Implementing Patient Access to Electronic Health Records Under HIPAA: Lessons Learned

by Tiffany Wang, Lisa Pizziferri, Lynn A. Volk, MHS, Debra A. Mikels, Karen G. Grant, RHIA, CHP, Jonathan S. Wald, MD, MPH, and David W. Bates, MD, MSc

Abstract

In 2001, the Institute of Medicine (IOM) and the Health Insurance Portability and Accountability Act (HIPAA) emphasized the need for patients to have greater control over their health information. We describe a Boston healthcare system's approach to providing patients access to their electronic health records (EHRs) via Patient Gateway, a secure, Web-based portal.

Implemented in 19 clinic sites to date, Patient Gateway allows patients to access information from their medical charts via the Internet in a secure manner.

Since 2002, over 19,000 patients have enrolled in Patient Gateway, more than 125,000 patients have logged into the system, and over 37,000 messages have been sent by patients to their practices. There have been no major security concerns.

By providing access to EHR data, secure systems like Patient Gateway allow patients a greater role in their healthcare process, as envisioned by the IOM and HIPAA.

Introduction

In the 2001 report *Crossing the Quality Chasm*, the Institute of Medicine (IOM) called for a new approach to the delivery of healthcare in America.[1] This report pointed out that despite remarkable advances in the fields of computer and medical sciences, the quality of healthcare leaves much to be desired. To close this "chasm" between the current and optimal states of healthcare delivery, IOM proposed 10 guidelines for developing an improved healthcare system.[2] One significant recommendation

entailed improving patients' access to their personal medical information and to clinical knowledge—an increase in patient control that could be achieved through the use of IT.[3]

Also in 2001, the 1996 Health Insurance Portability and Accountability Act (HIPAA) privacy rule went into effect. This rule created a minimum level of federal protections for the privacy of health information, while preserving more stringent state confidentiality laws.[4] The privacy rule applies to medical records, billing records, and other individually identifiable health information—whether in electronic, paper, or verbal form—that is used or disclosed by any covered entity.[5] This rule emphasizes the right for patients to have greater control over their medical records.[6]

In light of these nationally significant calls for secure patient access to medical information, the development and use of electronic health records (EHRs) has become increasingly relevant. EHRs provide an alternative to more traditional, paper-based systems for documenting and maintaining health information and can allow patients better access to their medical records. EHRs have many benefits, as they can improve the efficiency, safety, and quality of care.[7] Experience with EHRs has shown that the confidentiality of personal health information can be maintained with properly designed security systems.[8] However, making the information in EHRs available to patients poses difficulties to healthcare organizations and practices around the country and to providers concerned about HIPAA regulations, which include fines for breaches.[9,10]

In 2001, Partners HealthCare System, an integrated healthcare network of hospitals and medical practices based in Boston, began developing Patient Gateway, a secure Web-based portal that provides Partners patients with access to portions of their EHRs. The present article examines this approach to providing patients with access to EHR data and discusses the ways in which Patient Gateway has achieved and even facilitated compliance with HIPAA rules. As the use of Patient Gateway expands to more clinics and a broader group of patients and allows access to greater portions of medical records, new privacy and confidentiality issues of implementing patient access to EHRs will also need to be addressed.

Methods

Partners HealthCare operates and maintains an extensive clinical information system with a fully electronic ambulatory health record that is used by providers and staff in day-to-day care of patients. This EHR, called the longitudinal medical record (LMR), was internally developed in 2000. Launched in February 2002, Patient Gateway is an internally developed, Web-based portal, which allows enrolled patients to view limited information copied from the LMR; it was implemented in 19 different Partners clinic sites within its first two years. These clinics are located in both urban and suburban areas, encompassing low, middle, or high socioeconomic statuses or a mix of all three.

Patient Gateway offers patients using a secure login a number of online services: patients can send and receive electronic messages to their doctors' offices; complete request forms for prescriptions (Figure 1), appointments, and referral authorizations; view limited ambulatory medical chart information (a list of current medications and allergies); and access a health library and practice information (Figure 2). The Patient Gateway application, isolated on a separate server behind the Partners firewall, receives requests from patients and processes them. The system has limited capability to retrieve ambulatory medical record information (medication and allergy information only) and uses the login credentials of the Patient Gateway user to determine which patient record data to retrieve.

In developing the Patient Gateway system, members of the health information management (HIM) department were consulted to assess current policies and procedures and any changes that were needed. Two major areas, electronic communication and release of record information, were reviewed.

To provide EHR access while maintaining security and privacy, Patient Gateway employs policies and technical procedures that can be categorized in the following domains: authenticating and authorizing patient use, authenticating and authorizing staff use, and secure messaging.

Authenticating and Authorizing Patient Use

Utilizing usernames and passwords, Patient Gateway authenticates its patients, verifying that users are who they purport to be.[11] Patient Gateway also authorizes its patients, designating the specific functions and information to which authenticated users can gain access.[12] Patient Gateway utilizes a standard authentication process to verify the identities of users before they can gain access to any personally identifiable health information. Before individuals are granted a Patient Gateway account, their status as a patient in the clinic is verified.[13] To enroll, patients must provide information regarding demographics, their physicians, and their physicians' practices. They also must electronically acknowledge having read and agreed to the Patient Gateway terms of use and privacy policy. The information supplied at enrollment is then compared to the Partners patient registration database, which uniquely identifies each patient. When necessary, the Patient Gateway support staff contacts patients to resolve any discrepancies in this information. After approval, patients receive unique passwords and usernames through separate modes of communication—passwords are sent to the patient's registration address via postal mail, whereas usernames are sent using the e-mail address supplied during enrollment. Patients must then change the initial password to complete the process of activating their account. Guidelines to create strong passwords are provided by the Patient Gateway privacy policy.[14]

User logon and logoff methods are made simple to encourage the use of Patient Gateway for online messaging rather than non-secure alternatives such as typical e-mail. Additionally, after 30 minutes, Patient Gateway automatically logs off a user to protect against use by unauthenticated individuals. Along with the enrollment process, patient education is provided to underscore the need for and methods of protecting access to the system. Instructions about not sharing passwords emphasize patients' responsibility for maintaining the confidentiality of their health information.[15] Patients can change their passwords online at any time and are particularly encouraged to do so if they suspect others may have obtained them.[16]

Authenticating and Authorizing Staff Use

Because the HIPAA privacy rule states that an individual's health information may be used for treatment, payment, and/or healthcare operations without specific authorization,[17] Patient Gateway educates its users about who may potentially view patient messages.[18] The Patient Gateway privacy policy provides detail on who within Partners may actually view the messages: "Others besides the addressee may process messages during the addressee's usual business hours, after hours, during addressee's vacation or illness, etc. . . Messages and information sent to the practice may be shared with those who provide care or assist in care management as needed."[19] In addition to this patient education,

Patient Gateway uses technical safeguards to ensure patients that only appropriate personnel will view their personal health information.

For authentication purposes, all employees of Partners are assigned usernames and passwords, which are required to access any Partners computer. Usernames and passwords are also required for the staff to access Patient Gateway itself to review selected health information and messages from patients. After initial authentication, Patient Gateway ensures that the current staff user is still the authenticated user through methods similar to those used for patients.

In addition to authentication, employees must be authorized to access Patient Gateway. Clinicians and practice staff who are authorized sign agreements to access only the minimum electronic information necessary for their specific roles. The Patient Gateway application currently consists of several different mailboxes (or "desks"): general messages, appointments, referrals, and medications. Patients direct their messages to clinicians and practice staff, who are given access only to those Patient Gateway mailboxes for which they are responsible.

Messaging

To protect the confidentiality of electronic communication between patients and clinicians, Patient Gateway provides technical safeguards that may be absent in typical e-mail systems. The system can only be used by patients with Web browsers that support high encryption, as all communication between the patient's computer and the Partners computer is encrypted over a secure sockets layer (SSL) connection. Memory cache on the patient's computer is automatically turned off to avoid storage of data in memory on the client machine, which might belong to someone other than the patient (for example, a public computer or work computer).

Results

Patient Gateway was developed to be consistent with HIPAA requirements, putting in place mechanisms to help prevent the unauthorized disclosure of or inappropriate access to health information and maximize the security of health information transmitted via the Internet. HIM policies for electronic communication—which urge that care be taken to prevent misrouting of messages, to prevent inappropriate handling of clinically urgent messages, and to ensure security and confidentiality protections (technical and procedural)—were met or exceeded in the design of the new system. The new system was also found to be compliant with release of information policies, as Patient Gateway is offered to patients in a preexisting physician/patient relationship and laws in the state of Massachusetts ensure patient access to their medical chart information. As of November 2004, more than 19,000 patients had enrolled in Patient Gateway, more than 125,000 patient sessions had been logged into the system, and more than 37,000 messages had been sent by patients to their physicians' practices.

Authenticating and Authorizing Patient Use

The processes of authentication and authorization help to ensure that personal health information is protected and that patients may see only their own personal health information. In several cases, patients voiced their concerns about the confidentiality of the system to the Patient Gateway research staff. Almost

all of these patients had basic questions about the system's security, regarding the confidentiality of their social security numbers, health information, or Patient Gateway passwords, but seemed to be satisfied with clarifications provided by the Patient Gateway research staff. However, in one instance, a patient believed that he was able to view personal health information belonging to another patient. In fact, this patient was seeing the data of a test patient, a fictitious patient used in the enrollment demonstration to inform real patients about the capabilities of Patient Gateway. While this patient's concerns received a thorough response by Patient Gateway staff, his level of confidence in the security of the computer system may have already been affected.

Since the initial implementation of Patient Gateway, changes have been necessary in the area of password recovery. When Patient Gateway users forget their passwords, which are required to access the system, they can submit a request for a replacement temporary password. In the initial months of Patient Gateway, requests for replacement passwords fulfilled via postal mail to the address on file with the healthcare system's registration (just like distribution of the initial password). However, this resulted in a substantial delay for the patient and led to dissatisfaction. An improved approach was designed in which a secondary "shared secret" was stored by the patient when first activating the account. The patient is asked to answer a personally customized, secret question (for example, "What was the make of your first car?"), a technique also used in many other industries as part of the authentication process. If the secret question is answered correctly, the system creates a temporary password and sends it immediately to the e-mail address on file for the patient. Furthermore, an additional "challenge question" is asked when this temporary password is used based on information on file in the system. In addition to reducing the amount of time Patient Gateway staff spends on mailing individual password reminders, this system has assisted greatly in accommodating patient convenience concerns, without compromising the confidentiality of personal health information.

While Patient Gateway has strong measures to control patient access to medical information, it does not yet address healthcare proxies and friends or family members who may serve as caregivers. Although these individuals may often be key participants in a patient's care, they currently cannot access another individual's data using Patient Gateway, even with the individual's permission. While it is planned to change this, Patient Gateway currently is designed for use only by adult patients and selected Partners staff.

Authenticating and Authorizing Staff Use

Patient Gateway ensures that only the appropriate staff members may access protected patient information online. To date, there have been no patient complaints of staff inappropriately accessing Patient Gateway. However, some patients have questioned why the Patient Gateway triage staff and not their physicians are the first to read their e-mails. The triage staff can respond to these e-mails or forward them to patients' respective physicians when necessary. In response to these inquiries, the Patient Gateway research staff clarifies that messages may be processed by individuals others than the addressee. This process is also used with other messages (such as phone messages) left for the practice and as stated in the Patient Gateway privacy policy. [20]

Messaging

The HIPAA privacy rule requires that patients be allowed to see and obtain copies of their medical records. Through its secure messaging system, Patient Gateway allows patients to inquire about and

respond to selected contents of their medical records in a convenient and accessible way. While the privacy of the messages sent through Patient Gateway can be regulated, Patient Gateway currently contains no mechanisms to limit the content of messages to only questions and comments appropriate for electronic communication.

Of the more than 19,000 Patient Gateway accounts, only two have been closed because of message content. Both cases involved patients who sent inappropriate or urgent messages to their practices, despite clear instructions about the appropriate use of e-mail. In both cases, the patient had used other forms of communication inappropriately in the past, such as the telephone. The accounts were closed at the discretion of the practices.

Discussion

The 2001 IOM report *Crossing the Quality Chasm* emphasized the importance of patients having access to their medical information.[21] It called for the use of IT to increase patient knowledge and open patient-physician communication. That same year, federal HIPAA regulations mandated the need for patient access to medical records.[22] In response to this changing environment, Partners HealthCare developed Patient Gateway to provide a secure and convenient way for patients to view their medical records and communicate with their physicians.

Patient Gateway utilizes the security protections and messaging features that are unique to electronic data and communication. Medical information documented and transmitted over secure electronic systems like Patient Gateway can be kept confidential using technology not offered by paper-based systems. The technological capabilities provided by Patient Gateway have fostered compliance with the HIPAA privacy rule by facilitating the sharing of clinical data between patients and clinicians. However, enabling patients to gain access to medical information via the Internet still presents various challenges of privacy and confidentiality. As discussed below, Patient Gateway has revealed important issues that must be considered in further implementation of patient access to EHRs.

Authenticating and Authorizing Patient Use

In the future, Patient Gateway developers will be determining how to best address extended use of this tool by other active participants in a patient's care, with patient knowledge and permission as needed. Additional programming for incorporating different levels of authenticating and authorizing proxies will need to be implemented, as will a method for allowing access to subsets of health information according to patients' wishes. Future development will also address the use of Patient Gateway by parents for their children and by mature or emancipated minors.

Authenticating and Authorizing Staff Use

Patient Gateway educates its users about staff access to the content of their e-mails. However, patients' understanding of the privacy policy and expectations around communications need to be further considered. While patients are informed that staff members other than their physicians may view their messages, it must be clearly conveyed to patients that these less familiar individuals may also be the ones composing responses to messages.

Messaging

While Patient Gateway provides a messaging system that is much more secure than a standard e-mail system, how to best manage and store messages exchanged between patients and clinicians will need to be considered. Patient Gateway's privacy policy clearly advises patients that "Any electronic message you send or receive using Patient Gateway may be placed in your medical record."[23] However, Patient Gateway's current policy defers to providers' judgment as to whether an e-mail is included in patients' medical records. The potential benefits of standardizing the way in which messages are selected for documentation need to be considered. Also, a system to manage those messages not placed into medical records must be developed, deciding whether they are to be stored in a repository, archived in Patient Gateway, or deleted.

Future development of Patient Gateway will also need to consider the way EHRs are presented. Rather than allowing patients to view their complete medical records in original form, Patient Gateway currently presents selected information in a patient-friendly manner to make data more understandable to patients. A continued consideration will be which portions of their medical information patients will be able to access through Patient Gateway, and in what format. Although medical records clearly belong to the patients,[24] physicians are reluctant to allow patients to view their test results and notes, largely out of concern that patients may misinterpret or not understand the information.

Another key tension is that of providing security versus allowing access. The current password-giving approach has been highly secure, but could inadvertently block some users of Patient Gateway who have lost track of their login information. In addition, some patients choose to use standard e-mail instead of Patient Gateway to communicate sensitive health information, suggesting that at least some patients are not especially concerned or knowledgeable about security risks. Overall, implementation of Patient Gateway under HIPAA proved less onerous than many expected. The level of security has been outstanding to date; nevertheless, strong security may limit access, as noted above.

Limitations of Evaluation

Evaluation of Patient Gateway has produced valuable insight into an important way patient access to medical information may be integrated into healthcare delivery. However, a limitation is that it was done in a single integrated delivery system, which may differ from others. In addition, the evaluation was based on observations made during the first two years of implementation, and longer term issues may be different from those encountered to date, especially as more functionality is added.

Conclusion

The authors have been able to use the Patient Gateway tool to approach the vision of IOM. Compliance with the new HIPAA privacy rule in doing this was less difficult in many ways than had been expected. Secure systems like this can facilitate the flow of clinical information between patients and their physicians and allow patients to play a greater role in the healthcare process. Patient access to medical information can be secure and beneficial with the appropriate controls. Early and continuing consultation with HIM leadership at Partners has been a critical success factor in the design and rollout of Patient Gateway. However, significant challenges to the implementation of patient access to EHR data remain.

Being able to address these issues is critical for the continued success and expansion of patient access to EHRs.

Tiffany Wang is a research assistant at Partners HealthCare in Needham, MA. Lisa Pizziferri is a senior research associate at Partners HealthCare. Lynn A. Volk, MHS, is an associate director at Partners HealthCare. Debra A. Mikels is a corporate confidentiality manager at Partners HealthCare in Wellesley, MA. Karen G. Grant, RHIA, CHP, is a corporate director and Chief Privacy Officer at Partners HealthCare in Wellesley, MA. Jonathan S. Wald, MD, MPH, is an associate director at Partners HealthCare. David W. Bates, MD, MSc, is a director of Partners HealthCare in Needham, MA.

Acknowledgements

We would like to acknowledge Elena Cotto, Joseph L. Ferrari, Phyllis Kaplan, and Elizabeth Nelson of the Partners Patient Gateway Team for their contributions.

AHIMA does not support or endorse the products or services referenced in this manuscript.

Notes

1. Institute of Medicine. *Crossing the Quality Chasm: A New Health System for the 21st Century.* Washington, D.C.: National Academy Press, 2001.

2. Ibid.

3. Ibid.

4. Gunn, Patrick P., Allen M. Fremont, Melissa Bottrell, Lisa R. Shugarman, Jolene Galegher, and Tora Bikson. “The Health Insurance Portability and Accountability Act Privacy Rule: A Practical Guide for Researchers.” *Medical Care* 42, no. 4 (2004): 321–27.

5. U.S. Department of Health and Human Services. “Medical Privacy—National Standards to Protect the Privacy of Personal Health Information.” Available at www.hhs.gov/ocr/hipaa/finalreg.html.

6. Gunn, Patrick P., Allen M. Fremont, Melissa Bottrell, Lisa R. Shugarman, Jolene Galegher, and Tora Bikson. “The Health Insurance Portability and Accountability Act Privacy Rule.”

7. Bates, David. W., Mark Ebell, Edward Gotlieb, John Zapp, and H.C. Mullins. “A Proposal for Electronic Medical Records in U.S. Primary Care.” *Journal of the American Medical Informatics Association* 10, no. 1 (2003): 1–10.

8. HIMSS. “HIMSS CPRI Toolkit: Managing Information Security in Healthcare.” Available at www.himss.org/asp/cpritoolkit_toolkit.asp.

9. Bates, David. W., Mark Ebell, Edward Gotlieb, John Zapp, and H.C. Mullins. “A Proposal for Electronic Medical Records in U.S. Primary Care.”

10. U.S. Department of Health and Human Services. “Medical Privacy.”

11. HIMSS. “HIMSS CPRI Toolkit.”

12. Ibid.

13. Partners HealthCare Information Systems. “Patient Gateway Privacy/Terms of Use: Background Info.” Available at www.patientgateway.org/ptgw/logBWH.htm.

14. Partners HealthCare Information Systems. “Patient Gateway Privacy/Terms of Use: Privacy Policy.” Available online at www.patientgateway.org/ptgw/logBWH.htm.

15. Partners HealthCare Information Systems. “Patient Gateway Privacy/Terms of Use: Background Info.”

16. Partners HealthCare Information Systems. “Patient Gateway Privacy/Terms of Use: Privacy Policy.”

17. U.S. Department of Health and Human Services. “Medical Privacy.”

18. Partners HealthCare Information Systems. “Patient Gateway Privacy/Terms of Use: Privacy Policy.”

19. Ibid.

20. Ibid.

21. Institute of Medicine. *Crossing the Quality Chasm.*

22. U.S. Department of Health and Human Services. “Medical Privacy.”

23. Partners HealthCare Information Systems. “Patient Gateway Privacy/Terms of Use: Privacy Policy.”

24. U.S. Department of Health and Human Services. “Medical Privacy.”

Figure 1: Prescription Request Form of the Patient Gateway portal. After clicking "Renew" of a specific medication, the patient performs four steps to complete a prescription request: (1) confirm the medication details such as the number of refills and dose; (2) specify if the prescription should be held at the clinic for pick up, mailed to the patient, or sent to the pharmacy; (3) enter a phone number of where he or she can be reached for questions about the request; and (4) review information entered in prior steps and submit request.

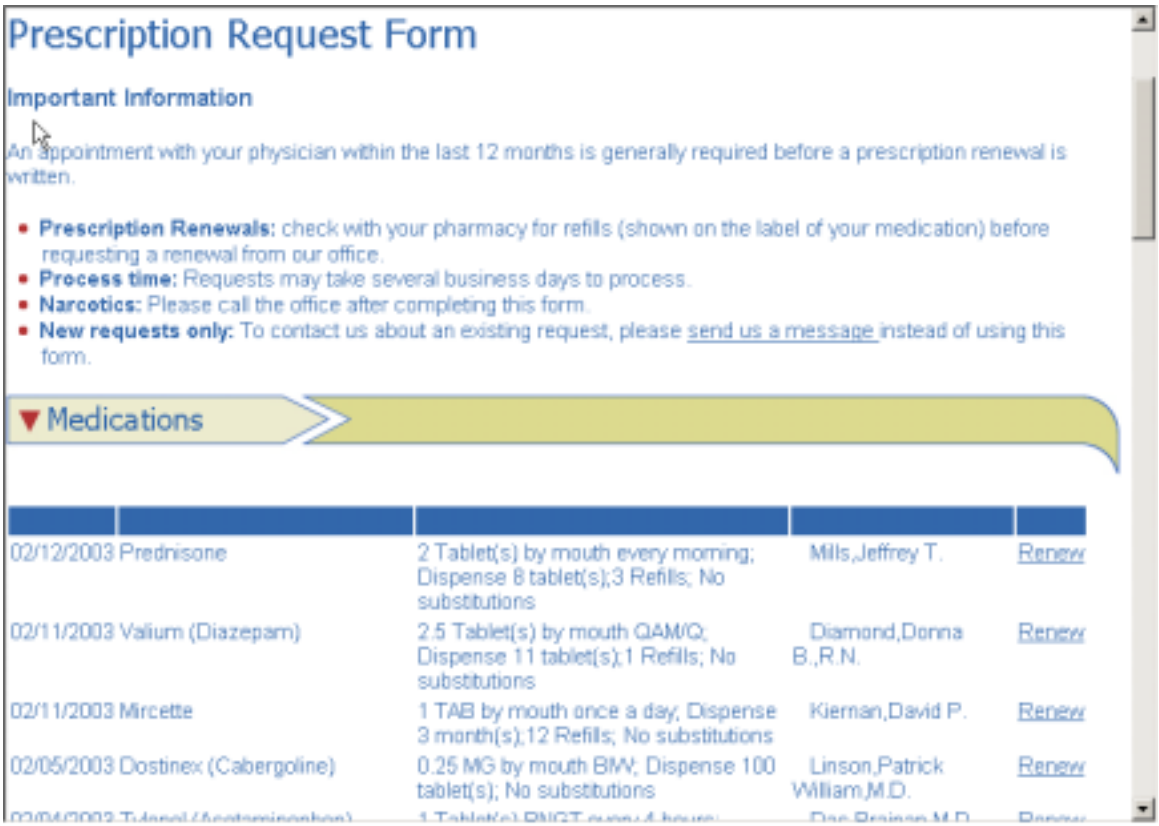

Figure 2: Opening screen of the Patient Gateway portal after a patient logs in using their username and password. Patients use the main menu to select tasks such as sending messages and requests, viewing health record information, and accessing the health library and practice information.