

September 23, 2008

The Honorable Michael O. Leavitt

Chairman

American Health Information Community

200 Independence Avenue, S.W.

Washington, D.C. 20201

Dear Mr. Chairman:

The American Health Information Community (AHIC) has identified and prioritized several health information technology applications, or “breakthroughs” that could produce specific and tangible value to health care consumers. To address these breakthrough areas, the Confidentiality, Privacy, and Security Workgroup (the CPS Workgroup) was formed and given the following broad and specific charges:

**Broad Charge:** Make recommendations to the AHIC regarding the protection of personal health information in order to secure trust and support appropriate electronic health information exchange.

**Specific Charge:** Make actionable confidentiality, privacy, and security recommendations to the AHIC on specific policies that best balance the needs between appropriate information protection and access to support, and accelerate the implementation of the consumer empowerment, chronic care, and electronic health record related breakthroughs.

Over the past two years, the CPS Workgroup has discussed and made recommendations (summarized in Appendix A) to advance the charges stated above. As the Department of Health and Human Services (HHS) prepares to transition AHIC to a new entity, the CPS Workgroup has set forth below some additional considerations for future work by the HHS or any successor to AHIC. These considerations reflect much of the ongoing deliberations of the CPS Workgroup in recent months. In this letter, we identify issues where we have developed a consensus as to desirable approaches, as well as issues that pose challenges ahead, even if the CPS Workgroup has not reached a consensus on the recommended approach. Our goal is to inform HHS and the AHIC of the results of our recent deliberations.

#### Introduction

The development of confidentiality, privacy, and security policies for an electronic health information exchange environment will take time, coordination, and a better understanding of the potential opportunities and challenges that may arise as electronic

health information exchange becomes more widespread. Throughout our deliberations, the CPS Workgroup recognized that existing Federal and State privacy and security laws constituted a foundation for safeguarding the electronic exchange of health information. This foundation covers many of the situations that exist in these new electronic health information exchange environments. Therefore, we sought to identify those issues that introduced new challenges to, or revealed gaps in, the policies that currently protect health information. To date, through both testimony and public comment, we have heard from over 50 experts and members of the public regarding electronic health information exchange activities and the types of challenges they face with respect to confidentiality, privacy, and security.

The development of health information technology (health IT) and electronic health information exchange continues to progress at a rapid pace. Initiatives have launched to electronically connect health providers, health plans, laboratories, pharmacies, public health entities, and others. There are also initiatives to provide consumers with the ability to collect and personally control their health information through tools such as personal health records (PHRs) and health record banks. We have found, however, that the maturity of these efforts varies greatly, as does their ability to electronically exchange health information. Few of these networks are at a mature stage; in fact, one of the key pieces of information provided to the CPS Workgroup is how limited many of these ongoing efforts are at this point, in terms of their ability to electronically exchange health information. Consequently, we recognize that many of these initiatives will change over the next several years with respect to how they electronically exchange health information and, as a result, we have been cautious about making overly restrictive policy recommendations based on speculation. We also have avoided suggesting significant new privacy and security restrictions based on possibilities that are not present either today or in the near term. As noted above, existing Federal and State laws provide some protections for personal health information. Throughout the letter we use the term “personal health information” for two reasons: 1) to refer generally to an individual’s identifiable health information, and 2) because health information in an electronic health information exchange environment may be maintained by entities outside the scope of the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The CPS Workgroup uses the HIPAA term “Protected Health Information” when we intend to refer to information expressly protected by HIPAA. and any recommendations for new policies or revisions to current law should build on this existing foundation.

A policy framework promoting confidentiality, privacy, and security is important to build trust in electronic health information exchange. Such a framework should support the development of electronic health information exchange initiatives that have the potential to benefit health care delivery, transparency, quality improvement, research, and population health. The CPS Workgroup has issued some recommendations with respect to this policy framework but the Workgroup is quickly nearing the end of its tenure. Below we have identified issues, as well as some recommendations, that we believe warrant additional consideration by the HHS and other policymakers as they look at the

appropriate protections to apply to the access, use, and disclosure of personal health information within an electronic health information exchange environment.

## Policy Factors, Challenges, and Considerations for Protecting Electronic Health Information Electronic Health Information Exchange Networks

### 1 - Policies Regarding Network Access

#### Electronic Health Information Exchange Networks Raise New Challenges

Throughout our deliberations, we have focused on whether there are differences between an electronic exchange environment and the health care environment today that raise new confidentiality, privacy, and security issues not fully resolved by current rules. For example, when a provider converts paper records to an electronic format, we see few, if any, new privacy and security challenges from those that exist today. But the availability of personal health information through electronic health information exchange networks (also referred to as “networks” throughout the letter) is a new development in health care. Thus, the Workgroup looked at the potential benefits of these networks and the greater availability of health information; the new confidentiality, privacy, and security questions raised as a result; and whether this new paradigm warrants the imposition of new requirements to ensure adequate protections for electronic personal health information.

Many of our conversations about these new networks focused on who has access to them and for what purposes. For example, with an electronic health information exchange network, depending on its overall structure, it may be possible for a health care provider or caregiver (and potentially others) to access or request personal health information: 1) without a patient’s knowledge, and 2) without the knowledge of the provider whose record is the original source of that information. Further, it may be possible for those with access to a network to obtain 1) an individual’s information for purposes other than Treatment of the individual (as that term is defined in the HIPAA Privacy Rule) and 2) information about an individual with whom a provider has no current or prior relationship. In addition, as these networks continue to grow, health information will become more readily available, and the purposes for which these networks are used will likely expand as well. These possibilities which exist in some network situations can create new challenges to ensuring the confidentiality, privacy, and security of personal health information.

Going forward, careful consideration must be given to the type, function, and roles of entities gaining access to personal health information through electronic health information exchange networks. While specific rules for these networks have not been defined at the Federal level, existing Federal and State laws, the voluntary policies adopted by these networks, the CPS Workgroup’s prior recommendations, and recommendations by others such as the National Committee on Vital and Health Statistics (NCVHS), the Markle Foundation’s Connecting for Health Initiative, the eHealth Initiative, and consumer groups form an appropriate starting point. In considering how to appropriately address the new confidentiality, privacy, and security

concerns raised by these networks, we recognize that placing overly stringent and unjustified limits on the purposes for which information may be accessed through a network may limit its utility as a public good. At the same time, we also acknowledge the need to build public trust in these networks.

The recommendations we set forth below should help facilitate the future development of a confidentiality, privacy, and security framework to govern these networks.

### Application of HIPAA

Concerns have been raised that entities not covered by the HIPAA Privacy and Security Rules may be able to access personal health information in electronic health information exchange networks. Under our June 12, 2007 recommendation (the June 12th recommendation), these concerns could be alleviated if the HIPAA (or equivalent) privacy and security rules were made to apply to all those who directly participate in these networks. We recognize, however, that simply instituting such a “blanket HIPAA coverage” approach may not allay all concerns. In some situations, for example, the rules that were developed for a HIPAA covered entity may not be appropriate for another participant in an electronic health information exchange network (e.g., a public health entity or PHR vendor). In other situations, the CPS Workgroup recognized that it may not make sense to impose all HIPAA obligations on a network itself. For example, as detailed in our April 22, 2008 recommendations, we do not see an affirmative reason to require networks to send individual privacy notices to (and perhaps receive individual acknowledgments from) all individuals whose information flows through those networks, unless the networks have an independent relationship with these individuals. We did recommend that these networks be required to make their privacy policies and practices publicly available on their websites (or through other means) (see Appendix A for further details).

### What Rules Should Govern Network Access and Use?

While there is a substantial debate about the appropriate purposes of these networks, there is widespread agreement that effective and improved treatment (i.e., better outcomes and care coordination) should be at the heart of these networks. Moreover, improving treatment is one area and perhaps the only area where there is no significant debate or disagreement regarding appropriate access to these networks.

We understand that many of these networks would allow health care providers to query the network for all available information on a patient for Treatment purposes. Such a query would be similar to a health care provider calling each hospital, primary care provider, and specialist in a given area to ask for personal health information about a patient. The administrative efficiency gained by this new capability is readily apparent. But improvements in efficiency alone would not necessarily justify the creation of new privacy and security rules. The Workgroup believes that further conversation about the new challenges raised by networks should focus primarily on whether networks yield new opportunities to obtain and use data that warrant additional protections. Additionally,

the ease with which information will be accessible outside of the Treatment context raises some concerns. For example, the National Committee on Vital and Health Statistics (NCVHS), released a report entitled “Enhanced Protections for Uses of Health Data: A Stewardship Framework for “Secondary Uses” of Electronically Collected and Transmitted Health Data” that discusses this issue in greater detail.  
<http://ncvhs.hhs.gov/071221lt.pdf>

The CPS Workgroup considered whether it could come to consensus on a recommendation that would allow network participants to access information in the network for Treatment, Payment and Health Care Operations (as those terms are currently defined in the HIPAA Privacy Rule) or at least certain Health Care Operations (primarily those operations identified in the HIPAA Privacy Rule where one covered entity can provide information for another covered entity’s health care operations 45 CFR 164.506(c)(4)). Although CPS Workgroup members were comfortable with allowing participants to access the network for Treatment purposes to the extent permitted under Federal and State laws, some members raised concerns about allowing participants to access the network for Payment and some or all Health Care Operations. Others believed that a regulatory framework that “matched” the HIPAA environment meaning one where uses and disclosures for Treatment, Payment, and those Health Care Operations identified above - was more appropriate. Thus, the Workgroup believes that appropriate network uses should be the subject of further consideration by HHS, and that any HHS approach should be sufficiently flexible to not only regulate today's practices but also anticipate future technological and public policy changes.

Of note, much of the Workgroup discussion focused on appropriate uses of the network by participants those entities with some contractual obligation to, or rights in, the network. The CPS Workgroup acknowledges that entities that are not technically network participants could seek to gain access to information in the network and HHS should also consider the terms of such access, if any.

Recommendation 1: The CPS Workgroup recommends that HHS work with other stakeholders to create a set of guidelines for protecting the confidentiality, privacy, and security of information that is collected by, or shared through, an electronic health information exchange network. Such guidelines should cover who can access information in a network and for what purposes. This effort may require revisions to, or clarifications of, the HIPAA Privacy and Security Rules. HHS should give particular consideration to those areas where there are “differences” in the way that information is accessed, used, and disclosed in an electronic health information exchange environment as compared to what occurs absent the presence of electronic exchange.

#### Application of Minimum Necessary to Network Uses

The CPS Workgroup discussed the “minimum necessary” provisions of the HIPAA Privacy Rule. Some CPS Workgroup members raised questions about whether the minimum necessary standard needs to be reevaluated for a networked environment, particularly since the requirement does not apply in the context of disclosures to or

requests by a health care provider for Treatment. CPS Workgroup members have also raised concerns that the minimum necessary provision is inconsistently defined and frequently misunderstood; Privacy and Security Solutions for Interoperable Health Information Exchange: Nationwide Summary (07/2007) - [http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS\\_0\\_1248\\_661884\\_0\\_0\\_18/Nationwide.pdf](http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_661884_0_0_18/Nationwide.pdf)

and others point out that the standard is consistent with fair information practices and meant to be flexible and vary in its application depending on the context. If our June 12th recommendation is implemented, electronic health information exchange networks would be subject to the minimum necessary standard and thus would need policies on minimum necessary that would apply to all uses and disclosures outside of Treatment.

Nonetheless, the application of minimum necessary to an electronic health information exchange network raises several questions:

- Does the current minimum necessary requirement appropriately address the activities of electronic health information exchange networks?
- If an electronic health information exchange network uses a record locator service model and does not store personal health information, does the network need to establish “minimum necessary” policies? As an alternative, should the network rely on the sender and/or receiver of personal health information to comply with any minimum necessary requirements?
- Is it important for electronic health information exchange networks that maintain personal health information to have similar minimum necessary policies? Would variation amongst networks’ policies create potential exchange or interoperability challenges?
- How will network policies on consumer choice (for example, policies that require consumers to opt-in to having their information exchanged through the network or allow them to opt-out, or that allow consumers to restrict information in sensitive categories) interact with policies regarding “minimum necessary” and what impact will that have on electronic health information exchange?
- Should data recipients be notified if the information has been limited in some way because of rules established by a participant or a consumer’s choice (e.g., through a minimum necessary policy, State law restrictions, or consumer preferences)?

Recommendation 1.1: The CPS Workgroup recommends that the guidelines developed by HHS pursuant to Recommendation 1 (and any revisions to the HIPAA Privacy and Security Rules) address how “minimum necessary” would apply to the access, use, and disclosure of personal health information in or through a network. While the rules may not need to be revised for this context, there is sufficient confusion and concern about how the minimum necessary rule would apply in this exchange environment that, at a minimum, HHS should provide additional guidance on this issue.

## Use of Networks for Research and Public Health

The CPS Workgroup also considered the extent to which current research rules apply to persons or entities that access data from an electronic health information exchange network for research purposes. In a paper environment, a researcher would have to go to each source to obtain health information, but in a networked environment they could potentially gather information from multiple sources through one organization or network. Also, in today's environment, presuming that the information at issue is controlled by HIPAA covered entities, whether the information is paper or electronic, the HIPAA research rules would apply. Thus, many research entities would not have direct access to most health care information. If our June 12th recommendation were implemented, researchers who were network participants would need to follow the HIPAA Privacy and Security Rules directly. Our June 12th recommendation, however, does not address the question of whether researchers should in fact have direct access to these networks and, if so, whether the HIPAA Privacy and Security Rules are practical or effective in this context. Accordingly, HHS (and others) should give further consideration to how researchers can access information from these networks, and the terms and conditions of such access. Because the Institute of Medicine is currently conducting a study of the impact of HIPAA on research, the CPS Workgroup decided it was premature to give further consideration to this issue.

**Recommendation 1.2:** The CPS Workgroup recommends that the guidelines developed by HHS pursuant to Recommendation 1 (and any revisions to the HIPAA Privacy and Security Rules) address the potential uses and disclosures of personal health information for research purposes.

With respect to uses of a network for public health purposes, the CPS Workgroup received testimony on the current and anticipated public health uses of electronic health information exchange networks. Based on this testimony, such current and future uses include improving the current public health reporting structure by providing more efficient and effective mechanisms for health care providers to electronically report public health information to public health authorities as authorized or required, and using network connectivity as a tool to send public health information from public health authorities to health care providers. The Workgroup does not believe these activities raise any new confidentiality, privacy, or security issues. If in the future public health authorities anticipate or propose any new or broader uses of these networks, particularly as vehicles for direct access to information by public health entities, HHS should examine the impact on confidentiality, privacy, and security.

**Recommendation 1.3:** The CPS Workgroup recommends that HHS work with other stakeholders to continue to monitor whether there are any new confidentiality, privacy, or security issues related to the use or disclosure of personal health information through an electronic health information exchange network for public health.

## 2 - Policies Regarding a Network's Own Activities and Operations

One key difference that exists in an electronic health information exchange environment is that a network operator could become a repository of, or potentially access, substantial amounts of personal health information. Therefore, it is critical to evaluate what uses the network itself or its operator can make of this information. Today, similar issues arise in the context of certain business associates (for example, a pharmacy benefit manager who may have prescription information for numerous health insurers). We encourage consideration of whether the business associate model offers the appropriate level of control in this area, or whether more stringent controls should be placed on how a network itself uses and discloses information. This discussion needs to incorporate both the potential purposes and public benefits of these networks, as well as appropriate consideration of the business models utilized by these networks. Therefore, the CPS Workgroup believes that limits on the extent to which the network or its operator can access and use personal health information that it maintains or exchanges may need to be established.

Recommendation 2: As part of its effort to create a set of guidelines for protecting the confidentiality, privacy, and security of information maintained by or shared through an electronic health information exchange network pursuant to Recommendation 1, the CPS Workgroup recommends that HHS also work with stakeholders to consider the appropriate uses and disclosures of personal health information by and from the network itself i.e., whether and to what extent the network will be able to act independently in the use and disclosure of personal health information for its own purposes.

### 3 - De-Identification

Additionally, the ability of the network to connect previously segregated information may also create new opportunities for health data analysis and "data mining" for a variety of purposes. With respect to information that is individually identifiable, our prior recommendations with respect to the application of the HIPAA Privacy and Security rules to network participants, as well as to the networks themselves, should help resolve the confidentiality, privacy, and security issues raised by the use of networks for these purposes. However, the HIPAA Privacy Rule does not cover the use of de-identified health information, as long as such information meets the HIPAA standard for de-identification. The growth of these networks as well as the increased availability of information via public databases may make it easier for recipients of de-identified health information to re-identify it. The CPS Workgroup briefly considered but did not have the opportunity to fully evaluate whether the current de-identification standard developed over seven years ago would need to be revised in order to ensure that information accessed from networks cannot be easily re-identified.

Recommendation 3: HHS should conduct an analysis of whether the current HIPAA Privacy Rule de-identification standard provides sufficient protection against re-identification and consider revising the HIPAA Privacy Rule, as appropriate.

### 4 - Consistent Rules for Personal Health Information

In an environment where health care providers may receive numerous pieces of personal health information from a number of sources in order to treat an individual, it is important that the rules they have to follow with respect to protecting personal health information do not become so overly complex that they provide disincentives to using electronic health information exchange networks or create obstacles to providing patient care. During its discussions, the CPS Workgroup has been careful to identify and think through the potential impact new rules might have on the current environment. We believe that as policies develop for electronic health information exchange both for participants and the networks, such policies may vary by type of entity but should not require a particular entity to treat information differently depending on its source (i.e., from a network, generated by the provider, or obtained directly from another provider). For example, when a health care provider accesses personal health information on a patient using a network, such information will, in most cases, be included in the provider's record of care for that patient, and the same rules regarding how that information in a record can be accessed, used, and disclosed should apply. Two sets of rules one governing information obtained from a network and one governing information generated by the provider or obtained from other sources would be impractical and could have significant cost, care, and efficiency implications.

Recommendation 4: The CPS Workgroup recommends that as HHS develops policies, guidelines, or requirements for safeguarding personal health information exchanged in a networked environment, network participants should not be required to treat personal health information differently depending on its source.

## 5 - Roles, Rights, and Responsibilities of Consumers

Participants in electronic health information exchange networks across the country have engaged in discussions about ways to empower consumers and enable them to take a greater role in their own health care. Providing consumers with certain choices regarding how their personal health information is exchanged is important. However, rules governing networks must also consider the needs of health care providers and other entities to access, use, and disclose such information in order to function and properly treat patients.

The CPS Workgroup also recognizes that relying solely on consumer consent or choice without additional rules governing an electronic health information exchange network would not be an appropriate or sufficient way to protect the privacy and security of information in these networks, as such an approach places the burden solely on consumers to protect their personal health information. While the question of what consumer choice should be provided is an open one (and one where the CPS Workgroup has not reached a consensus), we are of the view that consumer choice alone is not the solution to privacy and security concerns in this exchange environment.

Recommendation 5: The CPS Workgroup recommends that policies, guidelines, or requirements developed by HHS with respect to electronic health information exchange networks specifically address the role of consumers and their caregivers (health care

providers, family members, and other authorized individuals). These policies, guidelines, or requirements should determine the degree to which consumers should be permitted to control the use or disclosure of their personal health information by an electronic health information exchange network.

Recommendation 5.1: The CPS Workgroup recommends that HHS consider appropriate requirements for electronic health information exchange networks and their participants to safeguard personal health information in a way that supports the choices afforded to consumers through Recommendation 5.

Recommendation 5.2: The CPS Workgroup recommends that when consumers are provided the opportunity to choose whether or not to share certain personal health information, that such a choice be accompanied by appropriate consumer education. In making this recommendation the CPS Workgroup did not discuss who should be responsible for educating the consumer. We recognize that consumer education can be done through multiple venues and using different resources, and we leave to further deliberation the most appropriate ways to accomplish this goal.

#### Policy Factors, Challenges, and Considerations for Protecting Electronic Health Information Personal Health Records

#### 6 Safeguarding Information in a Personal Health Record

With personal health records (PHRs) and other tools designed to help consumers become more engaged in their health care, we are witnessing an increasing migration of personal health information out of the traditional health care system, which raises new confidentiality, privacy, and security concerns. PHRs are “an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.” The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms, April 28, 2008. Some PHRs are currently offered by covered entities, others are not. Some PHR service providers will participate in electronic health information exchange through a network, and some may not. If our June 12th recommendation were implemented, those PHR service providers that directly participate in these networks will be responsible for complying, at a minimum, with the HIPAA Rules to the extent they participate in the network. And of course, those PHRs offered by HIPAA covered entities should be covered under HIPAA. But PHR service providers that do not participate in networks, and that are not offered by covered entities, will not be covered by HIPAA. Many of these “uncovered” PHR service providers are entering into business alliances with covered entities to make their PHR products available to these entities’ patients or enrollees. But it is not clear as a legal matter whether such PHR service providers would be required to enter into HIPAA business associate agreements in order to download a patient’s protected health information into his or her PHR, because the patient likely will

have authorized the disclosure of that information. Indeed, the premise of the most visible PHR service providers involves consumer authorization to access health care records.

The Federal Trade Commission (FTC) has some authority to regulate PHR service providers under the Federal Trade Commission Act. For example, if a PHR service provider does not abide by its privacy policies, the FTC may bring an action on behalf of the individuals with PHR accounts for deceptive trade practices. But such protection is fairly limited, as the PHR service provider is bound only by what it has promised in the privacy policy; the policy itself does not necessarily have to meet any particular requirements.

Some policymakers have considered, and some stakeholders have recommended, that all PHR service providers be required to comply with the HIPAA Privacy and Security Rules. But others have questioned whether HIPAA is the right regulatory framework for protecting personal health information in PHRs. HIPAA may, in fact, provide PHR service providers with “too much” ability to use and disclose health care information. For example, Microsoft, Google, and Dossia significantly restrict in their privacy policies their own uses and disclosure of personal health information. While these approaches are driven (presumably) by business concerns, we do not want to encourage an environment where PHR service providers believe they should increase their use and disclosure of personal health information beyond the best practices developing today.

Because PHRs contain copies of information from the electronic records of health care providers or health plans, in addition to any information that may be entered into the record by individuals (the subject of the record in question), information in PHRs should be controlled solely by the individual or persons acting on their behalf and the CPS Workgroup agrees that, as a policy matter, consumers should have the sole right to choose whether information held in a PHR is accessed or disclosed, to whom, and for what purposes. In contrast, the HIPAA rules were designed to govern the access, use, and disclosure of protected health information by entities in the traditional health care system, which is why the rules permit the use and disclosure of protected health information for a number of purposes (such as Treatment, Payment, and Health Care Operations, and public health) without the consent or authorization of the individual. Such a regulatory framework may not be an appropriate fit for PHRs, where information in the record can only be accessed, used, and disclosed with the express authorization of the individual.

**Recommendation 6:** The CPS Workgroup recommends that HHS work with other Federal agencies, such as the Federal Trade Commission, and stakeholders in the public and private sectors to create a set of guidelines, policies, or requirements for safeguarding personal health information within a PHR. For example, NCVHS released recommendations on PHRs in February 2006, and the Markle Foundation’s Connecting for Health Initiative Released a Common Framework for Consumer Access Services in June of 2008. These policies, guidelines, or requirements should support the right of consumers to control how information is used or disclosed from their PHR.

Recommendation 6.1: HHS should consider whether the HIPAA Privacy and Security Rules should be revised or clarified, as appropriate, to provide for the privacy and security of PHRs maintained by a covered entity or their business associates.

Finally, to reiterate a point we have made above, if different policies are developed for uses and disclosures of personal health information by a PHR service provider, once the information is transferred (per authorization of the consumer/patient) to a health care provider or health plan, and stored in that provider or plan's record, the rules that govern the provider or plan's subsequent use of that information should be the same as the rules that provider or plan follows with respect to information currently stored in their records.

## Conclusion

These recommendations are supported by information obtained through research and testimony to the Confidentiality, Privacy, and Security Workgroup, which is contained in the supporting documents available at <http://www.hhs.gov/healthit/ahic>.

Thank you for giving us the opportunity to submit these recommendations. We look forward to discussing these recommendations with you and the members of the American Health Information Community.

Sincerely yours,

/Kirk J. Nahra/

Kirk J. Nahra, Co-Chair

Confidentiality, Privacy, and Security Workgroup

/Deven McGraw/

Deven McGraw, Co-Chair

Confidentiality, Privacy, and Security Workgroup

## Appendix A Recommendation History

On May 16, 2006, the AHIC received, and accepted, a joint recommendation from its Consumer Empowerment, Electronic Health Records (EHRs), and Chronic Care Workgroups to create another AHIC Workgroup comprised of privacy, security, clinical, and technology experts to frame the privacy and security policy issues relevant to all AHIC Workgroup charges and solicit broad public input and testimony. The joint recommendation charged the CPS workgroup to address issues such as methods of patient identification; methods of authentication; mechanisms to ensure data integrity; methods for controlling access to personal health information; policies for breaches of personal health information confidentiality; guidelines and processes to determine

appropriate secondary uses of data; and a scope of work for a long-term independent advisory body on privacy and security policies.

- Our first set of recommendations, which were accepted at the 1/23/2007 AHIC meeting, focused on patient identity proofing. We recommended that:
  - Entities that offer electronic access to data and services through secure messaging, personal health records (PHRs), or EHRs follow our framework for patient identity proofing;
  - For the purposes of secure messaging and accessing data through a PHR or EHR, information used solely for purposes of identity proofing a health care consumer or their authorized proxy(ies), if kept, should be securely maintained separate from the health care consumer's clinical data;
  - Converting from a paper-based health care practice to one that uses EHRs does not require a health care entity to identity proof their patients unless such conversion provides patients with access to data within the EHR;
  - Entities providing patient access to personal health information via secure messaging or a PHR should follow our identity proofing framework; and
  - Where applicable, the Certification Commission for Healthcare Information Technology (CCHIT) should develop certification criteria for the systems and networks they certify to support the identity proofing practices in our recommendations.
  
- In June 2007, we issued another recommendation, which marked a significant step forward in our efforts to determine what, if any, additional protections beyond those currently provided in federal and state law are needed to ensure the confidentiality, privacy, and security of individually identifiable health information in an electronic health information exchange environment. This recommendation was accepted at the 6/12/2007 AHIC meeting and provided that:
  - All persons and entities, excluding consumers, that participate directly in, or comprise, an electronic health information exchange network, through which individually identifiable health information is stored, compiled, transmitted, modified, or accessed should be required to meet enforceable privacy and security criteria at least equivalent to any relevant Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements (45 CFR Parts 160 and 164). Furthermore, any person or entity that functions as a Business Associate (as described in 45 CFR §160.103) and participates directly in, or comprises, an electronic health information exchange network should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements, independent of those established by contractual arrangements (such as a Business Associate Agreement as provided for in HIPAA).
  
- Our third set of recommendations, accepted by AHIC on 4/22/2008, further refined our previous recommendation by pragmatically exempting health information exchange networks that do not currently have direct relationships

with patients from having to directly comply with certain requirements of the HIPAA Privacy Rule. With respect to those networks that do not currently have direct relationships with patients;

- The obligation to provide the following “individual rights” under the HIPAA Privacy Rule would remain with the health care provider or health plan who is the original source of the patient data and who today has a direct relationship with the patient:
  - §164.520 Requirement to provide the patient with a notice of privacy practices for protected health information and to have receipt of that notice acknowledged by the patient;
  - §164.522 Right to request a restriction on protected health information;
  - §164.524 Right of individuals to access (inspect and copy) their protected health information;
  - §164.526 Right to seek amendment of protected health information; and
  - §164.528 Right to an accounting of disclosures of protected health information.
  
- Our recommendation also provided that electronic health information exchange networks which have direct relationships with consumers or patients should be required to meet all of the requirements of the HIPAA Privacy Rule. Moreover, we recommended that electronic health information exchange networks be required to make publicly available on their website (or through other means) a document that reasonably and accurately describes in plain language how they use and disclose health information and their privacy policies and practices, as well as how they safeguard patient or consumer information.