TESTIMONY FOR
AMERICAN HEALTH INFORMATION COMMUNITY'S
CONFIDENTIALITY, PRIVACY, & SECURITY WORKGROUP
29 September 2006

Michael Weiner, M.D., M.P.H.
Associate Professor of Medicine, Division of General Internal Medicine & Geriatrics,
Department of Medicine, Indiana University School of Medicine
Center Scientist, Indiana University Center for Aging Research
Research Scientist, Regenstrief Institute, Inc.
Director, Gero-informatics Program, Indiana University Geriatrics
1050 Wishard Boulevard, 6th floor
Indianapolis, Indiana 46202-2872
Tel. 317-630-7760

I would like to thank the Confidentiality, Privacy, and Security Workgroup for this opportunity to discuss security of messaging between patients and their clinicians.

At Regenstrief Institute and the Indiana University Center for Aging Research in Indianapolis, Indiana, I conduct research in medical informatics and geriatric medicine. My work includes studies of secure communications between patients and clinicians, including videoconferencing and methods using computers, telephones, and fax machines. As a physician, I use a comprehensive electronic medical record system to provide primary medical care to an urban population and to communicate with colleagues about my patients. As a patient, I have used the Internet to communicate with my own physicians. I will now discuss risks, benefits, barriers, and potential solutions for issues around secure messaging in healthcare.

The problem of security of health data originated years before personal computers were invented. Paper-based medical records are in many ways the least secure form of health data, whether in the hands of the patient or a medical provider. Paper is easily misplaced, lost, intercepted, and read by unauthorized parties.

Fortunately, computers provide opportunities to improve speed, efficiency, cost, and security of communications. Clinical electronic messaging can advantageously decrease the number of office visits in a general medical practice (1). Although clinical messaging is not just about electronic mail (e-mail), a third to three quarters of patients in the U.S. have access to e-mail, and research indicates that most patients feel that e-mail would be a useful way to communicate with their physicians. Up to 35% of patients have engaged in such communications.

Secure clinical messaging, whether by e-mail or not, requires identity proofing and user authentication. Identity proofing involves providing sufficient information, such as credentials or documents, to establish and verify an identity accurately. A subsequent authentication process (i.e., user authentication) involves reliably verifying a presented identity, such as to grant access to data or resources. Why is identity proofing separate from user authentication? The difference is largely practical. Identity proofing is meant to be a somewhat exhaustive review of permanent or what might be considered semi-permanent credentials. Since proofing has so far proven too inconvenient for everyday use, user authentication provides a rapid, easy method to verify an identity on an ongoing, often frequent basis.

Americans face multiple difficulties with secure messaging. Due to growth of regional populations and mobile workforces, many clinicians are relatively less likely to know, personally, each patient and the patient's family. Disabled patients may require proxies for authentication, and locating proxies and establishing their identities can be difficult and time-consuming, especially in a medical crisis. Clinicians and patients must access multiple, disparate systems, but remembering many authentication codes is difficult, and carrying written documentation of codes increases risk. Spoofing or faking an identity—the failed authentication—is common with

e-mail, and conventional e-mail systems do not provide strong authentication. Furthermore, with standard e-mail, passwords can be intercepted, and messages often land on multiple readable servers on the way to their destinations.

What is needed for accurate identity proofing in clinical messaging? I suppose if we had a DNA stamp at birth and another one at the proofing, and they matched, it might be perfect. In the real world, the goal is matching a person to the person's correct credentials, and statistics tell us that the more credentials we require, the more chances we have to be specific, at least under common circumstances. Although there is no perfect way to do this, especially with multiple, geographically separated systems, in-person identity proofing adds a measure of benefit. Through its deliberate and useful inconvenience, it requires more time and effort, adds one credential—a physical person—and provides the proofing agent with the opportunity for a personal inspection. Less involved methods of proofing increase the opportunity to misuse automation or match multiple credentials to one person.

The key is not so much whether in-person proofing should be done but how and when. Proofing should differ between clinicians and patients because, for patients, proofing is best accomplished directly with the physician, in the examination room. The physician sees the patient and establishes the credentialing on the spot. This is easy, customized, fast, and accurate, because the patient being evaluated is by definition the "real" patient and can directly receive information about future communications. For clinicians, on the other hand, the in-person proofing can be done in affiliation with an accredited institution, in advance of the messaging. Institutions, such as hospitals or medical practices, that provide clinical messaging should be subject to standard processes of accreditation that ensure minimum levels of security for events such as proofing.

The same goes for user authentication. User authentication in common electronic systems, such as e-mail and medical record systems, is most often done with combinations of username and password. For most purposes, authentication should require no more than a few seconds; for clinicians who log into information systems every few minutes, several seconds may even seem prohibitive. Frequently changing passwords theoretically increases security but causes inconvenience, especially via forgetting of short-term passwords. One-time password schemes, such as S/key, increase security but become inconvenient for repeated access to a system. RSA <http://www.rsasecurity.com/>, a division of EMC Corporation, has created SecurID, which creates a new, time-dependent password as often as every 60 seconds and provides the updated password directly for the user on a keyring-sized hardware token with a digital display. Although this approach has been quite successful—the company claims a 15-year track record with no reported security breaches—and provides a balance of preserved convenience and increased security, the physical devices are expensive (about $50 for a two-year license) and subject to loss and theft. Due to its limitations, SecurID is more feasible for use by clinicians than by patients.

An alternative approach is biometrics, by which a person-dependent attribute, such as a fingerprint or retina, is immediately analyzed and interpreted. This approach is also fast, successful, secure, reasonably accurate, and difficult to change. It is a viable option for many monitored environments, but lack of control over unmonitored authenticating machines increases the level of risk in those settings. Few medical institutions have deployed biometrics products on a large scale, though the prices for products such as fingerprint readers are dropping.

We do, of course, need to balance access to medical information with patients' privacy-related concerns. A treating physician without access to any medical data is usually partially

blindfolded in effect. I would not choose to receive medical care under such conditions. Nevertheless, patients should control who has access to data about their health and healthcare and when, but they should preferably determine this in advance of a crisis. This might mean providing permission to certain parties who are individually unknown at the time of specification.

For secure messaging, we need a way not only to authenticate the recipient but to authenticate the sender and protect and confirm the integrity of the message. By using a set of public and private keys or codes, public-key authentication systems can increase confidence levels in authenticating the sender and receiver and also encrypting the message in transit, minimizing the chance of interception. The keys are difficult to break or hack simply because they are long sequences of data, so even many random guesses in sequence are unlikely to succeed. PGP Corporation <http://www.pgp.com/> has provided such encryption products for several years. Public-key architectures provide ready, secure protection but have not been readily available in any major commercial e-mail system. Since they must typically be purchased or added separately and often unnecessarily require manual configuration, they are inconvenient and not widely used by the public. Public-key systems should be more convenient, consumer-friendly, and widely available and used, especially in commercial e-mail and health data systems.

The World Wide Web has provided a popular solution to many of these issues: Web-based e-mail. Web mail provides basic password-based authentication but can automatically encrypt messages from end to end and can provide streamlined documentation of a conversation, an essential feature in healthcare. Web mail is also relatively easy to configure and can provide access controls, message templates, customized messages, and routing (2). Today's Web browsers can also handle additional security certificates relatively easily. Although

vulnerabilities of keystroke logging and pirating from public terminals (3) persist, Web mail provides a useful blend of security, accessibility, cost, and ease of use. For communication of non-urgent problems, Web messaging is preferred over telephone by both providers and patients (4).

The need for strong authentication is not limited to a role or set of roles. Patients, proxies, and clinicians will require authentication at the appropriate times. These roles should most generally be considered equal in terms of the need to have qualifying criteria for proofing or authentication. Falsifying an identity can have widespread consequences, whether from the patient's or the clinician's perspective. Any storage of information used to match credentials with individuals will, of course, require a security method of its own, such as strong encryption, limited physical access, audit trails (5), and the other related and familiar methods of providing a multi-layered approach to protecting data (6).

What conformity and standardization of proofing and authentication are needed? There isn't just one correct answer in the industry, and we need room to grow and provide continual improvement on our methods. Patient-centered healthcare occurs one conversation at a time. At this level, justifying the complexities and costs of implementing multiple assurance levels in performing identity proofing and user authentication would appear difficult. Boosting adoption of safe technologies, however, does sometimes require new policy, rather than waiting for the market. Our federal government can help, not by creating guidelines or determining appropriate methods of achieving security, but by recommending minimum security schemes for protection. The federal government should also continue to stay involved in the creation, promotion, and adoption of data standards for storing and transmitting data. Although experts are likely to disagree about the best methods for achieving security, it is clear to all that widespread use of

data standards is needed for unanticipated and anticipated transfers of data among institutions, and inability to transfer data efficiently clearly jeopardizes healthcare.

In summary, several effective methods for effective protection of data are available but are expensive, unnecessarily difficult to use, or not widely available. Addressing these limitations of cost, ease of use, and availability will go a long way towards improving security. As secure messaging is pursued, we must always address three points. First, harm to a patient as a result of breaching security of clinical messaging is extremely rare, and our solutions should be consistent with a real or realistic level of harm. In many environments, threats to security of clinical messaging are exaggerated; these should be assessed carefully. Many citizens rely on less secure methods of authentication for personal banking systems that are routinely used to transfer large sums of money. Second, we must consider whether increasing the security of messaging provides limited, unfair, skewed, or unreasonable access to healthcare. We know, for example, that if the telephone were prohibited as a means of messaging, many of today's patients would be left at a disadvantage, perhaps without access to needed technologies or devices. Third, we must consider whether increasing security of messaging will hinder the patient-physician relationship (7). This two-way or multi-way relationship is fragile and essential to effective, desirable medical care. Many methods of implementing or augmenting security are available, but if we choose ones that provide a level of protection, privacy, or convenience that our public does not want and need, then we have not improved comfort, service, or health.

REFERENCES

1. Bergmo TS, Kummervold PE, Gammon D, Dahl LB. Electronic patient-provider communication: will it offset office visits and telephone consultations in primary care? Int J Med Inform 2005; 74 (9):705-10.
2. Liederman EM, Lee JC, Baquero VH, Seites PG. Patient-physician web messaging. The impact on message volume and satisfaction. J Gen Intern Med 2005; 20 (1):52-7.
3. Gerstle RS. E-mail communication between pediatricians and their patients. Pediatrics 2004; 114 (1):317-21.
4. Liederman EM, Morefield CS. Web messaging: a new tool for patient-physician communication. J Am Med Inform Assoc 2003; 10 (3):260-70.
5. de Meyer F, Lundgren PA, de Moor G, Fiers T. Determination of user requirements for the secure communication of electronic medical record information. Int J Med Inform 1998; 49 (1):125-30.
6. National Research Council. For the Record: Protecting Electronic Health Information. Washington, DC: National Academy Press, 1997.
7. Mandl KD, Kohane IS, Brandt AM. Electronic patient-physician communication: problems and promise. Ann Intern Med 1998; 129 (6):495-500.

Michael Weiner MD

Digitally signed by Michael Weiner
DN: cn=Michael Weiner, sn=Weiner, givenName=Michael, email=mw@cogit.net
Reason: I am the author of this document
Location: Indianapolis, Indiana, U.S.A.
Date: 2006.09.26 11:10:21 -04'00'