Next Generation: How Internet Technology Propels the Electronic Medical Record

Save to myBoK

by Suzanne Schoenfelt

Internet and intranet technology is beginning to alter the development of electronic medical records. How do these systems work, and how have they affected the way HIM professionals work? Here's a look at some successful examples of the use of this technology.

Technology is driving information transmission worldwide. Elaborate electronic systems must now interact with each other to integrate various data forms. The Internet has infiltrated multibillion dollar corporations as well as studio apartments. Electronic commerce is the newest, hottest market for commodities from investment instruments to laboratory equipment. Internet technology is intricately woven into our business, financial, and personal lives. As a result, we are seeing transformational, multilevel societal changes.

Compared with other data-intensive industries, healthcare lags behind when it comes to using Internet-driven technologies. This is partly attributable to a lack of financial incentive to invest in the technology. Sensitive security issues related to private medical information also hamper development. As a result, the healthcare industry has scratched only the surface of potential uses for Internet technology.

But the news isn't all bad. Because electronic commerce has advanced more significantly in other industries, the healthcare industry can capitalize on progress already made. In other words, we don't have to reinvent the wheel.

Despite these barriers, Internet technology is already somewhat established in healthcare. Areas of its application include patient and clinical/professional education, e-mail between physicians and patients, consumer health information, research, clinical work, administration, policies and procedures, marketing research, physician referral, bulletin boards, staffing, and discussion groups.

If knowledge is power, consumers are the ultimate beneficiaries of these innovations. Patients are increasingly able to take charge of their own healthcare thanks to technology, according to John Hoben, who believes that technology is moving the entire industry in a new direction. "Bringing resources and knowledge to people is changing the patient/physician relationship and leading toward consumer empowerment," says Hoben, a health systems consultant in upstate New York who specializes in helping provider organizations leverage the value of Internet technology.

And how will Internet technologies change the jobs of HIM professionals? Though electronic filing of patient data has not fully evolved, the technology is drastically altering the ways patient data is stored and secured, as well as how it changes hands within an institution. HIM is reconfiguring; responsibilities are shifting. An electronic system may, in the final analysis, reduce an HIM department's work load, but in the short haul, the work load may increase. Increasingly, HIM professionals are being called upon to understand technology, because technology increasingly assists with the performance of their jobs.

Tool of the Future: The Electronic Medical Record

Despite the barriers, institutions across the country want—and are developing and implementing—electronic medical records (EMRs). About one-third of the nation's health systems have installed some form of electronic records.[1] Most large system vendors offer (or soon will offer) Web-based medical record systems.

The Web is composed of two parts: telecommunications systems and a collection of tools, languages, and sites that allow the various systems to communicate and share data with each other. Technology-wise, to develop the EMR, most institutions have

first put into place some form of intranet and/or extranet system. Intranets use the same Internet tools and languages within the boundaries of a single company or enterprise. They are internal networks. Like intranets, extranets are also private networks with access limited to a restricted user population. Extranets have the capability of extending the boundaries of a single organization for secure communication.

An Interest in Intranets: Systems that Support the EMR

Technological advancement is moving at breakneck speed. Implementation is moving more slowly, and EMR development is at various stages across the country.

An early phase in the development of the EMR began with the work of Clement McDonald, MD, codirector of the Regenstrief Institute in Indianapolis. In 1965, as an intern, McDonald became interested in the immense bookkeeping effort required to deal with documenting patient information. In 1972 he began building a computerized medical record at Wishard Memorial Hospital in Indianapolis. In total, he has invested most of his career in developing the EMR.

"EMRs provide a way to unify data and organize information, as well as eliminate costs, problems with note reading, and lost charts," McDonald says. He believes that EMRs definitely save physicians time.

Today, the Regenstrief Institute (RI), where McDonald is director, houses the infrastructure for Indiana University Medical Center and uses a local area network to link more than 40 Indianapolis sites, including nine hospital emergency rooms, the state and county public health departments, 11 clinics, and 12 homeless care sites. RI's computer system, called the Regenstrief Medical Record System (RMRS), is one of the world's largest clinical databases, with EMRs for 1.4 million patients. It includes more than 100 million separate patient observations and test results, 6 million prescription records, more than 2 million dictated reports, 250,000 EKG tracings, and tens of thousands of radiology images.

In 1995, the RMRS began operating with Web technology. Patients' medical records may be viewed via Web browsers by authorized care providers. The browser permits the display of all text reports, EKG tracings, and radiology images. This year, RI began to study the use of voice-to-text translation, with the hopes of replacing dictation.

Out of Site: Systems With Off-site Access

WebCIS

One intranet system that has off-site access capability is WebCIS at Columbia Presbyterian Medical Center (CPMC) in New York City. WebCIS houses EMRs and holds a data repository of lab results, pathology reports, EKG and radiology results, and various forms of transcribed reports. Authorized users are provided security token cards to access WebCIS from outside the system. Users may call into the system from a personal computer located anywhere. In this way, a physician who receives a call at home from a nursing staff member or patient can easily access a patient's EMR from WebCIS.

This ease of access has numerous advantages for staff, according to Karen Rosendale, RRA, senior director of HIM at CPMC: "WebCIS improves the work flow for physicians and other users, and it has advantages for the HIM department as well." According to Rosendale, WebCIS has also been helpful for patients because physicians can acknowledge current health problems from any location.

To enter WebCIS for access to patient information, a user must have a log-in ID and password. Users cannot see a patient's entire medical record (for instance, a podiatrist cannot access a patient's OB/GYN records) but can obtain information deemed necessary for their access level. The HIM department uses secured users' PINs, just as physicians do. Through the system, users may also access electronic tools, such as MEDLINE and *Physicians' Desk Reference*.

Security safeguards for the system (besides token cards, log-in IDs, and passwords) include encryption and screen IDs that act as gatekeepers to confidential information if a user signs off or if the system times out. Password screens ensure that some documents are accessed only once; if a user walks away from the computer and does not disconnect, no other user can log back on, track back through the program, or move into confidential areas.

CPMC is also looking at introducing some new features focused on the consumer view of healthcare information, including patient ability to enter and review data over the Web and patient and provider application of automated guidelines over the longitudinal EMR, including reminders to both physicians and patients.[2]

Patient Web

As at CPMC, physicians at Lowell General Hospital in Lowell, MA, are able to access medical records electronically from inside and outside the hospital through an intranet system called Patient Web. The system operates as a virtual private network. From inside the hospital, users log into the system with a password. From outside locations, physicians may access a Web site, then log into the system with a token card and a PIN. Users are authenticated, then data sent through the system's firewalls is encrypted to ensure data security.

Security for the system is multi-layered. Patient Web also uses the Microsoft NT operating system, which has its own built-in security that decides what information is appropriate for a particular user. The system tracks information requests for all users. System users include HIM professionals, reimbursement specialists, and other authorized personnel.

Patient Web contains EMRs for all patients who come to the hospital. The hospital is moving toward putting all patient medical records into the system, says Patricia Crawford, ART, assistant director of medical records at Lowell General. Currently, Patient Web houses all lab results, x-rays, dictations, operative reports, patient histories, physicals, and physician and pharmacy orders. As soon as a lab test is completed, it goes directly onto Patient Web. This allows staff members to give patients test results more quickly. While Lowell General is still keeping paper copies for now, ultimately, the whole system of patient records will be electronic, Crawford says.

The system has greatly simplified some parts of the daily work flow, Crawford reports. "Information to fulfill daily requests from patients is taken directly from Patient Web," she says. "To have patient data at our fingertips makes the flow of correspondence more efficient." Patient Web has also been a great tool for physicians. A physician covering for another physician used to have to decipher notes from the previous doctor and scramble for tests and notes. Now, he or she can just click on Patient Web.

MIND

At the University of Washington Medical Center (UWMC) in Seattle, the use of the new technology marks the end of reliance on one paper file. "Users can now sign on electronically so we don't have to shuffle documents all over UWMC," says Nancy Dunnington, RRA, director of patient data services at the center.

With paper documentation, the medical records department could send a record to only one department at a time. With electronic documentation, information is available at the point of care. "We now move fewer charts than even two years ago, because online information keeps increasing," Dunnington says. The number of requests for patient records for clinic appointments continues to decline as more data is available online.

Authorized users access their clinical system through the Internet by use of passwords, access codes, and a secure pathway to access MIND, a clinical data repository (MIND stands for Medical Information Network Databases). The system is organized by document-type tabs denoting categories such as demographics, health problems/ conditions/findings/procedures; clinic notes; medications; visits; transcribed reports; procedures; labs; radiology; pathology reports; and providers. It also includes an online clinical reminder system that alerts patients for routine patient exams (e.g., mammograms). In addition, providers can quickly access knowledge-based systems. For instance, to learn more about a new drug, a physician clicks on an icon that links to a database with more information.

System users must have security clearance and passwords. The system determines user authorization, application access, and password accuracy. It also tracks every access and has standard Secure Sockets Layer (SSL) encryption. (SSL is a high-level security protocol based on public key encryption for protecting the confidentiality and security of data while it is being transmitted over the Internet.) The system is also capable of limiting access when there is a compelling reason. For instance, only essential personnel have access to data if a patient has any sort of notoriety. People may also be locked out of the system for breaching security or confidentiality.

Data access is role-based and determined on a need-to-know basis. Medical staff members and nurses have full access. Other full-access users are HIM staff, ancillary services, and billing staff. Limited-access users include referring providers outside Seattle who have access to only their particular patients' data for a six-month period of time for each episode of care or file clerks who check only names and numbers.

Electronic maintenance of data saves time, Dunnington says. Less information is lost when records are maintained electronically because physically moving paper creates opportunities to lose information. If documentation is lost, the department simply reprints and resends. (When using paper records, the department must first locate the lost document.) Users access the EMR more often; some departments and many users access all the information they need online. "Documentation is legible, and quality has improved," Dunnington says. "Everyone appreciates that."

The department also enjoys the internal efficiency of being able to answer requests for information by printing directly from the EMR rather than pulling, clipping, and photocopying hard copies.

The only major problem with MIND, says Dunnington, is "we all want everything now. There's an anxiousness about moving forward faster than we're able." Until resources are available and appropriate policies are put in place, some innovations must be delayed and/or carefully deployed, she says. However, it's likely that the staff will be encouraged by previous successes with the system. "The efficiencies we have all realized assist in the delivery of services and care as well as the rapid availability of information for many users," Dunnington says. "This system has been a major process improvement."

Mayo Integrated Clinical Information System

In addition to improving processes, an electronic system is a tremendous advantage for a team approach to medicine, says Karel Weigel, RRA, operations administrator in the division for support services at the Mayo Clinic in Rochester, MN. Team medicine—using input from various specialties to diagnose patients—was pioneered at Mayo, an integrated group practice that is somewhat different from standard hospitals.

Mayo uses intranet technology to link clinical information sites in Rochester, MN, Jacksonville, FL, and Scottsdale, AZ. The Mayo Integrated Clinical Information System (MICS) is being developed to implement the EMR, which has been in the making for 10 years. MICS allows multiple users to access the same information simultaneously. For example, an internist's patient can have an EKG, then be seen immediately by a cardiologist. When the patient reaches the cardiologist, the EKG is already in the data bank for viewing. "The physician is not waiting for physical pieces of paper," Weigel says. "Virtually all tests are immediately available."

The EMR, like its manual predecessor, is source oriented and is divided into sections composed of demographic data, the patient's history, clinic notes, lab information, pathology data, and other ancillary tests (including EKGs and x-rays). "Every patient at the Mayo Clinic has one medical record for life," Weigel says.

Governed by long-standing institutional policies on access to medical information, MICS is physically controlled to assure appropriate access to vital clinical information while maintaining patients' privacy and confidentiality. A user must sign on to the system and then be approved (by password verification) to access patient medical records. All Mayo physicians have access to clinical information. Other healthcare professionals (such as nurses and lab technologists) are allowed to log into the system; some employees have access for functions such as billing.

Security measures are based on the premise that all users must have access to the information they need, but nothing more. This is controlled with system and application security features, such as enforcement of password standards, inactive time outs, and ability to audit user access. Some access is controlled by the type of computer employees have, and users must have background security clearance. Once a user signs on, the system itself clears the user through a password. The system recognizes access and security clearance.

Currently, the Mayo staff still uses hard copies of medical records as well as the EMR, but Weigel says most medical information created today is electronic. "We look forward to the day when medical records are all electronic. At some point, we will change over completely to electronic patient records," she says.

Transmitting patient medical information electronically, Weigel says, is much less complicated than manual procedures. Benefits include ease of access and the opportunity to integrate patient information. However, because the current system

involves maintaining both paper and electronic information, some backlogs have appeared during the adjustment phase. As a result, Weigel says, the transition to the EMR is enormously labor intensive. But, she adds, "The system is so superior that it's worth going through the work and discomfort of the transition."

Mayo is still working to overcome some of the other barriers to implementing the CPR, such as overcoming users' qualms. "Some physicians are reluctant to learn to use the technology," Weigel says. "We must overcome that. Another barrier is security."

Security: The Hot Button

Nothing touches a nerve in the HIM community like security and patient confidentiality issues. For that reason, maintaining medical information online requires great caution. Information stored on the computer is not necessarily easy to access; in fact, some believe technology actually makes the data more secure. Technology provides additional security that a paper system cannot. Even so, there is no error-free system, and storing health information electronically raises old issues in a new context.

Increasingly, patients themselves are concerned about who has access to their information. These fears can be exacerbated by a general lack of understanding of technology and the Internet. Healthcare organizations need to address these fears. The Mayo Clinic, for example, addresses the issue with patients in a number of ways. When patients ask about security, they are reassured individually and they receive a patient brochure assuring them that health information is confidential.

It's true that no system is foolproof. The familiar image of the computer "hacker" is known to most consumers. Hoben, for one, doesn't believe these people pose a tremendous threat to health information security. "There are hackers in this country who can hack any system," he says. "Fortunately, many of these people are not hacking systems for the sake of blackmailing or selling information and use hacking mostly for good; some are contracted by, for instance, the FBI and the Department of Defense." Experts agree that the most common threats to health information confidentiality come from people within an organization who already have access—and frequently involve the health records of celebrities, VIPs, or others whose health is economically important or newsworthy.

For staff, using new technologies for computer-based records often means taking special precautions. UWMC believes that education is an important component of the process. All staff sign a security and confidentiality understanding. New employees participate in general security and confidentiality orientation. Departments provide more specific education about specific behaviors, such as appropriate care of passwords and logging off unattended workstations.

Technology itself can help foster awareness. Employees who are also patients may request a security alert on their medical records. When the record is accessed, a red security alert flashes on the computer screen to remind users about confidentiality. Additionally, this alert includes a reminder that misuse of information is illegal and against hospital policy.

In addition, each Monday, randomly chosen UWMC employees receive e-mail queries about use of the patient data stored in MIND. Intended to raise awareness, this practice reminds users of the importance of confidentiality. The query also asks employees for feedback about the system (as a way of gathering information). If employees don't respond to the e-mail missives, Dunnington contacts them personally. A response is required and if it is not received, a user's access could be cancelled.

Concerns about security have slowed down development of Internet-based systems, but that won't last forever. McDonald, for one, believes that industry should move forward and take advantage of available technological and electronic advances. "By making healthcare more broadly available and more efficient, we can do tremendous good for the world," McDonald says. "If we can make healthcare more efficient by using technological resources, we should do that."

A Model for Security

In the fall of 1998, the Three State Health Information Project released a security plan, the first part of a two-phase project sponsored by the Robert Wood Johnson Foundation, to find ways to offer a secure infrastructure for electronic commerce (handling administrative and medical data via the Internet) in healthcare. The report explains a series of six recommended health security levels for implementation. Levels of security vary depending on the type of information and the need to secure that information. (The EMR, for instance, is a health security level 6.)

The report also proposes a security model driven by certificates of authority (a digital means of verifying a user's identity), encryption technology, and corporate privacy guidelines. Phase two plans to implement local projects that put into place the elements necessary to develop a public key infrastructure (a secure infrastructure environment for healthcare electronic commerce). Phase two will implement the model developed in the first phase.

"Without the right policies and procedures, technology cannot protect data properly. In healthcare electronic commerce, 80 percent of security involves policies and procedures; 20 percent involves technology," says Walter Suarez, MD, executive director of the Minnesota Health Data Institute. Suarez admits that even with the best security systems in place, there will always be a very small risk of having information exposed. "We are trying to minimize that risk," he says. "Our hope is that the proposed structure will catch on to become a national model for a secure infrastructure approach to electronic commerce in healthcare."

Partners in the Three State Project include the Minnesota Health Data Institute, the Massachusetts Health Data Consortium, and the Foundation for HealthCare Quality in Washington. Organizations currently forming these state consortiums include, among others, the Mayo Clinic, Harvard Medical School, the University of Washington, and Blue Cross and Blue Shield of Minnesota. The Utah Health Information Network and North Carolina Health Information Alliance will participate in phase two.

Riding the Wave

Healthcare cannot afford to take a "wait and see" approach to technology. Access to patient information is too critical. Complex technological change—and its rippling effect on medical data—is staggering in its immensity and its pace. As a result, it becomes necessary to ride the wave of technology. Traversing the waters of technological evolution is a balancing feat of holding on while letting go, of releasing outmoded thinking while navigating a new electronic medium.

Not surprisingly, the HIM profession as a whole no longer finds itself on *terra firma*. The evolution of the EMR and of technologies such as intranets and extranets mean that HIM processes will evolve accordingly. The resulting transitions will be challenging and often difficult, but the stories told in this article are evidence that they can be accomplished successfully.

Click here to read "[Intranets -- From EMR to ER and Beyond](#)"

Notes

1. Menduno, Michael. "Prognosis Wired: Why Internet Technology is the Next Medical Breakthrough." *Hospital and Health Networks* 72, no. 21 (1998): 28-35.

2. "On the Move: Transferring Records Via the World Wide Web." *AHIMA Today*, October 21, 1997.

Resources

Bazzoli, Fred. "Building a Network on a Low Budget." *Health Data Management* 5, no. 12 (1997): 54-56.

Chin, Tyler L. "Defining a New Term." *Health Data Management* 5, no. 6 (1997): 30-33.

Chin, Tyler L. "On-call Physicians Gain Access to Records." *Health Data Management* 4, no. 10 (1996): 18-20.

Cupito, Mary Carmen. "Intranets: Communication for the Internal Universe." *Health Management Technology* 18, no. 7 (1997): 20-58.

Duffy, Tom. "Saving with VPNs: Memorial Hospital Alliance and Mede America Prove Virtual Private Networks Can Help Slash Costs in Health Care and Other Industries." *Network World*, May 18, 1998.

Ernst & Young, LLP. "Executive Summary: The Role of the Internet in Healthcare." Monograph. Ernst & Young, 1997, pp. 1-27.

Hagland, Mark. "Glimpses of a Web-enabled Future." *Health Management Technology* 19, no. 4 (1998): 22-29.

Hagland, Mark. "How 'WebCare' Is Changing Health Care Delivery, Hit by Hit." *Health Management Technology* 18, no. 4 (1997): 22-26.

Jones, Charles M. "The Internet Access Breakthrough: Bringing Healthcare Home." *Healthcare Informatics* 14, no. 7 (1997): 62-64.

Kohn, Deborah. "Let's Hear It for the Users! Diagnostic Imaging on the Internet." *Health Management Technology* 18, no. 5 (1997): 14-18.

McCormack, John. "Intranets." *Health Data Management* 5, no. 12 (1997): 29-35.

McDonald, Clement J. "The Barriers to Electronic Medical Record Systems and How to Recover Them." *Journal of the American Medical Informatics Association* 4, no. 3 (1997): 213-221.

McDonald, Clement J., William M. Tierney, J. Mark Overhage, Douglas K. Martin, and Gregory A. Wilson. "The Regenstrief Medical Record System: 20 Years of Experience in Hospitals, Clinics, and Neighborhood Health Centers." *M.D. Computing* 9, no. 4 (1992): 206-217.

Meyeroff, Wendy J., and Richard E. Meyeroff. "Got It? Share It." *Healthcare Informatics* 15, no. 11 (1998): 105-108.

Opus Communications. "The New Frontier: Patient Information on the Internet." Supplement to *Medical Records Briefing*, 1996.

Pasternack, Andrew. "Cyber-Emergencies: WWW.Milwaukee.ER." *Hospitals and Health Networks* 72, no. 14 (1998): 40.

Sherter, Alain L. "Providing Easier Access to Clinical Data." *Health Data Management* 5, no. 3 (1997): 33-37.

Siwicki, Bill. "An Internet Primer." *Health Data Management* 4, no. 3 (1997): 50-54.

Siwicki, Bill. "Applying the Internet in Healthcare." *Health Data Management* 5, no. 3 (1998): 39-48.

Siwicki, Bill. "Mayo Leading the Way." *Health Data Management* 5, no. 12 (1997): 49-50.

Tadjer, Rivka. "Web Site Triage—A Web Site that Links Medical Records Among Six Boston-area Hospitals and Leverages Proprietary and Existing Systems Is Up and Running." *CommunicationsWeek*, May 19, 1997.

Woody, Todd. "The Trillion-Dollar Opportunity." *The Industry Standard* 2, no. 11 (1999): 30-48.

Suzanne Schoenfelt is owner of The WordSmith, a medical, scientific, and pharmaceutical communications service in the Chicago area. Her e-mail address is WrdSm@aol.com.

Article citation:
Schoenfelt, Suzanne. "Next Generation: How Internet Technology Propels the Electronic Medical Record." *Journal of AHIMA* 70, no.8 (1999): 30-36.

Driving the Power of Knowledge