



By **KENNETH N. RASHBAUM, JD**

## EHR security: Confluence of law, patient protection, benefit to physicians

**E**lectronic health records (EHRs) are changing the paradigm of medical practice by making increasing volumes of information more central to patient care. Patient data come to you from an ever-widening array of sources—laboratory reports, digital radiology images, email and texts from patients and caregivers, and even social media—and corraling it becomes a daily challenge.

Maintaining this information securely is more difficult than in the paper world due to the volume and mutable nature of electronic patient information: it can be revised, altered, or lost easily. The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and laws of certain states mandate certain protections for EHRs and related information precisely because of the ease with which these data can be accessed or disclosed to unauthorized users, compromising the confidentiality at the heart of the doctor-patient relationship.

Properly addressing EHR security, however, can reassure your patients about taking advantage of the technology, can help you trust the integrity of the information in an EHR, and can enable you to access HITECH incentive payments to assist in the transition to digital medical records. And if you become enmeshed in a lawsuit, an updated and robust security protocol will allow you to have your electronic

evidence comport with the rules of evidence and thereby have it presented to a jury or judge.

### BEYOND HIPAA

Patient confidentiality in an increasingly digitized information environment was the *raison d'être* for the HIPAA privacy rule. The prime motivating factor in the law was the need for workers to obtain health insurance when they changed jobs. HIPAA mandated standardization of claims and condition codes. The concern then arose that, with all this patient-identifiable information traveling around the country electronically, a potential for abuse existed should it end up in unauthorized hands.

The U.S. Department of Health and Human Services (HHS) asked for comments and received thousands of them, many detailing horror stories of banks and employers obtaining medical information without consent. Accordingly, HHS drafted and implemented the HIPAA Privacy Rule and, later, the HIPAA Security Rule.

Information technology has advanced by great leaps since the Security Rule took effect in 2004, but the drafters were prescient. Even though the HITECH Act was required to update the rules to comport with technologic advances, the Security Rule remains the bellwether for you and your colleagues as to your obligations for patient information security.

It is deceptively easy to leave

patient information vulnerable, or to inadvertently disclose or access information improperly, but by the same token, it does not require a great deal of effort to put in place protocols that significantly reduce this risk. In fact, the Security Rule requires physicians and hospitals to have policies and procedures for protection of electronic patient information in storage and transmission, to train the staff on those procedures, and to update those protocols as necessary (for example, to include iPads and text messaging, which did not exist when the Security Rule became effective).

In the early days of HIPAA, caregivers were taught that it was a violation of HIPAA to look at the records of a patient for whom the caregiver had no clinical responsibility. In an EHR, doing so is much easier than in the paper days, when, for instance, a hospital chart had to be requested from the medical records office, and a large number of caregivers have been unable to resist the temptation to peek.

The HHS Office for Civil Rights recently fined the University of California, Los Angeles, Medical Center for a pattern of unauthorized access by physicians and staff to the EHRs of several celebrities. This sort of incident has been repeated at hospitals on the East Coast and elsewhere in the past 4 years, and medical practices are not immune. HHS has stepped up enforcement of HIPAA perhaps, in part, due to the ease with which EHR confidentiality may be compromised. If the patient is not under your care, the rule of thumb dictates, don't look at his or her records.

Another area of governmental scrutiny—and rightly so—is the provi-

sion of the Security Rule that requires encryption of data in storage and in transmission. “In storage” means on computers or portable device hard drives or on servers. This may not be a significant problem for the EHRs of large hospitals, but medical offices and physicians’ home computers are vulnerable to confidentiality breach if the computer media are not encrypted.

Similarly, the rule requires that email containing patient information be encrypted so that it may not be read if misdirected or intercepted. Encryption programs have declined in price considerably, and HHS generally will not hear an excuse that the physician didn’t think to get one.

## PORTABLE MEDIA

Portable media—such as tablet computers, smartphones, laptops, USB (“thumb”) drives—pose greater security risks because many users fail to use even the most rudimentary tools for security: the password. USB drives, which are very easy to lose due to their size, must be password-protected and encrypted. Similarly, tablet computers and laptops must have the capability to store encrypted patient information. Doing so is not difficult: many computers have the capacity for the user to create an encrypted folder, accessible only by a unique password.

Other portable media subject to the rule also can comprise vulnerabilities for patient confidentiality. Recently, the HHS cited Brigham and Women’s Hospital in Boston when a physician took his unencrypted external hard drive, containing identifiable data of

hundreds of patients, with him to Mexico, where he lost it.

## SEVERAL BENEFITS

Beyond the obvious, patient confidence in the security of electronic information will, studies have shown, make them more comfortable with EHRs and more willing to take advantage of the care-enhancing interoperability features. These include coordination of care; communication with physicians by email, which may, in many cases, save the time and expense of office visits; renewal of prescriptions over electronic media; reports of self-tests, such as glucose levels and blood pressure, directly to caregivers; and patient access to their own records, which can enhance their participation in their care.

Also, there is good money in good EHR security. The HITECH Act provides for \$27 billion in incentive payments to assist in the transition to an interoperable EHR. To qualify for this money, qualifying physicians (“eligible professionals”) must meet the criteria in the Meaningful Use Rule. One criterion is the ability to transfer patient information in a HIPAA-compliant manner. The commentary to this rule notes that such compliance must be documented by a HIPAA security risk analysis, which comprises a review of security protocols, updating where necessary, a review of the security aspects of information systems, and training on the updated protocols.

This risk analysis is not solely the province of technologists; it requires legal analysis of the requirements of

the law and the input from the clinicians as to how they use and disclose patient information. It is, in short, an interdisciplinary initiative requiring facilitation of a security team. The reward, in addition to enhanced patient confidence, can be a payment of \$44,000 to \$65,000, depending on the qualifying physician’s Medicare and Medicaid patient population.

The patient’s record often is a doctor’s most important evidence in a malpractice case or other lawsuit. After all, it is a contemporaneous record of what happened, in the caregiver’s own words.

Courts are, at this relatively early stage in EHRs, somewhat leery of electronic evidence, due to the fact that it is easier to alter than paper records. Accordingly, rules of evidence with electronic records are observed more strictly than with paper records, especially hospital charts.

For the electronic record or communication to be admitted into evidence, the proponent must show that it is authentic, reliable, and has been preserved intact. A robust, documented security protocol can be of great assistance in proving that the records have been kept in a secure manner, where no unauthorized person may gain access and, thereby, change the data.

Security protocols for the EHR, then, are a yin and yang. Failure to implement good security policies and practices may result in fines and loss of patient confidence (and, perhaps, loss of patient base if they leave the practice due to a security breach), whereas good security can be a three-pronged “win.”