Maintaining the Confidentiality of Medical Records Shared over the Internet and the World Wide Web

David M. Rind, MD; Isaac S. Kohane, MD, PhD; Peter Szolovits, PhD; Charles Safran, MD; Henry C. Chueh, MD; and G. Octo Barnett, MD

The Boston Electronic Medical Record Collaborative is working to develop a system that will use the World Wide Web to transfer computer-based patient information to clinicians in emergency departments. Maintaining adequate confidentiality of these records while still facilitating patient care is paramount to this effort. This paper describes an explicit protocol that would make it possible to electronically identify patients and providers, secure permission for release of records, and track information that is transmitted. It is hoped that other, similar efforts now underway will be able to use and build on this model. Comment on this proposal is invited from all parties with an interest in confidentiality. The system will be used only with "scrubbed" data—data from which all identifiers have been removed—until it is generally agreed that the confidentiality methods proposed here are appropriate and sufficient.

Ann Intern Med. 1997;127:138-141.

From Beth Israel Deaconess Medical Center, Massachusetts General Hospital, Children's Hospital, and Harvard Medical School, Boston, Massachusetts; and Massachusetts Institute of Technology, Cambridge, Massachusetts. For current author addresses, see end of text.

Safe, comprehensive, and cost-effective patient care depends on the provider's ability to obtain an accurate record of the patient's previous health care, including treatments and testing. Without this information, tests may be repeated or previous results ignored, allergies may not be known, and information about drug regimens may be miscommunicated. Never is the need for rapid access to information more apparent than when a patient seeks emergency care. When patients who are usually cared for at one institution go to the emergency department of another institution, there is reason to be concerned that missing information may result in less than optimal care. Inappropriate care caused by lack of access to information may delay diagnosis and result in improper therapy, iatrogenic illness, and increased health care costs. In the emergency care of an unconscious patient, lifesaving information may be unavailable.

The Boston Electronic Medical Record Collaborative is working to develop a system, the World Wide Web Electronic Medical Record System (W3-EMRS), that will use the Internet and the World Wide Web (1) to transfer hospitals' computer-based patient information to the emergency departments of participating institutions. We hope that this system, which has been described elsewhere (2–4), will alleviate the knowledge deficit of emergency care providers by improving their access to relevant patient information. The Collaborative, which consists of informatics researchers from three hospitals in Boston and the Massachusetts Institute of Technology, was created by a cooperative agreement award from the National Library of Medicine and the Agency for Health Care Policy and Research; institutional policies about the electronic transfer of patient information remain under active discussion.

An obvious and serious concern in a system such as W3-EMRS is the confidentiality and security of patient information. We propose an approach that we hope will define a standard for protecting the confidentiality of patient information while improving patient care by allowing emergency access to patient records. In this paper, we put forward our proposal and explain the principles and assumptions that underlie it.

These principles and assumptions are as follows. First, we recognize that tradeoffs between access and confidentiality must generally be made; it is not possible to achieve both perfect confidentiality and perfect access to patient information, whether that information is computerized or handwritten. Certain actions may improve access for a given level of confidentiality or improve confidentiality for a given level of access, but maximal confidentiality and maximal access cannot be attained simultaneously.

Second, we believe that advances in security on the Internet and the Web, which are needed for financial transactions, will be adequate to protect patient information during the transmission process (5). Consequently, we can expect the secure electronic transfer of the information and must concern ourselves primarily with ensuring the appropriateness of the transmission. To this end, we must define the methods by which a health care institution, using the Internet and the Web, can accurately identify a provider and a patient at a setting remote from that institution while the patient is obtaining care in the remote setting.

Third, we recognize that in an emergency, it may not be possible to ask a patient for permission to access his or her distant medical record. In this situation and in the absence of a previous statement by the patient forbidding such access, we believe that information may appropriately be released to emergency providers under the doctrine of implied consent (6). Conversely, if the patient is able to give consent, we require explicit consent for access. Others have suggested using a similar strategy for release of records in emergency settings (7).

Fourth, our experience with electronic patient records has led us to conclude that the most common threat to confidentiality is the inappropriate accessing of information by authorized providers. One way of reducing this threat is to establish severe punishments for providers who violate patient confidentiality. Because many institutions with varying employment practices will be participating in the W3-EMRS project, the institutions will probably need to agree on ways to settle disputes over appropriate punishments for cross-institutional violations of confidentiality. To know who has reviewed patient information using the W3-EMRS server, the technology will keep track of information on all requests for access. Federal sanctions (8) for the inappropriate use of patient information were proposed in the last session of the United States Congress and are likely to be reintroduced in the current session.

Fifth, we recognize that the confidentiality of electronic patient records is of paramount importance to many persons (9–15). Until the confidentiality-related aspects of the W3-EMRS are performing as intended and until the medical, legal, informatics, and civil liberties communities are comfortable with the confidentiality of the system, only "scrubbed" patient data—data from which patient identifiers have been removed and in which aspects of the cases have been changed—will be displayed on the W3-EMRS servers. Thus, the initial implementation of the W3-EMRS will serve as a demonstration and proof of concept. With these principles in mind, we propose the following approach.

Proposal

We define a *reporting institution* as a hospital or other clinical setting from which recorded patient data may be requested. We define a *reporting provider* as a provider at a reporting institution who has recorded information about a patient. A *recipient institution* is a hospital or other clinical setting in which a patient is being seen that desires access to patient information kept at a reporting institution. A *recipient provider* is a provider at a recipient institution who is caring for a patient and desires access to patient information kept at a reporting institution.

Scope

This report is not concerned with methods of providing security for documents transmitted over the Internet or Web. Nor is it concerned with the selection of particular security technologies for authentication or for permanent, secure, and indelible audit trails. Rather, it addresses the functional specifications that any security technology will be required to meet to support the provision of care across health care institutions. Our suggested protocol for the protection of confidentiality addresses a single important scenario—the treatment of a patient in the emergency department—in which patient care would be improved through the interinstitutional transfer of records.

Confidentiality

It is assumed that patients have an ethical and legal right to the confidentiality of their medical record (16). Therefore, it is considered appropriate to allow access to a patient's record only with the patient's consent. In the absence of exceptional circumstances, explicit consent must be obtained. However, in certain serious medical situations, the doctrine of implied consent allows it to be assumed that a patient would provide consent if that patient were competent, even though the patient is incapable of communicating consent. On the other hand, if the patient has explicitly stated in a reporting institution that his or her medical record should not be released over the Web, then the record will not be accessible on the Web even in an emergency.

Participating institutions must provide for the electronic recording of patient refusals to allow emergency release of their records over the Web. Therefore, providers should be encouraged to ask patients to indicate explicitly whether they would allow release of their records for Web transmission. The recording of a patient refusal must electronically prevent the release of records over the Web.

Requirements for Access

Access to the record of a competent patient (17) will be provided if all of the following criteria are met: 1) The patient has not recorded, at the reporting institution, a previous explicit prohibition to the release of records over the Web; 2) the patient consents to access for a specific episode of care at the recipient institution; 3) the identity of the patient is authenticated; and 4) the identities of the recipient institution and provider are authenticated.

A patient will be deemed competent if he or she meets the usual medical and legal criteria for competence and is capable of communicating consent to the reporting institution. A patient who does not meet these criteria will be considered incompetent.

Access to the record of an incompetent patient will be provided if all of the following criteria are met: 1) The patient has not recorded, at the reporting institution, a previous explicit prohibition to the release of records over the Web; 2) the situation is such that a delay in access to the patient's record could result in serious harm to his or her health; 3) the identity of the patient is authenticated; 4) the identities of the recipient institution and provider are authenticated; and 5) the recipient provider has confirmed the need for emergency access to the patient's record.

Authentication

A competent patient will be considered authenticated if the following information is correctly transmitted to the reporting institution: last name and first name, date of birth, sex, mother's first name, and father's first name. An incompetent patient will be considered authenticated if the following information is correctly transmitted to the reporting institution: last name and first name, date of birth, and sex.

A recipient institution and provider will be considered authenticated if the following criteria are met: 1) the request for information originates from an electronic address that the reporting institution knows to belong to a recipient institution, 2) the recipient provider gives his or her name, and 3) a secure password is provided to the reporting institution. This secure password must be known to belong to a specific provider who works in the emergency department at the recipient institution. A secure password must be time-limited and must have been generated by a hardware device in the possession of the emergency department provider.

Consent

A patient will be considered to have consented to transmission of his or her medical record to the recipient provider if the patient or designated proxy answers affirmatively when asked for this consent.

Confirmation of Emergency Need for Access

A recipient provider will be considered to have confirmed the need for emergency access to the record of an incompetent patient when the provider certifies that such access is appropriate. This will require that the provider record indelibly that 1) the patient is not competent to give permission for access and 2) the patient is at risk for serious harm to his or her health if access to the record is delayed.

Maintaining Integrity of the Medical Record

All data sent to the recipient institution will become part of the patient's medical record at that institution. This is necessary to document the basis for decisions that are made in the emergency department. These data will be permanently and clearly labeled as having been obtained from the reporting institution.

Patient's Right To Review Record of Release

For any instance of access to a patient's record by a recipient provider, the reporting institution is responsible for maintaining an indelible record or audit trail of the authenticated providers and institutions to which the record was released. The indelible record includes all data released. This audit trail is available to the patient on demand. In addition, upon any such release, the patient will be sent a notification of the release with instructions on how to obtain the content of the data released.

Breaches of Confidentiality

Institutions participating in the W3-EMRS project will agree on a series of procedures to use to deal with employees who may have inappropriately obtained access to patient information. This may include the development of an interinstitutional committee empowered to sanction inappropriate behavior.

Discussion

Several projects (18–23) other than our own are attempting to use the capabilities of the Internet and the Web to assist in the dissemination of patient information to providers. All of these projects raise serious questions about protection of the confidentiality of patient information made available in this manner. In the course of its work, the Boston Electronic Medical Record Collaborative, which consists of clinicians and developers from four separate institutions, reached a consensus on the above proposal. We hope that other groups will be able to use our proposal as a model and will build on the protections that we have envisioned. We hope, moreover, that as other groups begin to use the Internet and the Web to transmit patient information, the confidentiality of patient information will remain a paramount concern.

Part of our strategy for maintaining confidentiality relies on holding individual clinicians responsible for breaches of confidentiality and punishing such breaches. Individual institutions have used such strategies in the past to improve confidentiality (12) and have increased the level of accountability by informing responsible providers when information has been accessed (13). We have proposed that this strategy be used by insisting on institutional agreements on sanctions and by providing patients with a complete accounting of all information that is transmitted over the Web. Because clinicians who request information are required to have a hardware device that generates a time-limited password, we can be essentially certain about the identity of the clinician so that breaches can be appropriately tracked and punished. An unauthorized user would be unable to pose as an authorized clinician under such a system. Institutions participating in the W3-EMRS project will need to make continued efforts to maintain the confidentiality of patient data. A contemporary review of "best practices" in this area emphasizes the development of an organizational culture that supports privacy and security through a combination of policies, educational efforts, sanctions, and technical mechanisms (24).

In putting forward this proposal, we invite comment from the medical, medical informatics, legal, and civil liberties communities and from the public at large. We believe that until there is general consensus that the structures we intend to use to maintain the security and confidentiality of medical records on the Internet and the Web are adequate, it will not be possible to realize the potential that this exciting new technology has to improve patient care.

We are convinced that improvements in patient care can be expected from the more widespread availability of vital clinical information. We hope that as a medical community and as a society, we can develop methods to implement such technology in a way that leaves most persons feeling that patient rights have been appropriately protected. We welcome the advice and criticism of all those who agree or disagree with this proposal.

Grant Support: In part by a cooperative agreement award from the Agency for Health Care Policy and Research (HS08749) and the National Library of Medicine (U01 LM 05877).

Requests for Reprints: David M. Rind, MD, Center for Clinical Computing, Beth Israel Deaconess Medical Center, 350 Longwood Avenue, Boston, MA 02115.

Current Author Addresses: Drs. Rind and Safran: Center for Clinical Computing, Beth Israel Deaconess Medical Center, 350 Longwood Avenue, Boston, MA 02115.
Dr. Kohane: Children's Hospital Informatics Program, Children's Hospital, 300 Longwood Avenue, Boston, MA 02115.
Dr. Szolovits: Massachusetts Institute of Technology, Laboratory for Computer Science, 545 Technology Square, Room 416, Cambridge, MA 02139.
Drs. Chueh and Barnett: Laboratory of Computer Science, Harvard Medical School, Massachusetts General Hospital, 50 Staniford Street, Boston, MA 02114.

References

1. **Lowe HJ, Lomax EC, Polonkey SE.** The World Wide Web: a review of an emerging internet-based technology for the distribution of biomedical information. J Am Med Inform Assoc. 1996;3:1-14.
2. **Kohane I, Greenspun P, Fackler J, Cimino C, Szolovits P.** W3-EMRS: Building national electronic medical record systems via the World Wide Web. J Am Med Inform Assoc. 1996;3:191-207.
3. **Kohane IS, van Wingerde FJ, Fackler JC, Cimino C, Kilbridge P, Murphy S, et al.** Sharing electronic medical records across multiple heterogeneous and competing institutions. Proc AMIA Annu Fall Symp. 1996:608-12.
4. **van Wingerde FJ, Schindler J, Kilbridge P, Szolovits P, Safran C, Rind D, et al.** Using HL7 and the World Wide Web for unifying patient data from remote databases. Proc AMIA Annu Fall Symp. 1996:643-7.
5. **Garfinkel S, Spafford G.** Practical Unix and Internet Security. 2d ed. Sebastopol, CA: O'Reilly and Associates; 1995.
6. **Sprung CL, Winick BJ.** Informed consent in theory and practice: legal and medical perspectives on the informed consent doctrine and a proposed reconceptualization. Crit Care Med. 1989;17:1346-54.
7. **Donaldson MS, Lohr KN, eds.** Health Data in the Information Age: Use, Disclosure, and Privacy. Washington, DC: National Academy Pr; 1994.
8. Senate Bill 1360: The Medical Records Confidentiality Act of 1995. 104th Congress, 1st Session.
9. **Woodward B.** The computer-based patient record and confidentiality. N Engl J Med. 1995;333:1419-22.
10. **Barrows RC Jr, Clayton PD.** Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc. 1996;3:139-48.
11. **Anderson R.** Clinical system security: interim guidelines. BMJ. 1996;312:109-11.
12. **Safran C, Rind D, Citroen M, Bakker AR, Slack WV, Bleich HL.** Protection of confidentiality in the computer-based patient record. MD Comput. 1995;12:187-92.
13. **Wald JS, Rind D, Safran C.** Protecting confidentiality in an electronic medical record: feedback to the author when someone reads a clinical note [Abstract]. American Medical Informatics Association, Spring Congress. 1994:42.
14. **Slack WV.** The issue of privacy. MD Comput. 1997;14:8-10.
15. **Slack WV.** Private information in the hands of strangers. MD Comput. 1997;14:83-6.
16. **Winslade WJ.** Confidentiality of medical records. An overview of concepts and legal policies. J Leg Med. 1982;3:497-533.
17. **Appelbaum PS, Grisso T.** Assessing patients' capacities to consent to treatment. N Engl J Med. 1988;319:1635-8.
18. **Willard KE, Hallgren JH, Sielaff B, Connelly DP.** The deployment of a World Wide Web (W3) based medical information system. Proc Annu Symp Comput Appl Med Care. 1995:771-5.
19. **Cimino JJ, Socratous SA, Grewal R.** The informatics superhighway: prototyping on the World Wide Web. Proc Annu Symp Comput Appl Med Care. 1995:111-5.
20. **Kohane IS, Greenspun P, Fackler J, Szolovits P.** Accessing pediatric electronic medical record systems via the World Wide Web [Abstract]. Pediatric Research. 1995;37:139A.
21. **McDonald CJ, Overhage JM, Tierney WM, Abernathy G, Dexter P, Smith B, et al.** The Regenstrief medical record system: cross-institutional usage, note writing, and MOSAIC/HTML. Proc Annu Symp Comput Appl Med Care. 1995:1029.
22. **Jagannathan V, Reddy YV, Srinivas K, Karinthi R, Shank R, Reddy S, et al.** An overview of the CERC ARTEMIS Project. Proc Annu Symp Comput Appl Med Care. 1995:12-6.
23. **Kittredge RL, Estey G, Pappas JJ, Barnett GO.** Implementing a Web-based clinical information system using EMR middle layer services. Proc AMIA Annu Fall Symp. 1996:628-32.
24. **Computer Science and Telecommunications Board, National Research Council.** For the Record: Protecting Electronic Health Information. Washington, DC: National Academy Pr; 1997.