

HIT Privacy, Security, and Safety Risks: A Legal Perspective

by Kenneth N. Rashbaum, Esq.

Kenneth N. Rashbaum is a partner in the New York office of Sedgwick, Detert, Moran & Arnold, LLP.

“Imagine, if you will” were the words the writer Rod Serling would intone at the beginning of each episode of the classic television series *The Twilight Zone*. What followed would be a tale, with a cautionary bent, a lesson for the future which, as Mr. Serling would clearly imply, was already here.

Such is the case with Health Information Technology (HIT). Even if your hospital or practice is not yet up to cyber-speed, electronic health information is as present as the stethoscope—and so are the risks of inappropriate disclosure, security breaches, and compromises in patient safety.

So let us accept Rod Serling’s invitation and enter the HIT twilight zone. Imagine, if you will:

1. Cap Spaulding¹, a second-year resident in Oncology, having finished an extended shift, throws his dog-eared spiral aid books, and his laptop into his backpack and heads home, only to realize that he failed to complete his charts. He smiles, remembering that his hospital has an electronic medical record (EMR) system, and he can complete his entries remotely. He leaps from the bus, enters a nearby coffee shop, orders a double espresso, fires up his machine, logs onto the record system and begins to type. He reaches for his coffee but his hand stops in mid-air, frozen by the words spoken from six inches behind his right shoulder, “Oh my God! Debbie Jones! I work with her. I didn’t know she had cancer!”
2. Marcia Ballard, Attending in Plastic Surgery, needs to review four extensive charts for the QA review tomorrow. But her daughter’s play is in two hours. She downloads the charts onto a USB thumb drive, so she can complete her review at home. The download is interrupted a few times by error messages, so when the transfer is complete, Dr. Ballard has only 20 minutes to pick up her daughter. She flings the USB drive into her bag, where it lands on top of her sunglass case. When Dr. Ballard throws the bag onto the front seat of her car, the USB drive tumbles onto the street. Two days later, the entertainment section of the local newspaper features an article about the recent facelift of Jennifer Jones, international film star—and a patient whose chart Dr. Ballard had loaded onto her USB.
3. Physician’s assistant, Darren York, is asked by Dr. Michael Field to check the hematocrit on an 85-year-old man who had fallen the previous evening. The patient is responding poorly, and Dr. Field is concerned that there may be a bleed. York assures Dr. Field that the hematocrit has not varied appreciably in the last 12 hours. Suddenly, the patient’s blood pressure drops and he becomes unresponsive. Resuscitation fails and the patient dies. Autopsy reveals a large hemothorax and a perforation

of the thoracic aorta. An audit trail, located during the ensuing QA investigation, shows that York viewed only lab results from the day before the patient’s fall.

Dr. Field, suspecting that the patient may have had a bleed, fires off an angry e-mail to his resident in which he asks the resident to check on another patient because “I don’t trust York. He’s got a history of ignoring labs or even reading the wrong ones.” The e-mail makes its way into the patient’s chart, as per protocol for patient and treatment-related e-mail to automatically be entered into the EMR. The e-mail is disclosed during the discovery phase of the ensuing lawsuit, and the case is settled before trial for far more than its objective value.

HIPAA and Beyond: Regulations and Enforcement

Despite the reports of the demise of HIPAA, it has been ramped up for 2008 due, in no small measure, to the ubiquity of electronic information from technological advances, coupled with news stories of theft or loss of sensitive personal information. In the next six months, hospitals and medical practices in various parts of the United States will be subjected to spot security audits by the U.S. government.²

In its Privacy Rule, HIPAA sets forth the minimum standards for protection of medical information traceable to a particular patient (known as protected health information, or PHI). The HIPAA Security Rule provides specifications for the use, storage, transmission, and disclosure of identifiable medical information in electronic form.³

Required specifications for PHI include:

- implementation of security management processes, including risk analysis, risk management, workplace use and security protocols, and audit controls;
- security incident procedures; and
- sanctions policy for enforcement of those procedures.

“Addressable” specifications, which must be implemented so long as administrative and financial wherewithal is present include encryption of e-mails containing PHI.

The Centers for Medicare and Medicaid Services (CMS) has authority to enforce the HIPAA security rule and, contrary to popular misconception, CMS is quite serious about its enforcement mandate. In December 2006, CMS issued a Security Guidance focusing special attention on remote access to PHI, and security risks in portable media.⁴ CMS stated “there is growing concern” about laptop computers, personal digital assistants

Continued on next page

Continued from previous page

and USB thumb drives. The CMS Guidance also notes that the HIPAA security rule *requires* regular review and modification of information security policies, revision where necessary, and training on those policies. CMS, in the introduction to the Guidance, noted that it “may rely upon this Guidance” in determining whether violations of the security rule have occurred, “and it may be given deference in any administrative hearing” pursuant to the HIPAA enforcement rule.

In 2007, CMS paid an unannounced visit to Piedmont Hospital in Atlanta for a HIPAA Security Audit. Auditors were on site for weeks. Areas of concern included conduct which provided a risk of inappropriate disclosure, loss or theft of electronic PHI storage devices, and lack of attention to security.

While institutions cited in news stories on sub-standard compliance (such as UCLA⁵ and Kaiser Permanente⁶) have not been audited as of this date, the frequency of such data security breaches has not been lost on CMS. It recently announced that it was retaining an accounting firm to assist in security compliance reviews, and that it anticipates at least 10–20 reviews in 2008.⁷

Yet, those who focus only upon the dragon of HIPAA ignore, at their peril, the sharp-toothed gremlins of state laws on data breach prevention and health privacy. Most states now have statutes which require security measures for sensitive personal information and provide for costly, time-consuming, and expensive procedures in the event of loss of data, as recently experienced by a hospital in New York whose patient database backup tape went missing. Additionally, juries look rather severely upon hospitals which fail to comply with patient privacy. An appellate court in New York recently ruled, in the case of *Randi v. Long Island Surgical Center*, that a jury’s award of \$300,000 in punitive damages where the Center *inadvertently* disclosed information about the plaintiff’s abortion to the plaintiff’s mother, was consistent with the facts of that case and appropriate (though the verdict was reversed on other grounds).⁸

While it may go without saying that these matters siphon off scarce financial and personnel resources, the damage to reputation from privacy or security breaches—while more difficult to quantify—is an injury from which recovery can take years and whose costs may be incalculable.

Prepare for Compliance, Not the Audit or the Law Suit

Creating and implementing sound information management practices can considerably reduce the likelihood of an audit (including those triggered by news stories) or a lawsuit. Admittedly, managing EPHI (Electronic Protected Health Information) when creation, transmission, and storage tech-

nology are advancing daily is difficult. Attention to the basics of privacy, security, and confidentiality preservation, though, can form the cornerstone of a workable electronic information management policy.

- First, form a working group to lead the process; include at least one senior officer.
- Next, focus on the risk areas: remote access to EPHI; e-mail risk management (education for avoidance of “smoking gun” e-mails); patient safety issues in access to and use of electronic medical records; employee blogs (if permitted at all) which may reveal enough about “fictional” patients to permit identification.
- Finally, consider an outside individual or entity (e.g., a consulting company experienced in data management and business processes) or a law firm to lead the initiative, in order to lend the project additional gravitas and credibility.

Document the processes and training so that, in the event of inquiry, you have something to which you can refer to show compliance. In the New York case, *Randi v. Long Island Surgical Center*, the court specifically noted, in holding that punitive damages are appropriate for such a privacy breach, the absence of a written privacy policy or any documentation which reflected the existence of the “unwritten code of privacy.”

Neither federal nor state laws require perfection, nor do they mandate a privacy police force. They do require reasonable efforts to provide for information security and protect patient privacy. The steps described above, if documented and implemented, can go a long way toward convincing a HIPAA administrative judge, a state investigative body, or a court that such efforts have been, and are being, conducted. ■

Notes and References

- 1 All names and examples are fictional
- 2 Vijayan J. HIPAA audit at hospital riles health care IT. *Computerworld*. June 15, 2007.
- 3 The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
- 4 HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information; 12/28/2006.
- 5 Steinhauer J. California hospital faces sanctions after workers wrongly looked at patient records. *New York Times*. April 8, 2008
- 6 Lee HK Postings ordered halted: ex-Kaiser worker put links to data on patients on Web. *San Francisco Chronicle*. March 24, 2005
- 7 Ferris N. CMS to check hospitals for HIPAA security compliance. *Government Health IT*. January 17, 2008
- 8 *Randi A. J. v Long Is. Surgi-Ctr.* 2007 NY Slip Op 06953 [46 AD3d 74]