

January 23, 2007

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 has identified and prioritized several health information technology applications, or “breakthroughs,” that could produce a specific tangible value to health care consumers. To address one of these breakthrough areas, the Confidentiality, Privacy, and Security (CPS) Workgroup was formed and given the following Broad and Specific Charges:

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

**Specific Charge for the Workgroup:** Make actionable confidentiality, privacy, and security recommendations to the Community 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.

## BACKGROUND AND DISCUSSION

The following recommendations were developed by the American Health Information Community (AHIC) Confidentiality, Privacy and Security (CPS) Workgroup on the topic of patient identity proofing. They seek to advance the Specific Charges of the Consumer Empowerment, Electronic Health Record (EHR), and Chronic Care Workgroups and are not intended to introduce barriers to the efficient and effective provision of health care.

Furthermore, the recommendations below intend to establish a baseline for patient identity proofing in the electronic health information exchange environment. Where a particular recommendation presents a range of possible options for patient identity proofing, those options should be evaluated in the context of the specific environment to ensure the appropriate confidentiality, privacy, and security protections are put in place.

We suggest that these recommendations, if accepted by the AHIC, be considered by the Department of Health and Human Services (HHS) for adoption as HHS policy regarding current and future activities, including appropriate federal contracts, and pilot and demonstration projects as they relate to the specific Workgroup charges listed below and their broad charges where appropriate. Furthermore, it is the Workgroup's intention that these recommendations apply more broadly to the health care system, and that public and private sector organizations would parallel HHS in their implementations.

## GENERAL STATEMENTS

1. We defined patient identity proofing as the process of providing sufficient information (e.g., identity history, credentials, documents) to correctly and accurately establish and verify an identity to be used in an electronic environment (e.g., via the Internet).
2. The purpose of these recommendations is to advance the specific charges of the Chronic Care, EHR, and Consumer Empowerment Workgroups. The Workgroup discussions and these recommendations are related solely to the following issue areas. More widespread application of these recommendations may necessitate further review.
  1. Chronic Care - Make recommendations to the Community so that within one year, widespread use of secure messaging, as appropriate, is fostered as a means of communication between clinicians and patients about care delivery.
  2. EHR - Make recommendations to the Community so that within one year, standardized, widely available and secure solutions for accessing current and historical laboratory results and interpretations are deployed for clinical care by authorized parties.
  100. Consumer Empowerment - Make recommendations to the Community so that within one year, a pre-populated, consumer-directed and secure electronic registration summary is available to targeted populations. Make additional recommendations to the Community so that within one year, a widely available pre-populated medication history linked to the registration summary is deployed.
3. All data included in secure messaging, EHRs, and Personal Health Records (PHRs) should be considered sensitive. Appropriate policies and supporting security measures must be in place to mitigate the risks of unauthorized or unintended data disclosure.
4. It is important to understand that patient identity proofing is just one part of an overall process (e.g., validation, revocation) for issuing and maintaining electronic identity credentials. All parts of the process are interdependent and, if they do not achieve comparable levels of security, the overall strength of the electronic identity credential may not be adequate.

## RECOMMENDATIONS

Recommendation 1: Entities that offer health care consumers or their authorized proxy(ies)[FN1] electronic access to data and services through secure messaging, PHRs, or EHRs should perform, or rely upon, identity proofing performed by the entity or an accountable trusted third party[FN2] that meets or exceeds one of the following options (1.1, 1.2, 1.3). Note: If the primary method chosen by an entity does not apply in some instances, one of the other methods below should be chosen. Failure to meet identity proofing requirements for electronic access to health information should not impede patient access to health care.

### 1.1:

When it is practical and feasible for a health care consumer or his/her authorized proxy to present themselves in-person, in-person identity proofing should be performed by the health care entity. Identity proofing can be achieved by using, at a minimum, a valid, government issued, picture-ID to verify identity. Examples of such documents include: A passport; driver's license or state issued ID; permanent resident card; military ID.

### 1.2:

When the healthcare consumer or his/her authorized proxy has an established and durable relationship (e.g., long-standing, trusted) with an entity, this relationship could be used to confirm the consumer or proxy's identity on the basis of that relationship. Examples of confirmation may include: in-person or telephonic dialogue, etc., where confirmation occurs at the time of the request. (i.e., a voicemail or message left for the entity to confirm at later time would not be acceptable).

### 1.3:

When the healthcare consumer or his/her authorized proxy is unable to meet the criteria necessary to satisfy 1.1, the entity determines that 1.2 is not viable, and a relationship exists between the consumer or proxy and the entity, identity proofing should consist of a method that verifies a person's identity based on information they know or can produce about themselves when asked. The entity or trusted third party should 1) request basic identity data (e.g., name, address, date of birth, etc.), and 2) require the individual to provide some personal information specific to that relationship (e.g., last prescription, electronic device).

The CPS Workgroup recognizes that some entities may offer PHRs and related services to health care consumers with whom they have no prior relationship. These may include PHRs that are not in any way connected to other information, or can include more "integrated/interoperable" PHRs. The Workgroup began to explore this difficult issue in its public meetings and has considered oral and written testimony, but needs further information before it can make recommendations with regard to identity proofing in these situations.

We have concluded that option 1.1 above - in-person identity proofing might be used in some of these circumstances. In other cases, option 1.1 may not be practicable. We will be exploring alternative mechanisms to identity proofing by the entity itself (e.g., through a trusted third party) to enhance the opportunities for identity proofing in these circumstances. The Workgroup did not reach a consensus on other options that could provide a sufficiently protective method to identity proof in circumstances when the credentialing cannot take place in-person. We will continue to consider this issue in future discussions to examine whether appropriate alternatives offering similar protections exist (or are expected to emerge).

Recommendation 2: For the purposes of secure messaging and accessing data through a PHR or EHR, document(s) and the information therein or other 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.

Recommendation 3: 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. Where this conversion also provides patients with access to data within the EHR (such as via flash drive, Internet, or remote access), health care providers should follow the identity proofing recommendation schema noted in Recommendation #1.

Recommendation 4: Entities that provide patient access to personal health information via secure messaging or a PHR (such as via a flash drive, populating data records stored on the Internet, or remote access), should follow the identity proofing recommendation schema noted in Recommendation #1.

Recommendation 5: 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 these recommendations.

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

Co-chair

Confidentiality, Privacy, and Security Workgroup

Sincerely yours,

Paul Feldman

Co-chair

Confidentiality, Privacy, and Security Workgroup

1 The Workgroup would assume that establishing authority to act as a proxy would mirror the HIPAA Privacy Rule's provisions for personal representatives (45 CFR §164.502 (g)), applicable state law requirements, or would require patient authorization.

2 A trusted third party is an entity that both the health care consumer or their authorized proxy and health care entity trust or can reasonably rely upon, for the purpose of performing identity proofing on behalf of the entity.