Coordinated Care with Electronic Health Records

Implementation of an electronic health record system will create an interoperable healthcare system for more efficient patient care.

By Amy Scanlin, MS

Healthcare is entering a new era — one that will be especially important for individuals with autoimmune and immune deficiency diseases. This new health information technology (HITech) era will make health information interoperable, allowing physicians, labs and insurance companies to exchange data and communicate quickly and efficiently to provide the best possible care for patients — all made possible with electronic health records (EHRs). Whether the patient is between specialists for a chronic disease, having routine exams or tests, or even a victim of a disaster such as Hurricane Katrina, EHRs will enable a wider breadth and depth of care.

EHRs store patient information, protect patient privacy and allow for the retrieval and proper dissemination of information, including insurance. As more healthcare entities (ambulatory, emergency, hospital-based) roll out their EHR programs, EHRs will become an integral part of healthcare for every American. The government is going to great lengths to ensure this initiative is successful on all levels, and as we get closer to the deadline of full EHR implementation, things are changing rapidly.

EHR Beginnings

On April 27, 2004, President Bush signed Executive Order 13335 with the goal of developing and implementing a nationwide infrastructure for health information technology that would improve the quality of healthcare. He also established the Office of the National Coordinator (ONC) of Health Information Technology within the U.S. Department of Health and Human Services to ensure a number of benchmarks are met:

1. Patient's health information is secure, protected and available to the patient.
2. Appropriate information is available to guide medical decisions at the time and place of care.
3. Healthcare quality is improved while reducing healthcare costs resulting from inefficiency, medical errors and inappropriate care.
4. Information dissemination between hospitals, laboratories and physician offices is improved.

Bush's goal was to provide the majority of Americans access to their EHRs by 2014. And, while President Obama's February 2009 joint address to Congress echoed the initiative to move forward with EHRs, he wants to speed up the timeline. Obama's American Recovery and

Reinvestment Act of 2009 (ARRA) gives priority to EHRs as part of his overall healthcare reform, and he is providing stimulus money to healthcare providers that initiate and can show "meaningful use" of electronic systems.

Starting in 2011, financial incentives will encourage healthcare providers to convert to electronic systems earlier than 2014.[1] As 2014 nears, the incentives will become smaller, and by 2014, financial penalties will be imposed on healthcare providers that have not switched to electronic health information systems. "The expectation is that adoption will increase dramatically when these incentives become available," says Deven McGraw, director for the health privacy project at the Center for Democracy and Technology.

According to an article in *Healthcare IT News*, "More than two-thirds of physicians in the country will respond to the incentives offered by the HITECH (Health Information Technology for Economic and Clinical Health) portion of the American Recovery and Reinvestment Act because it represents a 'significant' incentive. However, participation is likely to be skewed toward practices with more than three physicians." Therefore, to achieve the greatest results, it is suggested that the government provide smaller practices with technical and financial assistance.[2]

Where Are We Now?

The current EHR adoption rate is roughly 10 percent, making 2014 a very ambitious timeline to get healthcare providers on board. Large organizations such as Kaiser Permanente and the U.S. Veterans Administration are currently leading the way, but smaller practices are slower to go electronic. One reason is that switching to an electronic system is costly, which is why the government is offering financial incentives. In addition, many physicians are comfortable with the way their offices currently operate and are uncomfortable with changing computer systems and the associated issues such as computer literacy, security, etc. There is also a lot of confusion about the best way to go electronic.

To receive stimulus money, not only must the healthcare provider use a "certified" EHR product, it must be doing so in a "meaningful" way. The term "meaningful" is at the center of debate as planners — from Congress to HITech companies to physicians — come together to determine specifically what "meaningful use" means. It is anticipated that electronic prescribing, laboratory reporting, clinical summaries for care coordination and quality data will be covered in the definition.[3]

Therefore, for companies that are ready to go electronic, it is recommended that the contracts with EHR providers include a provision that states the system will work when the definition of "meaningful use" has been determined by the Secretary of Health and Human Services.

The requirement for the use of a "certified EHR" also remains to be defined. Currently, EHR products are certified by the Certification Commission for Healthcare Information Technology (CCHIT). On May 29, 2009, CCHIT released its "Concise Guide to 2009 CCHIT Criteria for ARRA-qualified EHRs," and it anticipates final criteria to be in place in August after the proposed criteria are examined by the ONC to ensure compliance with ARRA stimulus guidelines. Each year, the certification criteria are intended to improve upon the previous year's requirements, as technology gets more advanced and improvements are needed in the system. According to the ONC, "There is a lot of work that needs to done. Numerous efforts are under way to address critical issues and launch grant and incentive programs to spur the adoption of EHRs. These programs will be announced in the next several months."

Starting in 2011, financial incentives will encourage healthcare providers to convert to electronic systems earlier than 2014.

EHRs in Action

The Department of Veterans Affairs (VA) has been using EHRs for over a decade and has won awards from Harvard's Kennedy School of Government and praise from journals such as the *New England Journal of Medicine* for one of the most comprehensive and sophisticated usage of EHRs in the nation. The initiatives VA is using are similar to those patients can expect to see as healthcare providers adopt the EHR system.

When doctors view a patient's records, they instantly see active health concerns, allergies, medications, recent lab results, etc. The system also alerts doctors, before an order is placed, to any potential problems, and offers benefits such as e-scribing (an automated prescription drug process) to prevent misread prescription orders.

VA's EHR system uses VistA Imaging, which allows doctors to see X-rays, pathology slides, photos taken during endoscopies, surgeries, eye exams, etc., including those taken at other VA locations. The system also uses bar-coded medication administration that scans the prescription and the hospitalized patient's wristband to ensure accuracy. VA states that medication errors have been reduced by two-thirds with this technology.

> *Patients' health information should be shared only under necessary circumstances that enable providers to accomplish their specific goals for patients.*

Patients can also create a Personal Health Record (PHR) using VA's My HealtheVet, at www.myhealth.va.gov, and VA is gradually allowing online access to the patient's EHR as part of this PHR (patients can request their full records at any time). This is highly beneficial to both doctors and patients, because patients are able to take a more active role in their healthcare. "We use the EHRs as a teaching tool for patients," says Gail Graham, deputy chief officer for health information management at the Veterans Health Administration's Office of Health Information. "Right now, patients can view portions of their EHRs like upcoming wellness reminders, and they can refill VA prescriptions online. Next, we are working on secure patient messaging where they can ask questions of a physician and receive answers on their personal and secure account, while keeping within the HIPAA requirements. We are trying to advance as the technology enables."

Another upcoming feature of the PHR is the ability for patients to allow others to see their records, such as a family member or other caregiver. This will be especially helpful for adult children helping aging parents or for veterans who receive some of their care from non-VA sources. "We have been fortunate," says Graham, "that our vets have embraced the electronic health record and have come to expect it. It allows for the continuity of care wherever the patient is in the country. We see big changes as [the adoption of EHRs increases and] we are able to connect more with the private sector. Our goal is to be here to support the president's initiative."

Patients' Role in EHRs

One of the major benefits of EHRs is the ability of patients to take an active role in their care. When checking in for an appointment, patients are by law given a "Notice of Information Practices" to sign. Patients have the right and should be provided access to view their health information in a readable format (however, they may be charged a copy fee). Information should be checked to be certain it is up to date and accurate. Patients may dispute the accuracy of their records and either have the information changed or have the dispute documented in the records if the request for change is denied. This is an important step, because incorrect information replicated through the course of care can have serious consequences. Potentially, incorrect information could be anything from administrative errors to medical identity theft, so the opportunity and responsibility for review should be taken seriously. Patients should also understand what health information is in their EHR, how it is being used and who has access to it.

A major initiative for the government is to educate people about HITech and to communicate with everyone involved. According to Meryt McGindley, acting communications director for the National eHealth Collaborative, "We want people to know why this is important, how the healthcare system will go about making the switch and how we will overcome barriers to implementation. We have choices in this country as to where we get our healthcare, and healthcare reform is a major topic of discussion. A lot of people think doctors are already networked and that we are a lot further along than we are. So ask questions when you are choosing a doctor, choosing a specialist, choosing a hospital. Will [the healthcare providers] all be able to communicate?"

Security and Privacy Laws

Patients' health information should be shared only under necessary circumstances that enable providers to accomplish their specific goals for patients. A 2006 *Los Angeles Times* article estimated that approximately 150 people can have access to an individual's records while they are hospitalized.[4] The intent of new privacy and security policies is to define the type and amount of information collected on a patient, limit who has access to that information and, in turn, limit the potential for misuse.

While there are many federal and state laws protecting patients' privacy, the most familiar law related to medical privacy is the Health Insurance Portability and Accessibility Act (HIPAA). This federal law allows "covered entities" to use the data for routine healthcare purposes (like treatment, payment and administrative tasks) without patients' consent. However, it does prevent the sharing of personal health information for non-routine purposes without consent.

HIPAA and other laws were created before the idea for EHRs, so although the law covers health information in electronic form, additional issues and considerations are still being worked out.[5] "Many of these gaps were resolved in the recent economic stimulus legislation, which made a number of improvements in the HIPAA privacy rule. Ensuring appropriate implementation of these new provisions will be key to ensuring there are sufficient privacy protections for patients whose records are stored and shared electronically," says McGraw.

Of particular importance for many chronically ill patients is access to EHRs by health insurance companies. Health insurance companies fall into the same "covered entities" category under the federal HIPAA law. They must provide patients with a privacy notice and take precautions with information to protect patients. However, it is less of an issue that insurance companies are going to unlawfully use data, and more of an issue of *how* they are going to use the insured's information. Insurance companies do have the right to use patients' data for medical underwriting and deciding whether, for instance, a test the doctor prescribed is medically necessary. This utilization review by insurance companies is where many have concerns, because should insurance companies see something as a pre-existing condition, they can deny coverage. This is particularly true if the health plan is individually purchased. Individually purchased plans do not have the same federal protections as group (employer) plans, and that lack of protection is something that is being addressed in the healthcare reform.

Another major concern in the electronic age is security. Is the unsecured exchange of electronic information allowing patients' information to get into the wrong hands? If so, how can the government, hospitals, developers of EHR software and patients keep information secure? "Good security," says McGraw, "will keep unauthorized persons (such as hackers or hospital employees who are snooping in records of patients they are not treating) from accessing the record."

There are also concerns about whether privacy protections — the policies and standards for who can access information and for what purposes — will serve as a barrier to the ability of patients and physicians to access health information. But, that shouldn't be an issue if privacy rules are designed to allow for easy physician and patient access, while limiting or prohibiting the ability of others (such as marketers) to access the record. Today, privacy rules permit physicians to access data for treatment purposes, and patients are able to get an electronic copy of their records (if their providers keep records electronically) in a shorter period of time.

The policies and standards for internal compliance and enforcement by CCHIT were created by the American Health Information Association, the Health Information and Management Systems Society and the National Alliance for Health Information Technology, and are instrumental in the issue of security because they set standards for certification of EHR systems. Software developers are using these criteria to ensure systems can work together (interoperability) and safely. The ONC adds that "privacy and security in electronic health exchange,

the cost of this technology and how useful it will be in the day-to-day provision of care are some of the key issues that need to be addressed. We recognize the critical importance of privacy and security for electronic health information and will continue to address this issue through our policy and implementation work. The technology exists, and continues to be enhanced, to provide a secure and private environment to store and exchange health information."

Patients' Role in Security and Privacy

Patients also have a responsibility to help keep their information safe as they view their records on a computer. On home computers, firewalls, virus protection and malware protection is essential. There are free and for-fee programs on the market that offer varying levels of protection, and they are updated regularly.

> ***The use of someone's healthcare file or medical records without their consent constitutes medical identity theft.***

Security becomes more difficult when using a shared computer, such as a library or Internet café, because it's possible that the computer may have malicious software installed by someone looking to steal information. If a shared computer must be used to view information, first inquiring about what kinds of security scans are run on the computers is important. A location that offers more security scans and more protections will better help protect information. Also, shared computers may not have had malware installed, but someone may have inadvertently visited a website or opened an email that had malware attached. To help secure information, login IDs and passwords on a shared computer should never be saved, and at the end of each session, the browsing history and "cookies" should be deleted.

If patients feel that their personal information has been violated, they should contact the privacy officer for their health plan or provider. This is also the person to turn to if patients have trouble getting a copy of their records. When unable to resolve this issue, patients may want to file a complaint with the Department of Health and Human Services Office of Civil Rights within 180 days of the incident. If it is determined that there is a violation, this office will impose penalties against the defendant. More information on how to file a complaint can be found at www.healthprivacy.org and www.hhs.gov/ocr/hipaa.[6]

Medical Identity Theft — A Special Precaution

The use of someone's personal health, insurance, social security number, healthcare file or medical records without that person's consent constitutes medical identity theft, a serious fraud with serious financial consequences. And it also causes complications for patient care.

Government and computer security experts are working hard to provide additional safeguards in preventing medical identity theft. It is still a relatively new issue, though it is clear that the number of cases is growing exponentially. As EHRs gain ever-increasing footholds in the nation's healthcare plan, the government is working with its own agencies, as well as private sectors, to better understand how to detect and prevent medical identity theft.

"Health information technology offers great promise to improve the health and care of every American," according to the ONC. "Electronic health records can reduce medical errors, make care more efficient and are essential to moving our healthcare system into the 21st century."

As 2014 nears, patients can expect to see changes in the way providers manage their care. In the meantime, many issues are being worked out, and many risks are being mitigated.

References

1. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848084_0_0_18/HITStrategicPlanSummary508.pdf.
2. Merrill, M. "Higher P4P Rewards Equals Greater Participation." Healthcare IT News, May 7, 2009, http://www.healthcareitnews.com/news/higher-p4p-rewards-equals-greater-participation.
3. Manos, D. "New Health IT Policy, Standards Panels Start Work." Healthcare IT News, May 29, 2009, http://www.healthcareitnews.com/news/new-health-it-policy-standards-panels-start-work.
4. Foreman, J. "At Risk of Exposure." Los Angeles Times, Jun. 26, 2006, http://articles.latimes.com/2006/jun/26/health/he-privacy26.
5. Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. Dec. 15, 2008, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf.
6. "Health Privacy: Know Your Rights." Online brochure of the Health Privacy Project, www.healthprivacy.org.

AMY SCANLIN, *MS, is a freelance writer specializing in medical and fitness writing.*