HITECH Imposes New EHR Security Measures

Federal penalties for breaches of personal health information are significant and will be enforced.

BY ERIK L. GOLDMAN

DENVER — If federal stimulus money to the tune of $44,000 per physician has warmed more solo and small group practices to the idea of adopting electronic health record systems, the new Health Information Technology for Economic and Clinical Health Act could cool their enthusiasm.

The HITECH law imposes significant responsibility on medical practices in the event of a breach of patients' protected personal health information.

"The statute giveth, and the regulations taketh away," Gerry Hinkley, a partner specializing in health-information law with a San Francisco law firm, said at the annual conference of the Medical Group Management Association.

HITECH imposes a host of new security obligations on all practices covered by the Health Insurance Portability and Accountability Act (HIPAA).

Most worrisome to the average physician are those that pertain to breaches of health-information security, said Mr. Hinkley.

The law defines "breach" as unauthorized acquisition, access, use, or disclosure of personal health information that compromises the security or privacy of that information and carries significant risk of financial, reputational, or other harm to the subjects of the record in question.

If a breach occurs, the medical practice must notify each patient whose personal health information has been accessed, modified, or inappropriately disclosed because of the breach as soon as possible, but definitely within 60 days of breach discovery. The practice must also post information on its Web site indicating that a breach has occurred.

If the breach potentially affects more than 500 residents of a state, the practice is also obliged to notify local newspapers and other media outlets, as well as the office of the U.S. Health and Human Services Secretary.

"You need to state what happened, when it happened, when it was discovered, the specifics of what was breached, what course of action [the affected] patients have, and what you are doing to mitigate the damage," said Mr. Hinkley.

He added that these notification rules have technically been in effect since late September, but enforcement won't start until March.

The regulations distinguish between mistaken access to a patient's health record by an authorized person vs. access (especially intentional access) by an unauthorized individual. The former is not considered a breach.

"This is really about prevention of leakage of sensitive health information to unauthorized persons," he said in defense of the rules.

So if a doctor loses a mobile device or laptop computer that contains patient health records, must he or she call the local media?

That really depends on how well the information has been protected. If the patient files are easily opened, then yes, the lost device would likely constitute a breach. But if the records are well encrypted and password protected, then the information is considered secure and unbreachable, even if the device itself falls into unauthorized hands, Mr. Hinkley noted.

"You really need to talk to your [EHR] vendors about how they encrypt patient data," Mr. Hinkley advised. He added that electronic communications with patients should, when possible, take place via secure online portals rather than ordinary e-mails or text messages. Material exchanged via e-mail could be considered breachable personal health information, and it's a risk doctors need not take.

HITECH extends a medical practice's responsibility for personal health-information security to all of the practice's business associates, which will include any and all entities with which the practice exchanges potentially sensitive information, including other clinics, vendors, health-information exchanges, regional health-information organizations, e-prescribing gateways, and IT vendors.

"Your business associates are directly responsible to comply with the security rules and can be held accountable to the government for any violations," Mr. Hinkley said. Business associates are required to quickly report any potential breaches or violations to the practice, but the burden is on the practice to ensure that business associates are in compliance with current rules.

That means that all contracts with business associates—especially new ones—need to contain language addressing personal health-information security, and need to demand compliance with HIPAA and HITECH.

Both HIPAA and HITECH stipulate that the exchange of personal health information among authorized clinical staff must be for "meaningful use."

Furthermore, only the "minimum necessary" amount of information for that meaningful use should be transferred. Currently, the disclosing party has discretion to determine what is the "minimum necessary" information in a given clinical situation. But there could be serious penalties if that determination is contested.

Both "minimum necessary" and "meaningful use" are very vaguely defined in the existing law, leaving a lot of room for interpretation and risk, Mr. Hinkley said, adding that "if you act unreasonably as far as disclosing more patient information than is necessary for a given case, there's some significant enforcement risk."

Medical groups and health IT organizations are pushing for the U.S. Health and Human Services Department to clarify those terms so that the ground rules and boundaries are well defined. Mr. Hinkley said to expect more clear definitions between now and next summer, when he expects the government to start enforcing this aspect of HITECH.

Under existing laws, patients have the right to "individually requested privacy restrictions," and the new laws will sustain and extend those rights. As of next year, patients will have the right to prohibit a medical practice from disclosing any information to insurers about a patient's self-pay services.

The regulation is an effort to protect patients from insurance company abuses around preexisting or potentially high-risk conditions, explained Mr. Hinkley. For example, a patient will now have the right to pay out of pocket for an HIV test and know that his or her serostatus will not be reported to an insurer that might drop the patient or significantly increase premiums if the patient were found to be HIV positive.

Expect heavy HHS enforcement of this and other privacy restriction rights, Mr. Hinkley said. "The [department's] Office for Civil Rights will step up efforts to make the public aware of this. It applies to anything a patient wants to do outside the scope of a health plan. So you will need to have procedures to document these requests and set up policies about how you're going to manage them."

Penalties for breaches of personal health information and other HIPAA/HITECH violations are significant, ranging from $50,000 to $1.5 million per violation if judges deem that "willful neglect" was involved. But even "unknowing" violations can cost as much as $25,000 per incident. And this is not including any criminal penalties that might be associated with violations.

Mr. Hinkley said to expect significantly ramped-up enforcement of HIPAA and HITECH beginning in the spring.

So "this is a great time to do a HIPAA compliance tune-up," he added. "Go back and review your electronic health record system [and] all your practice procedures, talk to your vendors, and make sure everything is in compliance." ■

Rhode Island Is Using E-Prescribing Data to Track H1N1

BY MARY ELLEN SCHNEIDER

Public health officials in Rhode Island are using electronic pharmacy data to track the use of oseltamivir and other antiviral medications being used to treat patients infected with the pandemic influenza A(H1N1) virus.

As part of an ongoing partnership with Surescripts, an electronic prescribing network, all 181 pharmacies in Rhode Island now can send and receive electronic prescription information over a secure network. As a result, pharmacies are able to transmit information to the Rhode Island Department of Health on all antiviral prescriptions written in the state. Even if a physician uses a handwritten prescription, the information is available from the pharmacy's electronic system.

At a press conference, Dr. David Gifford, director of the Rhode Island Department of Health, said prescriptions for antiviral medications provide a good proxy measure for infection with H1N1 virus and are a complement to other surveillance systems such as school absenteeism and emergency department visits.

Real-time electronic data on antiviral prescriptions also allow health officials to match supply and demand, he said. If prescriptions are about to outpace the supply, the health department can anticipate shortages in the antiviral supply and release more medication.

Antiviral prescriptions provide a good proxy measure for H1N1 infection, complementing school absenteeism and emergency department visits.

Additionally, if there are reports of a large volume of H1N1 illness in a community, but not a lot of prescribing of antiviral medication, there might be a need for more physician education, Dr. Gifford said. Conversely, if the pharmacy data show a large amount of antiviral prescribing in areas where there is not a lot of H1N1 activity, it could indicate inappropriate prescribing of oseltamivir (Tamiflu) for seasonal influenza, he said.

"This is really a whole new tool in our tool bag," Dr. Gifford said.

The statewide initiative is believed to be the first in the nation and allows pharmacies to send data that have been stripped of personal patient information to the health department on a weekly basis. The prescription data include the patient's age and zip code as well as the prescribing physician's name, allowing health officials to track the progress of the outbreak by communities. ■