropriate model for governance that would grow up from the states (see Section 6 for suggested national initiatives).

One state was able to give a detailed set of objectives for participation in a regional or national initiative to frame national technical and policy standards necessary to promote the exchange of health information between states. Starting immediately, they proposed to help formulate a regional or national task force charged with promoting the advancement of health information technology, utilizing the current knowledge of the Markle Foundation, the State Alliance for e-Health, and other national resources. In addition to collaborative policy formation, a second objective of coordinating between states and federal programs would be to provide clarification on existing regulations and to ensure that guidance is provided on the technological standards for the Nationwide Health Information Network. This body was also suggested to undertake the coordination of other issues such as developing a plan for sharing data across state borders in the case of disaster or emergency and continuing to explore legal templates that could be shared between states. One final objective of this body is important to note: the representatives of this national standards body would be charged with implementing the plans adopted through this collaboration in their state.

5.2 Multistate Practice and Policy Solutions

Implementation of practice and policy solutions was also an area where limited examples of multistate coordination were provided by the states. Six states provided potential multistate solutions although many of these ideas involved the intersection of these initiatives with national-level activities, either by way of states feeding their accomplishments to a federal initiative engaged in standardizing practices and policies, or by mandating that the multistate group watch and adopt policy guidance released at the federal level.

Three states mentioned a desire to pursue standard policies with other states concerning public health emergency or similar “break the glass” procedures, which allow authorized professionals to have access to previously unauthorized information, after verifying emergent need for the additional information. One state team suggested that efforts currently under way through their department of health and department of emergency management to pursue communications plans and strategies in the case of a bioterrorist attack or natural disaster could be connected regionally because there are similar programs in neighboring states. The proposition is to become more involved with these existing efforts rather than to create a new set of policies and procedures that could be agreed upon by a group of states. Each state’s department of health and department of emergency management branches would take a leadership role in ensuring that this coordination became a priority in interoperability discussions. These efforts could also be appropriately harnessed in natural disaster and public health emergency situations.

Three other states expressed a desire to standardize the criteria used to identify a patient within an electronic exchange of health record information. In 2 states, this desire was mentioned but no specific plan was outlined for coordination between states. The third outlined a solution to create model policies and procedures within their state to ensure appropriate capture, verification, and match of patient identifiers with patient information in a health care system. A second part of this solution was to look toward federal efforts, such as the Confidentiality, Privacy, and Security Workgroup of the American Health Information Community, and other nationwide efforts, such as the Markle Foundation's Connecting for Health Initiative, both of which have endorsed guidelines concerning the identification of patients, for guidance when creating these policies.

Multiple groups are currently working on policy issues with a broad lens, which could be applicable to many, if not all, of the states. Private groups such as the Markle Foundation and public entities like the State Alliance for e-Health continue to work on providing significant guidance in terms of privacy policies that enable appropriate electronic exchange.

5.3 Multistate Legal and Regulatory Solutions

Only 2 states explicitly discussed working with model state law in their implementation plans. One team felt that model laws would improve interstate communication, but did not elaborate further on how the drafting of model laws might occur. Another state suggested working with the federal government and national leaders to explore the use of uniform state consumer banking laws or other templates for structuring laws that govern the secure and private exchange of health information. Both states mentioned the National Conference of Commissioners on Uniform State Laws as a possible vehicle to lead the effort of reviewing and subsequently harmonizing federal and state law. One of the plans did not discuss specific tasks needed for the formulation of model laws, but indicated that resources would be available in their state through September 2008 to continue working on basic components necessary for such an initiative.

Two states proposed specific plans to align the legal environment in a multiple state area either in general or around certain issues. The first plan was to pursue a compact between 3 states before the end of 2008 to clarify the legal interstate environments related to each state's exchange programs. The first step to this plan is to have each state define their specific legal or statutory barriers to the exchange of information across state lines.

A second implementation plan outlined the development of 2 standardized laws between neighboring states:

- Develop a standardized genetic information protection law: 6 to 9 months from start of bridge phase. Recommend adoption and begin education and provider outreach at end of development phase.

- Develop a standardized age of consent law: 6 to 12 months from start of bridge phase. Recommend adoption and begin education and provider outreach at end of development phase.

5.4 Multistate Technology and Data Standards Solutions

Five states proposed specific plans to either work with other states in creating regional standards for technical issues or to work on creating standards in conjunction with any national collaborative effort. One state suggested working with other states as they develop a core set of privacy and security solutions to ensure regional acceptance. Another plan outlined working with 2 neighboring states to develop use cases, create common standards for electronic health information exchange and devise tests for exchange, with the goal of testing clinical data messaging between the 3 states before the end of 2008. A secondary goal was to look at differences in security requirements, redundancy, and failover capacities in a fourth state. Two other states indicated that they would like to incorporate pilot programs into the exchange programs that are currently being constructed that would attempt data exchange with a small subset of appropriate states. Another state indicated that it would like to initiate discussions with a neighboring state regarding exchange of data between their immunization registries.

5.5 Multistate Education and Outreach Solutions

None of the state project teams proposed any multistate education or outreach plans.

5.6 Analysis of Feasibility and Barriers to Implementation

Less than half of the states provided specific plans to coordinate with other states regarding the privacy policies and security standards that would be required for interstate exchange of personal health information. The majority of states, however, did express a desire to continue the collaborative work begun under this project. A number of issues could account for the small number of specific plans despite the clear desire to engage in such activities. First, the timeline for the work undertaken in this project found the state teams hard pressed to develop a full and adequate understanding of the complexities involved in the exchange of health record data within their own state. As previous reports released from this project have indicated, creating common privacy and security standards for exchange between 2 hospitals located in the same city can be difficult and time consuming, and in many cases, these discussions have not even begun at the local level. The ability to discuss these issues with other states when there is still a fundamental lack of knowledge at a local level makes multistate collaboration a secondary concern at this time. The addition of differing state laws, community needs, and competing interests also create obstacles to interstate discussion. One state indicated that despite their extreme desire to move forward with discussions with other states, the scarce resources available to them made it necessary to focus on their immediate needs within the state first.

This does not mean that the best method for moving forward is to have each state work independently. A second major issue affecting the feasibility of multistate solutions is funding. The practical aspects of coordinating funding from multiple states make these types of solutions somewhat prohibitive. Many states are still struggling to secure the funds necessary to work on privacy and security issues within their own state, and developing sufficient support in multiple states at the same time would require an enormous effort. Funding is more likely to come from a private or external source than from state governments themselves. It is not unreasonable to assume that this funding could be secured in some areas, but it hasn't been secured yet.

6. IMPLEMENTING NATIONAL SOLUTIONS/RECOMMENDATIONS

Reports submitted by the state project teams typically expressed a desire to see greater coordination of governance, policy, regulation, technology standards, and education at the national level rather than in scattered regional pockets. Twenty-one states made some type of recommendation regarding national-level intervention. Although states made recommendations, they were not asked to outline specific implementation plans for national activities. A number of states offered to participate in leadership and the development of policy and technical standards, especially when they felt they had already made significant headway through local initiatives. The theme, however, indicated a strong feeling that these efforts should be synchronized by a clear national directive and not left completely to local efforts, which are scattered and often lacking adequate resources. As 1 state put it, the fear that everyone was “reinventing the wheel” ran strong, but so did the feeling that this project had provided a sense of relief to many, knowing that many states are wrestling with similar problems and are interested in working together to perpetuate their collective knowledge.

6.1 National Governance: Identification of Responsible Bodies

Scattered throughout the state reports were mentions of possible organizations that could serve as responsible bodies to govern privacy and security at the national level. The responsible body indicated in the recommendation typically depended on the specific issue. Overall, there seemed to be a general understanding of the multiple government organizations governing the multiple privacy and security issues that affect the appropriate exchange of health record data. Seven specific recommendations were put forth regarding the responsibility of the federal government to either provide additional guidance for a specific issue, or to create centralized governance of the multiple privacy and security concerns that will affect electronic health information exchange on a nationwide level.

One state suggested that the Veterans Administration become more involved in the national discourse surrounding electronic health information exchange. Although the specific reasoning for encouraging greater involvement was not identified in the state report, the fact that the Veterans Administration does maintain a centralized electronic medical record system for its patients may provide a unique learning opportunity. Although this system would not be directly transferable to the systems currently being constructed at the local and state level, the technological capabilities regarding patient matching and especially those regarding workflow considerations may be of great help to informing practice guidelines concerning a system that is integrated across the country.

Other suggestions about the responsibilities of existing entities included greater coordination with government agencies or bodies for which privacy and security issues are related to

their main focus, such as the Office for Civil Rights (OCR), the Centers for Medicare & Medicaid Services (CMS), the Health Information Technology Standards Panel, and the Certification Commission for Health Information Technology. In the case of OCR, 1 state proposed that they publish de-identified case studies of their enforcement actions on their website. It is important to note here that OCR now publishes specific but de-identified case examples of corrective action obtained from covered entities through enforcement of the Privacy Rule. One state also suggested that the US Department of Health and Human Services (HHS) undertake a process to strengthen the relationship between state activities and federal activities. Among other objectives, the state felt that this process would help to clarify the objectives and responsibilities of the current initiatives and at the same time create a mechanism that would facilitate stronger communication between them. It was also expected that this initiative would strengthen communication between the federal initiatives and the individual state health information exchange initiatives.

Similarly, 2 states proposed the creation of a *new* body that would coordinate privacy and security issues among all of the existing initiatives. Both states suggested that this body should be driven by input from the states to continue the collaborative spirit begun on this project, but that the final products of the group would be released as federal guidelines. One state also suggested specifically that this body develop electronic health information exchange procedures and review laws for the exchange of information between states. This need identified by the state teams may be filled in all or in part by the 2007 formation of the State Alliance for e-Health. The National Governors Association Center for Best Practices was awarded a contract from the Office of the National Coordinator for Health Information Technology to establish and manage the State Alliance for e-Health, a consensus-based, executive-level body of state elected (and appointed) officials to collectively address state-level health information technology (HIT) issues and challenges to interoperable electronic health information exchange.

6.2 National Practice and Policy Recommendations

Seven states proposed recommendations for federal guidance on practice and policy. First, although the state teams recognize that the variation in the way consent and authorization policies are defined and implemented is largely driven by state laws, there is widespread confusion when organizations try to reconcile the requirements of state law with federal regulations, especially with regard to specially protected data. Although most of the state teams developed plans to create uniform approval policies within their state, 3 state teams suggested the variation in approval practices could be resolved more expediently if a basic or core set of practices and policies for consent and authorization could be defined and coordinated at the national level so that states could choose to adopt those that best met their needs.

One state discussed the view that most of the attention had been focused on the technical aspects of HIT implementation, but less attention had been given to the workflow issues that many providers and other stakeholders had expressed concern about during the course of the project. Therefore they proposed the creation of a new body, the Community of Practice Support Network, which would focus entirely on practice issues related to HIT.

Three states suggested that federal policy guidelines regarding certain data elements would greatly reduce the burden of developing technical standards. Two states suggested using the American Society for Testing and Materials continuity of care record as a policy adoption target that would encourage the development of a data set that health care providers would feel comfortable using. One state outlined a solution that would produce standards at the federal level for patient identification that were driven by consensus policies. Their plan suggested specific tasks such as convening a national advisory council, performing a literature search and secondary source review to inform standards identification, and, finally, developing recommendations and producing a final report.

6.3 National Legal and Regulatory Recommendations

As with many of the issues discussed in this report, states expressed a desire to see leadership at the national level with legal and regulatory changes even as they continued to pursue many issues unique to their own state context. Although many states proposed legal and regulatory solutions at the state level, the majority of recommendations given for national action were in this area. Twelve states indicated that they would like to see legal and regulatory guidance at the national level. These suggestions took on 2 major themes: passing new federal legislation/regulatory guidance or providing clarification/updates to current legislation.

New Federal Legislation or Regulatory Guidance:

- **HIEs:** Three states suggested that new legislation or guidance be put forth at the national level concerning HIEs or other clearinghouse organizations. One solution put forth by a state involved national legislation that would enable information sharing between state-level HIEs. The legislation would designate a federal privacy and security standard that preempts more stringent state legislation in connection with information sent from one state to another via a health information network. This state also suggested that the legal status of HIEs be addressed at the national level, as well as the process of developing a framework for liability that addresses the role of the state-level HIE organization and the interaction of federal and state-level regulatory frameworks.

Updates or Clarifications to Existing Federal Legislation or Regulatory Guidance:

- **Medicaid:** One state suggested advocating that federal guidelines related to Medicaid data release be reviewed and streamlined. The desired outcome would be changes to federal or state guidelines related to sharing of Medicaid data. Another state asked both CMS and the Office of Inspector General for a favorable advisory opinion excepting some specific level of cooperation between physicians and

hospitals with respect to sharing money for technology or participating in demonstration projects.

- **Stark and Antikickback Laws:** Two states suggested expanding the scope of these regulations to target providers who serve the historically underserved, and to amend the regulations such that hospitals are allowed and possibly induced to provide physician practices that are serving economically disadvantaged populations with not only hardware, software, and training, but also additional technical resources to implement and support the technology.
- **Clarification of Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules:** Three states suggested clarification in areas within the HIPAA Privacy and Security Rules that were considered unclear. One state noted that their stakeholders felt that the Privacy Rule requirements for psychotherapy notes were not clear but did not explain the issue further. One recommendation was to change the HIPAA Privacy Rule so that it would require the provider to obtain a patient's legal permission once, at the initial point of service, that would permit the provider to release the information for specific purposes and to specified entities in the future. The suggestion to make patient permission mandatory for current exchanges for treatment, payment, and health care operations was thought to facilitate future requests for the release of the information held by that specific provider. The state team believed that making this a federal recommendation or standard would facilitate the interstate exchange of information. One state proposed a process to more thoroughly review the areas of ambiguity between the HIPAA Privacy and Security Rules and their own state laws.
- **42 C.F.R. pt. 2:** One state suggested that HHS explore the contours of consent/approval without the need for legislative action although they also recognized that their suggestion may require congressional action. The team is recommending that HHS more clearly define 42 C.F.R. pt. 2 so that a single consent would allow for unlimited downstream releases for certain purposes and clarify that authorization can describe generally the entities to which Part 2 records may be disclosed. As an alternative, 42 C.F.R. pt. 2 could be amended to provide that patient authorization is not required to exchange the data for treatment purposes only.
- **CLIA:** One state discussed the Clinical Laboratory Improvement Amendments, detailing specific conflicts that it imposes in their state due to ambiguity about the terms utilized. One other state proposed to review the CLIA regulations in light of HIE organizations that endeavor to provide electronic laboratory reporting services.
- **FERPA:** Two states called for clarification and/or revision of the Family Educational Rights and Privacy Act (FERPA) and educational institutions' rights to deny medical record release.

6.4 National Technology and Data Standards Recommendations

Six states outlined suggestions for standardizing data technology and data standards at the national level. Many of these states expressed the feeling that there needed to be clearer examination of the role of an emerging standard-setting organization as a mechanism to respond to an evolving interoperable environment more quickly and effectively than state-by-state or federal legislative processes. One state suggested, in general, maintaining a continued focus on national data standardization for allergies, problem lists, laboratory tests, etc. One state team outlined several specific technological issues that their

stakeholders believed should be the responsibility of the federal government rather than the states in order to achieve consistent and rapid adoption. These issues included the following:

- Establish approved national standards for data exchange that must be adopted by all entities involved in an HIE. An effective enforcement agency is also necessary.
- Standardize the use of an access control system access model and implement it across the full spectrum of health care entities.

A number of other states echoed the need for national standards with regard to the following:

- Standards need to be developed for role-based access control as defined initially by the HIPAA Rules with regard to treatment, payment, and health care operations, and covered entities, and then expanded to noncovered entities and individuals or entities likely to have access to data.
- The electronic health record audit trail, documenting by time and date stamp and source for all read and write access to protected health information, currently required under the HIPAA Security Rule, should be reinforced and required under state regulations for all electronic health information exchange.
- Consumers should have the option to receive automatic reports each time their records are accessed. In addition, there should be a standard process for consumer-initiated data review and correction to ensure the integrity of data.
- A model for appropriate practices in security standards should be formulated that includes a review of all existing security standards and a data classification schema.

Other specific issues addressed in other state project team reports included the following:

- **Promoting establishment of a standard set of patient identifiers:** The lack of a consistent set of patient identifiers creates security issues for matching patient records and can delay or impede electronic health information exchange. One state recommended advocating for a national patient identifier or a standard patient identification process/algorithm, but also noted that their choice should align to the national direction.
- **National standards defining security breaches:** Providers are responsible under the HIPAA Rules to protect against security incidents, so education and clarification would be helpful regarding what constitutes a security incident. The proposition is that national standards should override current state laws related to breaches and serve as a “ceiling” instead of a “floor.”
- **Authentication and authorization standards:** The federal government needs to make the development of national standards for authorization and authentication a high priority. This might be done by identifying authentication as one of the use cases within the American Health Information Community, and by asking the National Governors Association to facilitate agreement among the states for minimal requirements for provider authorization. This suggestion also notes that many organizations are already addressing the need for defining policies, practices, and business rules to support information technology standards, including the Council for Affordable Quality Healthcare, the Committee on Operating Rules for Information

Exchange, the Health Information Management Systems Society, the National Quality Forum, and others.

6.5 National Education and Outreach Recommendations

Three states outlined recommendations to provide education and outreach at the national level. One state indicated a responsibility for providing education to patients and consumers with regard to privacy and security concerns, but felt strongly that an effective education campaign could only exist if led by a broad public information effort at the national level. The state suggested that this campaign should be conducted by HHS at the national level and that HHS should draw upon the experience of the Office for Civil Rights, which has responsibility for enforcing the HIPAA Privacy Rule. Another state indicated that consistent and uniform messaging in the form of federally recommended education materials should include patient-consumer advocacy components and promote the idea of patient rights.

6.6 Analysis of Feasibility and Barriers to Implementation

States had a clear interest in seeing an increased role from the federal government to ensure that privacy policies and security standards were consistent enough across the country to assure smooth transition to nationwide health information exchange. Some clear barriers to national-level implementation plans do exist, however. States indicated that many of these national suggestions were feasible as long as the objectives of the initiative were clearly defined, the appropriate stakeholder support was gathered in conjunction with the initiative, and the initiative had strong and dedicated project manager(s). As 1 state noted, “other projects and industries have demonstrated that private and secure data exchange is possible from a technology standpoint but there are other barriers to overcome.”

One of those barriers is the time frame that would be necessary to develop and implement national standards. Many of the states noted an understanding that, although the possibility of fragmentation exists, changes can happen on a local level more quickly than at the national level. Although not framed as a barrier, another state noted a list of the entities that would need to be involved in defining policies, practices, and business rules for HIT standards—including the Council for Affordable Quality Healthcare, the Committee on Operating Rules for Information Exchange, the Health Information Management Systems Society, and the National Quality Forum—and that federal agencies and offices such as the Agency for Healthcare Research and Quality, the Office of the National Coordinator of Health Information Technology, and the Office of Civil Rights within HHS should be involved in the coordination of these efforts. Although not mentioned specifically, it would also be important to include CMS as part of the list. Even then, this list is far from exhaustive, and it gives only a small indication of the number of national-level entities that would have to align in order for some of these initiatives to move forward.

Another state team noted that the diversity of business practices associated with health information exchange as well as the diversity of interpretations and applications of the HIPAA Rules, state and national laws, and data standards would need a national-level panel of experts to work out, yet the feasibility of finding resources to support this work, particularly technology experts with the time and incentives to participate, would be difficult.

A second barrier included the possible negative consumer reactions to any change in the HIPAA Rules or current federal/state laws. One state noted that there could be significant public debate regarding the considerable privacy concerns against the general public good that would come from having health record information available to provide continuous care to the patient.

Despite a desire to see some national guidelines, there was also an understanding that individual state autonomy and local desire for stricter standards needed to be considered. Although a few states called for national-level education efforts, 1 state noted that such education efforts would likely not be helpful due to the unique privacy rights and independent nature of their local providers. They did not believe that general marketing themes would transfer easily to their state.

APPENDIX A
GLOSSARY OF ACRONYMS

Glossary of Acronyms

| | |
|----------|--|
| AHRQ | Agency for Healthcare Research and Quality |
| BAA | business associate agreement |
| CLIA | Clinical Laboratory Improvement Amendments |
| CMS | Centers for Medicare & Medicaid Services |
| HHS | Department of Health and Human Services |
| EHR | electronic health record |
| FERPA | Family Educational Rights and Privacy Act |
| IP | Implementation Plan |
| HIE | health information exchange |
| HIPAA | Health Insurance Portability and Accountability Act |
| HISPC | Health Information Security and Privacy Collaboration |
| HIT | health information technology |
| HIV/AIDS | human immunodeficiency virus/acquired immunodeficiency syndrome |
| IAS | Interim Analysis of Solutions |
| IAV | Interim Assessment of Variation (of Business Practices, Policies, and State Law) |
| IPWG | implementation planning work group |
| NPI | national provider identifier |
| PHI | protected health information |
| RHIO | regional health information organization |