American Health Information Community

Confidentiality, Privacy, & Security Workgroup

Hearing on Identity Proofing and User Authentication

September 29, 2006

Panel III – Identity Proofing and User Authentication Methods to Provide Access to Current and Historical Laboratory Results and Interpretations in an Electronic Health Record

Written Testimony: Michael H. Zaroukian, MD, PhD, FACP

Chief Medical Information Officer, MSU HealthTeam

Associate Professor of Medicine, Michigan State University

Chairman Feldman and Nahra, Workgroup members, panelists, and guests:

Thank you for inviting me to share my thoughts regarding methods for identity proofing and user authentication to provide access to current and historical laboratory results and interpretations in an electronic health record, or EHR. The opinions I will share today are informed by my day-to-day work as a primary care physician communicating electronically with patients and my personal and organizational experience with EHR and other health information technology, including 1) directing the enterprise-wide implementation of an advanced ambulatory EHR system at a large public university; 2) my tenure as national president of an independent EHR user association; 3) my participation in the university's cybersecurity initiative and privacy board; 4) my role in the development and pilot implementation of a secure patient portal and messaging website; and 5) my perspectives as principal investigator for a Regional Health Information Organization planning grant in mid-Michigan.

In response to the first question, I believe that identity proofing and user authentication methodologies should differentiate based upon the data reception method and the interconnectivity of specific EHR systems. Results directly transmitted from a laboratory source system to auto populate structured data fields in an EHR would not need to have distinct identity proofing and authentication technologies, policies and implementation strategies. Instead, identity proofing and user authentication would leverage the processes used by the receiving EHR system.

However, when a person directly accesses a laboratory's secure website to view, copy, transcribe, or otherwise transfer results to the receiving EHR system, high-assurance identity proofing should be required for initial website registration, followed by the presentation of identity credentials that yield high-confidence user authentication for each login.

Manual transfer of results from a laboratory system's secure website to an EHR carries with it substantial potential threats to data integrity and patient safety if errors are made or data are deliberately altered. As such, it is reasonable to consider strong identity proofing and user authentication strategies for health professionals who engage in such activities. However, final decisions should reflect consideration of: 1) the potential impact of authentication errors (i.e., inconvenience, suffering, reputational damage, financial loss, personal safety, or legal jeopardy); 2) the likelihood that such errors will occur, 3) the cost of implementing and maintaining each strategy under consideration; 4) the burden placed on the user for identity proofing and authentication; and 5) the acceptability of the authentication technologies, policies and procedures to those expected to use them.

The act of querying another provider's EHR for data (e.g., in-office laboratory results) can add additional layers of complexity. Direct connections between EHR systems in different practices create security vulnerabilities that can be exploited by unauthorized users. It is likely that the entity sending results from its EHR would require that those accessing its system adhere to its policies and practices for identity proofing and user

authentication. Depending on the authentication strategies required, this could rapidly become unmanageable in regions where retrieval of information from multiple disparate systems is desired but a health information exchange and interoperability (HIEI) utility is not available to allow for a uniform, secure approach to identity proofing and user authentication.

Turning to the question of expecting private industry EHR services to comply with Federal information security practices when importing data from Federal agencies, I believe that expecting compliance with such practices is reasonable as long as existing statutes or policies allow for efficient access for authorized users at a reasonable cost. However, if existing statutes or policies impose an undue burden in this regard, efforts should be made to amend them.

It is reasonable to expect different identity proofing and user authentication processes for patients and clinicians, who can differ considerably in their computer literacy, computing assets, IT support, and other important variables that could affect their ability to access and use HIT systems. As such, some identity proofing and user authentication methodologies (e.g., complex passwords, biometrics) will not be suitable for many patients. Authentication workflow efficiency for patients may be a less critical issue because patients would only be occasional system users.

On the other hand, as frequent users of the same system, clinicians have a critical need for efficient, reliable and ubiquitously available user authentication strategies. Any system that fails to meet reasonable clinician usability expectations is likely to be underused or result in authentication "workarounds" that could increase system vulnerability and compromise patient data privacy, confidentiality, and security.

As to the question of the role DHHS should play in establishing guidelines for identity proofing and user authentication vs. healthcare industry self-policing in this area, I don't see these options as mutually exclusive. I believe that providers, patients, HIT vendors, and other stakeholders would welcome and benefit from DHHS' provision of clear, practical, and implementable guidelines. At the same time, I would caution DHHS to refrain from imposing regulations that prescribe specific identity proofing and user authentication methods. The Certifying Commission on Health Information Technology (CCHIT), with input from the EHR/HIT stakeholder community, should also continue to incorporate the latest science and best practices for ensuring the privacy, confidentiality, and security of protected health information in its EHR certification criteria.

Considering the issue of whether in-person identity proofing processes or automated on-line processes provides greater benefit, the conventional wisdom in healthcare is that in-person identity proofing is necessary to be confident that the asserted identity of an individual is correct. The combination of a government issued photo ID and health insurance documents is usually considered sufficient for initial identity proofing for new patients in typical healthcare settings. In-person identity proofing is required in my practice to issue initial user authentication credentials for registration to our secure patient portal website where patients can access information about their own health conditions, view results or engage in other online healthcare transactions involving protected health information.

However, requiring in-person identity proofing to grant initial access to a secure system can increase the inertia to registering to use a secure system compared with online processes, particularly for disabled patients and busy providers who may have to complete in-person identity proofing for multiple, geographically separated healthcare entities (hospitals, laboratories, other physician practices, etc.). This can delay or decrease patient and provider participation, thereby diminishing the beneficial impact of the system.

Other industries use technologies, policies and practices for identity proofing and user authentication that could improve secure access to online information if applied to healthcare. For example, the banking industry uses two-factor authentication approaches that have been well-accepted and commonly used by consumers to establish identity. Such authentication requires the use of two independent factors, such as presenting “something you have” (an ATM card) and “something you know” (a personal identification number, or PIN). While cards and other hardware token solutions (e.g., smart cards, USB tokens, one time password tokens) will continue to evolve as security vulnerabilities are found and exploited, the form factor will need to continue to be acceptable to prospective users (e.g., tokens must be easy to use and small enough to be carried in a pocket, wallet or purse or attached to a keychain).

While two-factor authentication represents an improvement over single-factor authentication with a user password, it is vulnerable to Trojan attacks as well as phishing or “Man-in-the-Middle” attacks, making the combination of technology, communication strategies (e.g., never send users an e-communication requesting personal information), and user education (e.g., ensuring anti-virus, anti-spyware, and firewall protection) important for mitigating these risks.

In 2001, the Federal Financial Institutions Examination Council (FFIEC) published a set of guidelines for authentication in an internet banking environment that can inform similar approaches in healthcare. Implementing two-factor authentication in a manner that is effective and acceptable for patients and providers who may need to be able to access a secure website from different Internet-connected computers in multiple locations will likely make "who you are" authentication (e.g., thumbprint biometric devices) unfeasible in the near term, and would favor certain “what you have” approaches, such as USB tokens with one-time passwords. Feasibility would likely hinge on each user being able to avoid having to carry multiple hardware tokens to authenticate across disparate systems.

Balancing accessibility to medical information in electronic form with the need to be responsive to the privacy concerns of the consumer/patient is complicated by widely varying patient views regarding the degree to which their specific health information (i.e., immunizations vs. mental health data) should be treated as confidential (1, 2). For example, hundreds of patients in my own practice knowingly transmit their health information to providers using standard, unencrypted email systems despite warnings regarding the lack of security controls and the availability of a secure patient portal. This underscores the relative lack of concern for security among some patients, as well as their prioritization of user convenience over confidentiality. These and other data from the literature (3, 4) suggest that convenience is a critical success factor for implementing identity proofing and user authentication to secure websites for retrieval and communication of health information. At a minimum, the combined burden of identity proofing, user authentication and results retrieval for providers will probably have to be lower than the time and effort required to order the same tests. I am not aware of any studies that have looked at the impact of requiring two-factor authentication on the willingness of providers or patients to use a secure website to retrieve results.

I believe it would be appropriate for the healthcare industry to adopt the concept of multiple assurance levels analogous to those defined in OMB Memorandum M-04-04 (modified to reflect healthcare impact categories) for identity proofing and user authentication in granting access to EHR data. The current processes used to credential physicians for hospital privileges represents a model in this regard, in which established mechanisms exist for proving the identity, education, training, certification, and procedural experience of individual providers before granting them access to certain hospital resources or privileges to perform specific tasks. At the same time, I would caution against recommending strategies that require repeated authentication within an information system

that a provider has already authenticated to, such as requiring physicians to enter a password within the system to be able to view an HIV test result or write a prescription for a narcotic medication.

The main concerns I have regarding the type of information collected and stored for identity proofing relate to the possibility that the information could be used for identity theft or to otherwise bring harm to the individual, as outlined in the potential impact categories defined in OMB Memorandum M-04-04. In general, only the minimum amount of personal identity information needed to achieve a high level of identity assurance should be collected, and any retained information must be securely maintained.

I have additional concerns regarding the collection and storage of biometric data, such as fingerprints, voiceprints, hand geometry, and iris or retinal scans. The possible theft or misuse of such highly identifying data could cause significant harm, including the possibility that biometric data could be used for identity vetting across national background checking databases that might reveal highly sensitive information regarding an individual's past behavior or misidentify an individual as being a patient safety or data security risk.

I hope this information has been helpful. Thank you.

References:

1. Dick RS, Steen EB, Detmer DE, eds. *The Computer-Based Patient Record: An Essential Technology for Healthcare, Revised Edition*. Revised Edition ed. Washington, D.C.: National Academy Press; 1997.
2. Hassol A, Walker JM, Kidder D, et al. Patient experiences and attitudes about access to a patient electronic healthcare record and linked web messaging. *J Am Med Inform Assoc*. 2004;11(6):505-13.

3. Tjora A, Tran T, Faxvaag A. Privacy vs usability: a qualitative exploration of patients' experiences with secure Internet communication with their general practitioner. *J Med Internet Res*. 2005;7(2):e15.

4. Masys D, Baker D, Butros A, Cowles KE. Giving patients access to their medical records via the internet: the PCASSO experience. *J Am Med Inform Assoc*. 2002;9(2):181-91.