

In an environment of reduced health care budgets, health care organizations are facing more demands to implement new and costly information technology initiatives. At the federal level, President Obama recently signed into law the American Recovery and Reinvestment Act, which allocates more than \$20 billion to meaningful use of health care information technology in coming years. At the state level, Minnesota legislation has mandated statewide implementation of interoperable electronic medical records (EMRs) by all hospitals and health care providers by 2015. And at the same time, patients are demanding a greater level of access to their medical records and more input into their health care decisions.

At the intersection of these opportunities, requirements, and desires is the need to share patients' health information while ensuring its security. Information about our health and health care is by far the most sensitive data we own. From chronic conditions to medications to genetic makeup, our personal health information (PHI) reveals intimate details about who we are, what we do, and what we may be like in the future. For these reasons, interoperable health information systems that share electronic personal health information (ePHI) must be built, deployed, and adopted in a manner that ensures responsible, appropriate, and authorized use.

Privacy and confidentiality concerns

Though many large medical or-

ganizations have switched from paper to electronic medical records, only about 17 percent of the nation's physicians are using computerized patient records today, according to a government-sponsored survey published last year in *The New England Journal of Medicine*. In the world of paper-based health records, it would be virtually impossible to identify and aggregate all of an individual's medical records, which might be stored in dozens of physicians' offices, hospitals, laboratories, and other facilities in diverse geographical locations. The current lack of records coordination has the indirect effect of protecting patients' sensitive health information from disclosure. This inadvertent protection, however, is likely to disappear with the creation of the Minnesota Health Information Exchange (MN HIE) and the National Health Information Network (NHIN), *state and federal organizations tasked to adopt standards to ensure interoperability with other regional and national systems. MN HIE will connect doctors, hospitals and*

Interoperable systems raise ePHI security concerns

Exchange of ePHI causes healthcare organizations to re-evaluate the security of their IT network

By Scott Warzecha

clinics across the state so they can quickly access secure electronic medical information."

The development and deployment of interoperable medical records systems through the MN HIE and NHIN raise important questions of privacy and confidentiality. As the amount of easily accessible health information increases, so do the potential risks to privacy and confidentiality stemming from inappropriate disclosures.

The primary concern with regard to interoperable systems and the availability of ePHI outside the walls of the care facility are that irresponsible health care entities and rogue employees will divulge information or that snoopers and hackers will get access to private information. In a recent example, 15 employees of a Kaiser Permanente hospital in California were fired in March for accessing the medical records of the mother of octuplets who were born at the hospital. And in April 2008, the American Health Information Management Association issued a report on records privacy following a rash of

security violations that included the medical records of actor George Clooney and singer Britney Spears.

ePHI and HIPAA

The precise structure and operating mechanism of the MN HIE and NHIN have yet to be determined. Under any likely arrangement, however, individual ePHI will be accessible via an interoperable network.

With the implementation of an interoperable exchange network come wide-ranging health information technology implications. Securing ePHI via an interoperable network is more complex than assuring general IT security of patient data stored within an entity's internal network.

The HIPAA Security Rule specifically addresses the confidentiality, integrity, and availability of ePHI as it is created, received, maintained, and transmitted by health care entities. The rule cites security standards for implementing ePHI security in terms of administrative, physical, and technical safeguards. Because of the possible vulnerability of an "open network," the rule is intended to ensure that covered entities are taking all precautions necessary to make certain that ePHI is not compromised.

While implementing an EMR can bring your organization into 21st-century health care IT, it also exposes the organization to potential risks and vulnerabilities if your network is not properly configured and safeguarded against security breaches. Consider these questions when as-

Physician

The Independent Medical Business Newspaper

sessing risks related to EMR and other HIT use within your organization:

- How will I protect the confidentiality of ePHI through interoperable systems?
- Who in my organization needs access to the EMR system and the ePHI within it?
- How will I prevent ePHI from being accidentally or maliciously disclosed through the health information exchange?
- How will I ensure that ePHI is readily available to me when and where I need it?
- What kind of performance standards does my network have? Is it reliable enough for eHealth standards?
- In the event of a data loss, what are my backup policies and retrieval tactics?
- How will I involve my patients in their health and health care decisions?

The consumer's new role

In the receding economy, health care consumers are demanding more from their health care providers in order to control their own health care costs. Consumers want open access to their medical records without having to call a clinic, hospital, or other health care entity.

Through the use of information technology such as personal health records (PHRs), consumers are becoming more involved in their own health care decisions. Consequently, most of the information exchange between health care entities and consumers is taking place via the Inter-

net. The Markle Foundation reported in a 2008 survey that 54 percent of consumers have an interest in PHRs and believe PHRs would help them avoid duplicate tests, track health care expenses, and manage their own health better. However, consumers say they see privacy as the single greatest barrier to PHR adoption. The privacy and security of ePHI exchange is in the hands of the health care entity.

The ultimate solution roadmap

The ultimate solution for consumers would be to have individ-

ual access to their personal health information; control over who accesses it; and confidence that its collection, use, and disclosure is limited to those who have a medical need to access it. The standards and technology required to implement this level of control will likely take five to 10 years to mature. In the meantime, the following roadmap proposes a multi-year plan that will protect privacy, ensure accountability, and promote patient safety.

Present through Year 3: State-of-the-art security technology can now enable access controls that

prevent unauthorized individuals from gaining access to any system storing or providing ePHI. Health care providers have necessary access to ensure the patient receives treatment, but this access is carefully tracked to provide accountability.

Years 3 through 6: By this time, the Health Information Exchange networks will have access controls that recognize the role of the treating clinician. This role is assigned to individuals who have a treatment relationship with the patient and thus have a legitimate reason to access that patient's ePHI. Currently, this level of access is somewhat available in single-organization EHR systems; extending it beyond internal walls and throughout the HIE and NHIN would be a significant gain.

Years 6 through 10: Access standards will place more control into the patient's hands. Fail-safe mechanisms will be built into this system to ensure that the critical patient data is available in case of emergencies.

Gaining public trust and assurance

If the road to securing ePHI seems long, difficult, and costly, that's because it is. Patient privacy and confidentiality do not come cheap—or easy. However, these protections are crucial in establishing and maintaining the public trust in the MN HIE and NHIN. To do less, risks losing the public's confidence in the entire health care system and doing irreplaceable harm to an individual's identity.

Recommendations for Patient Involvement

Patients need understandable, culturally appropriate information about the changes in healthcare delivery that will result from the adoption and use of MN HIE and NHIN. Patients need to be aware of their options for participating in ePHI exchange and how it will affect them.

- **Patient-based access.** As the HIE and NHIN directives are implemented, patients will have the right to accept or decline the right to participate in the NHIN. At the very least, individuals should have the choice whether to make their health records available via the NHIN and they should have some control over the content of the health information disclosed.
- **Role-based access.** The health care professional's level of access to an individual's ePHI will depend on the role of the professional—and the needs he or she fulfills. Thus, treating physicians and nurses would get a higher level of access than billing clerks and food service workers. Role-based access criteria already have been adopted by many large health care organizations with EHR systems, and this requirement should be expressly mandated for all health care records systems.
- **Contextual access.** The scope of information disclosed to third parties for non-medical purposes is limited using contextual access. For example, life insurance companies would receive only information related to mortality risk, and employers would receive only information related to an individual's ability to perform a specific job.