HealthConnect: Clinical Grade Patient-Physician Communication

Kenneth D. Mandl, M.D., M.P.H, Isaac S. Kohane, M.D., Ph.D.
Informatics Program and Divisions of Emergency Medicine and Endocrinology
Children's Hospital, Harvard Medical School, Boston, MA

ABSTRACT

A critical mass of Internet users is leading to a wide diffusion of electronic communications within medical practice. Unless implemented with substantial forethought, these new technological linkages could disturb delicate balances in the doctor-patient relationship, threaten the privacy of medical information, widen social disparity in health outcomes, and even function as barriers to access.

The American Medical Informatics Association (AMIA) recently published recommendations to guide computer-based communications between clinicians and patients.

This paper describes the motivations for and the design of HealthConnect, a web-based patient-doctor communications tool currently in use at Children's Hospital, Boston. Structural and process-oriented features of HealthConnect, as they relate to promotion of adherence with the Guidelines, *are discussed.*

INTRODUCTION

Patients and physicians increasingly choose electronic forms of asynchronous interchange to communicate. As the percentage of American homes with computers passes the 50% mark, doctors and their patients are exploring the use of electronic mail in the medical context.[1] While electronic correspondence can connect doctors with patients,[2] thereby increasing access to care and enhancing patient education, there are potential pitfalls of using standard electronic mail systems for medical communication. The 1998 *AMIA Guidelines for the Clinical Use of Electronic Mail with Patients*[3] provide an approach to effective and medicolegally sound practice. We present here, a description of HealthConnect, a web-based messaging tool designed to foster safe, reliable, and effective communication, like that advocated by the AMIA guidelines.

MOTIVATIONS

Access. Inequitable distribution of new technologies may widen social disparity. An effective therapy with differential access according to socioeconomic characteristics or ethnic group may cause a divergence in health status outcomes among segments of the population. Thus when consumer informatics tools are offered to a population, particular attention should be paid to the demographics of access. More than half of the patients in our population have ongoing access to the Web or e-mail. There is a direct correlation between income and being "on-line." More patients can access the Web than have personal or professional e-mail addresses. About one third have on-line resources only at home, one third only outside the home, and one third both in the home and elsewhere.[4] In order to maximize access by a mobile population of web users and potential web users, we therefore needed a lightweight Web-based tool that required no specialized software aside from a standard Web browser. HealthConnect had to be available at any time from any Internet connected device. It could not require a pre-configured machine or a lengthy download at startup. This approach would allow a sizeable group of patients who do not own computers to use HealthConnect.

Privacy and Security. Currently, standard e-mail systems do not usually use strong authentication methods. The identity of the doctor or the patient is vulnerable to falsification. Many standard e-mail systems use store and forward protocols that leave copies of messages on various insecure servers and end-user hard drives. Patients or physicians who use e-mail for medical interchange in the workplace are not assured confidentiality and may unintentionally expose sensitive details of illness or social circumstances to an employer. Further, patients using family e-mail accounts at home may lack privacy from spouses, children, or parents.

Electronic access to a physician or patient for confidential exchange requires means for authentication of users. An institutional approach to communicating medical information could not involve transmission of unencrypted messages with patient-identifiable data to across the Internet.[5,6] Nor may a health care institution jeopardize patient's confidentiality and privacy by engaging them in a form of communication that leaves their medical data stored on insecure mail servers and personal computers.

Reliability. The formalization of electronic communication requires a 'clinical grade' of system dependability. Reliance on the multiplicity of e-mail

1091—8280/99/$5.00

systems in use by various doctors and patients precludes any centralized approach to quality assurance and back up. Even under normal conditions, the delivery of e-mail may be substantially delayed. Inconsistent use of read-receipts leaves both parties unsure as to whether message exchange was successful.

Any health communications tool would need to be sufficiently robust to provide the kind of transactional integrity associated with consumer financial applications such as electronic debit cards. In addition to assuring system-wide transactional integrity, the reliability of *usage* would be enhanced by requiring that a health care communication application manage message receipts and notification of all parties upon arrival and reading of new messages.

Transparency. Currently when patients and doctors use electronic media to communicate, they may or may not have mutually agreed on the nature of the 'contract' or understand well each other's expectations. Further, patients may not clearly understand where messages are going, and who (front desk staff, practice nurse, third party payor) will have access to them. A system such as HealthConnect would need to provide transparency about the flow of information and messaging.

Documentation. Documentation of care in the medical record is critical to provision of effective treatment and is medico-legally imperative. Electronic mail with patient identifiable data sent provider-to-provider [7, 8] or provider to patient rarely becomes available in the patient's medical record. Rather, pieces of the interchange may exist on the hard drives of several geographically diverse personal computers or servers. As a medical communications application, HealthConnect was designed to document activity in the patient's medical record.

Patient Education and Instruction. Each patient encounter with the health care system provides an opportunity to further that patient's education and in doing so empower them in their own care.[2] Health care web sites can provide a lot of useful information, particularly when they are disease-specific.[9] However, following an encounter with the health care system there is an opportunity to provide particularly customized education information, in the form of "outbound" messaging, to that patient. HealthConnect was designed to take advantage of this educational opportunity.

DESIGN

Overview. HealthConnect is Web-based messaging software that 1) allows physicians to prescribe individualized plans of care for patients that become available on the World Wide Web; and 2) enables secure web-form exchange between physicians and patients. The initial commercial implementation of HealthConnect* is in the Children's Hospital, Boston Emergency Department where it has been in use since December of 1998. A multi-clinic version of HealthConnect is currently being implemented.

Two computers serve HealthConnect, one inside and one outside the hospital firewall. Web forms are used for messaging rather than standard e-mail protocols. That is, although to the users, the messages appear within a user interface very much like e-mail, all communications occur by transactions with the HealthConnect database. HealthConnect provides access through several user-specific views which are described here.

Registration Secretary View. When the patient registers in the Emergency Department, secretaries enter twice (for error checking) patient home or work

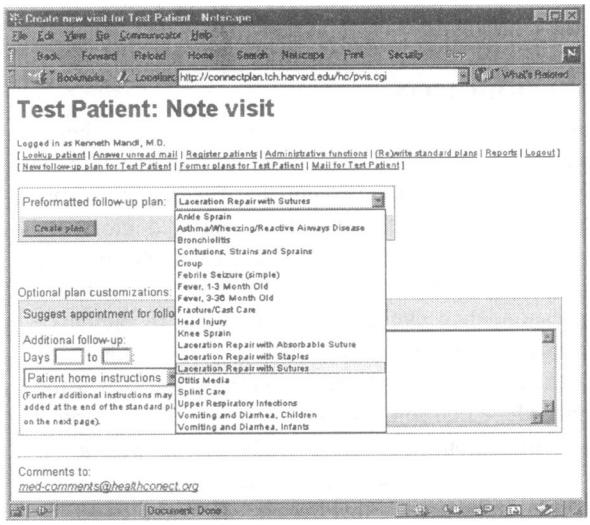

Figure 1. Treating Doctor Plan Selection Dialogue

e-mail addresses.

Treating Doctor View. At the end of an Emergency Department visit, the doctor opens the provider-side of HealthConnect from a bookmark in a Netscape browser window, and chooses a standard plan from a drop down menu (Figure 1). Username and password are required for authentication. A standard

* Developed with W3Health, Boston, MA (www.W3Health.com)

plan for the designated diagnosis is generated. The plan is broken down into fragments, each of which has a date range specifying when it will appear on the patient's view of the plan.

A drug-prescribing dialogue box can be opened. Choosing a standard drug and regimen results in printing a legal paper prescription as well as adding lay English directions to the plan.

Templates allow follow-up appointments or other patient instructions to be added to the plan. Any of the standard plan text is editable. When the plan is complete, the physician finalizes it causing 1) printing of a hard copy of the plan, to be given to the patient; 2) publishing, on the Web, of a secure document for the patient to view for ten days after the Emergency Department visit. The hard copy of the plan contains a URL (www.HealthConnect.org), as well as a unique username and password.

Patient View. In order to access HealthConnect, the patient need only have access to a Web browser. If the patient has supplied the registration secretary with an e-mail address, he will receive an every other day reminder to check www.HealthConnect.org. This reminder is a standard, insecure e-mail and contains no medical information. The e-mail is sent from and is from the address, user-support@healthconnect.org. The patient either uses the hyperlink to open HealthConnect, or types the URL in his browser location window.

Upon login, the patient receives 1) guidelines for *appropriate* use of HealthConnect for non-emergent situations only and 2) a disclaimer concerning security and privacy issues.

The patient logs in with the username and password which are printed on the hardcopy of his HealthConnect discharge instructions. Logging in brings him to a view of that day's plan (Figure 3). There are 5 navigation buttons for 1) exchanging messages with the physician; 2) viewing the follow-up plan overview from any current or previous visit; 3) obtaining help; or 4) logging out.

When the patient sends a message to the physician, a Web form reminds him 1) to check HealthConnect, and not his standard e-mail account for a response; and 2) to not expect a response for up to twenty-four hours.

When the physician has proactively sent the patient a message, or responded to a message, a standard e-mail is generated and sent to the patient's own e-mail address as a notification. The physician response is available on a securely communicated Web form on the patient's HealthConnect page.

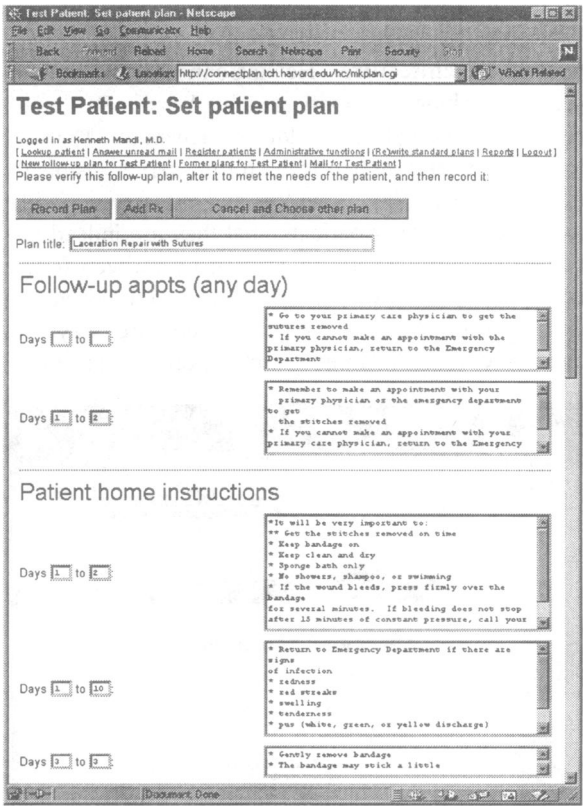

Figure 2. Treating Doctor Plan Edit View

Physician Message Response View. The system provides centralized patient messaging. All patient mail is sent to a single generic physician responder. That responder is given a view of all incoming messages, linked to the patient plans prescribed the treating doctor. Response can be initiated with a *reply* button (patient message text will be quoted in the response) or a *send new mail* button.

System Administrator View. The system administrator can authorize new users, assigning appropriate privileges. The administrator can also view detailed reports of patient registration, plan prescribing, patient sessions, and all messaging.

Authoring View. There is an authoring mode for generating standard plans. These plans are created as fragments including an introduction and a series of specific instructions, each of which has a date range indicating when they will appear on the Patient's view. Plans can be maintained as draft plans and ultimately published so that they are available to the treating doctor from the drop down list.

Documentation. All messages and plans are stored in the hospital Oracle database and accessible to users through a standard interface.

System Architecture. HealthConnect runs off of secure machines authenticated by Versign™ digital certificates issued to Children's Hospital. That is, these certificates authenticate, for the server visible to the plan-prescribing providers and the server visible to the plan-viewing patients, that they are indeed the correct servers. There no caching of the web forms on the patient browsers, so no data is left behind on the local machine. Of course, there are ways to overcome a no-caching directive on the browsers

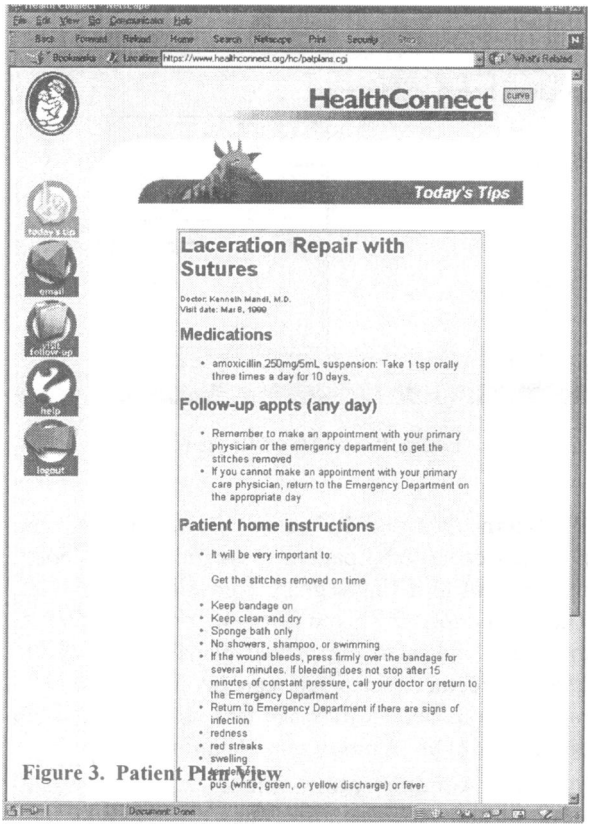

Figure 3. Patient Plan View

(e.g. the patient can explicitly save the page) but our design goal is to avoid loss of privacy by insufficient vigilance by the patient (e.g. at the workplace) rather than preventing the patient from storing the data. All communication is end-to-end encrypted through use of the Secure Socket Layer (SSL) protocol.

The application logic on the provider's server was implemented as Perl scripts running on a Linux server. The application logic on the server visible to the patient was also implemented as Perl Scripts running on a Linux server. The patient-specific plans are stored in a relational database. The plans are forwarded from the provider's server to the patient's server via SSL protocol. All databases are mirrored and backed up daily.

GUIDELINE ADHERENCE

The AMIA Guidelines for the *Clinical Use of Electronic Mail with Patients* are divided into those concerning communication, medicolegal and administrative considerations. Here we present architectural and process-oriented features of HealthConnect as they relate to promotion of adherence with the *Guidelines*.

Establish turnaround time for messages. Do not use e-mail for urgent matters. The printed discharge instructions and user interface and explicitly set customizable expectations for patients about message turn around time. The log-in screen and mail composer display instructions for appropriate use of electronic mail as well as the appropriate actions to take in urgent and emergent situations.

Inform patients about privacy issues. Patients should know who besides addressee processes messages. The current version of HealthConnect uses a centralized response model. All messages go to the generic "Emergency Physician." In a multi-clinic model of HealthConnect currently in the implementation phase, there is a list of recipients that the patient can choose from. Additional rules about night, weekend, vacation 'coverage' of e-mail response can be easily displayed on a Web page.

Establish types of transactions (prescription refill, appointment scheduling, etc.) and sensitivity of subject matter (HIV, mental health, etc) permitted over e-mail. In the current version of HealthConnect most of the plans deal with medical subject matter of relatively low sensitivity (lacerations, fractures, upper respiratory infections, etc). Concerns about privacy of information are diminished when password authentication and SSL encryption are used. We therefore give patients no explicit instructions regarding sensitivity of subject matter permitted. Data are being collected on uses of HealthConnect.

Instruct patients to put category of transaction in subject line of message for filtering. In the multi-clinic version of HealthConnect currently being implemented, there is a drop-down menu to choose transaction type.

Request that patients put their name and patient identification number in the body of the message. Identification of the patient is accomplished through the unique username and password.

Configure automatic reply to acknowledge receipt of messages. Patients are instantly notified about receipt of messages.

Print all messages with replies and confirmation of receipt, and place in patient's paper chart.

Messages are logged in the Hospital Oracle database and become available as a part of the patient's electronic medical record.

Request that patients use autoreply feature to acknowledge reading provider's message. Doctors are instantly notified about receipt of messages.

Maintain a mailing list of patients, but do not send group mailings where recipients are visible to each other. Use blind copy feature in software. In the multi-clinic version of HealthConnect, reminders and educational materials can be sent to multiple recipients who cannot view the identity of other recipients of the message.

Send a new message to inform patient of completion of request. It would be advisable for the physician responding to patient messages to adhere to this guideline.

Avoid anger, sarcasm, harsh criticism, and libelous references to third parties in messages. It would be advisable for the physician responding to patient messages to adhere to this guideline.

Consider obtaining patient's informed consent for use of e-mail. A use agreement appears on the login page.

Use password-protected screen savers for all desktop workstations in the office, hospital, and at home. HealthConnect times out after 10 minutes, requiring another password login to continue.

Never forward patient-identifiable information to a third party without the patient's express permission. HealthConnect only allows communication with within a designated health system.

Do not share professional e-mail accounts with family members. As a secure application with authenticated login, physician's family members do not have access to HealthConnect.

Use encryption for all messages when encryption technology becomes widely available, user-friendly, and practical. HealthConnect automatically uses SSL encryption for all messaging. The user need not be aware of encryption methods.

Do not use unencrypted wireless communication with patient-identifiable information. SSL encryption is employed for all wireless TCP/IP communication links.

Double-check all "To:" fields prior to sending messages. It would be advisable for the physician responding to patient messages to adhere to this guideline.

Perform at least weekly backups of mail onto long-term storage. Define "long-term" as the term applicable to paper records. HealthConnect performs daily backups.

Commit policy decisions to writing and electronic form. Printed discharge instructions specific to the patient's condition and including disclaimer are given to the patient prior to discharge.

SUMMARY

HealthConnect is a Web-based communications tool designed to promote appropriate, secure communication between doctors and patients. Adherence to the *AMIA Guidelines for the Clinical Use of Electronic Mail with Patients* can effectively be promoted through appropriate software design coupled with careful use of electronic communication.

References

1. Mandl KD, Kohane IS, Brandt AM. Electronic patient-physician communication: problems and promise. *Ann Intern Med.* 1998;129:495-500.

2. Szolovits P, Doyle J, Long WJ, Kohane I, Pauker SG. Guardian Angel: Patient-Centered Health Information Systems. . Report TR-604. Cambridge: MIT Laboratory for Computer Science; 1994.

3. Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. The AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic-Patient Electronic Mail. *J Am Med Inform Assoc.* 1998;5:104-11.

4. Mandl KD, Katz SB, Kohane IS. Social equity and access to the World Wide Web and e-mail: implications for design and implementation of medical applications. *Proc AMIA Annu Fall Symp.* 1998:215-219.

5. Halamka JD, Szolovits P, Rind D, Safran C. A WWW implementation of national recommendations for protecting electronic health information. *J Am Med Inform Assoc.* 1997;4:458-64.

6. Rind DM, Kohane IS, Szolovits P, Safran C, Chueh HC, Barnett GO. Maintaining the confidentiality of medical records shared over the Internet and the World Wide Web. *Ann Intern Med.* 1997;127:138-41.

7. Borowitz SM, Wyatt JC. The origin, content, and workload of e-mail consultations [see comments]. *Jama.* 1998;280:1321-4.

8. Sands DZ, Safran C, Slack WV, Bleich HL. Use of electronic mail in a teaching hospital. *Proc Annu Symp Comput Appl Med Care.* 1993:306-10.

9. Kassirer JP. The next transformation in the delivery of health care [editorial]. *N Engl J Med.* 1995;332:52-4.