

FEATURE STORY

Scott C. Withrow

healthcare financial management association www.hfma.org

how to avoid a HIPAA horror story

The HITECH Act has expanded the financial risk for hospitals that do not meet the privacy and security requirements under HIPAA.

AT A GLANCE

- > The Health Information Technology for Economic and Clinical Health Act of 2009 significantly expands the financial risk of violations of the Health Insurance Portability and Accountability Act (HIPAA) and extends HIPAA procedures and penalties to business associates.
- > Hospitals, physicians, and their business associates should ensure that HIPAA privacy and security provisions are adopted.
- > Compliance efforts should focus on high-risk areas, including information access management, access control, and impermissible disclosures of protected health information.

Imagine you are the CFO of a regional hospital sitting in your office on a sunny, warm Friday afternoon in late spring, winding up the day and looking forward to the weekend. You then receive a page: "CODE TRIAGE EXTERNAL." You quickly learn a bus carrying a high school girls' soccer team and their supporters to their state tournament game has collided with a beverage truck on a nearby highway, and the bus overturned. Many bus passengers are injured and in transit to your hospital.

You report to the emergency incident commander, who has initiated the well-rehearsed hospital emergency incident command system and is setting up the command center. The communications unit leader contacts off-duty personnel, who hurry to the hospital. Bloodied girls begin flooding into the emergency department (ED), where they are quickly triaged and color-coded. Red-coded patients are rushed into treatment rooms for life-saving care. Yellow-coded patients receive prompt attention to stabilize their conditions. Green-coded patients are escorted to another lobby area within the hospital where ancillary personnel gather patient information, assist with contacting family members, and arrange discharge. Administrative personnel work into the night to track and complete the registration of a total of 30 injured bus passengers.

The emergency management plan works as designed, enabling the hospital to provide excellent health care under extraordinary demands. Miraculously, all passengers survive and recuperate from their injuries. On the following Friday, you watch as the last injured bus passenger is discharged from the hospital. All hospital personnel feel rewarded and proud of their life-saving efforts.

You return to your office to wind up the day and begin looking forward to the weekend. Just as you are ready to leave, the phone rings and you answer. A reporter from the local newspaper wants your comment on a story he intends to run in the Sunday newspaper. The reporter says a list containing the names, addresses, phone numbers, and primary diagnosis of the injured bus passengers treated at your hospital was sent to a local law firm that specializes in personal injury lawsuits, and family members have been receiving calls from the law firm about suing the beverage distributor that owned the truck involved in the accident. An informant has told the reporter the list was sent to the law firm by an ED physician working in the hospital. The reporter thinks disclosure of the list might be a violation of the Health Insurance Portability and Accountability Act (HIPAA). The rewarding feeling vanishes, and you now feel sick to your stomach.

HIPAA Security

HIPAA mandates certain privacy and security protections to encourage the realization of administrative efficiencies through healthcare information technologies. Privacy and security are distinct but related concepts. Privacy refers to obligations of authorized persons using personal health information to keep such information secret. The ED physician working in the hospital is authorized to use personal health information and is obligated to keep the information private. You cannot believe a physician would breach the privacy obligations by sending a list of patients to a plaintiffs' law firm. Security refers to procedures designed to prevent unauthorized persons from accessing personal health information. Maybe the law firm placed a "mole" in the ED who somehow breached the security procedures during the ED chaos resulting from the bus accident to obtain the patient list without authority.

HIPAA security provisions include administrative safeguards (45 C.F.R. §164.308 [2010]), physical safeguards (45 C.F.R. §164.310 [2010]), and technical safeguards (45 C.F.R. §164.312 [2010]). New York University has posted an excellent set of HIPAA security procedures implementing

Rapid technological developments have greatly increased security risks. Anyone holding an iPhone or a similar device in the hospital is well-equipped for spying.

these safeguards at www.nyu.edu/its/policies/#hipaa. The two most commonly violated security provisions, according to enforcement statistics of the Centers for Medicare & Medicaid Services, are information access management (45 C.F.R. §164.308[a][4] [2010]) and access control (45 C.F.R. §164.312[a][1] [2010]). Information access management includes specifications for granting access to electronic protected information through access to a workstation, transaction, program, or process. Access control encompasses specifications for unique user identification, automatic logoff, and encryption of electronic protected information, both in motion and at rest.

Could a law firm mole have improperly gained access to a workstation during the ED chaos, intercepted an unencrypted wireless communication, or hacked into the electronic medical records system provided by an outside vendor? Rapid technological developments have greatly increased security risks. Anyone holding an iPhone or a similar device in the hospital is well-equipped for spying. The HIPAA security officer follows the security incident procedures (45 C.F.R. §164.308[a][6] [2010]) and rules out a breach of security due to improper workstation access or unencrypted communications.

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) extended the HIPAA security provisions and penalties beyond covered entities (such as hospitals and physicians) to include all business associates (such as electronic medical record vendors and IT services) (see HITECH §13401, codified at 42 U.S.C. §17931 [2010]). The HIPAA security

officer asks the hospital's electronic medical record vendor to follow the security incident procedures to rule out the possibility of outside hacking. The vendor reports back with computer logs ruling out hacking. You begin to think the incident is in fact a privacy breach by an authorized person rather than a security breach by an unauthorized person.

HIPAA Privacy

HITECH also extended the HIPAA privacy and penalty provisions to business associates (HITECH §13404, codified at 42 U.S.C. §17934 [2010]). Tulane University has posted an excellent set of privacy procedures at tulane.edu/counsel/upco/privacy-policies.cfm. The two most commonly violated privacy provisions, according to the Department of Health and Human Services (HHS) Office of Civil Rights enforcement highlights, are impermissible uses and disclosures of protected health information (45 C.F.R. §164.504[e][4] [2010]) and lack of appropriate administrative, technical, and physical safeguards of protected health information (45 C.F.R. §164.530[c][1] [2010]). HIPAA regulations do not prescribe the particular privacy safeguards that covered entities and now business associates must implement, because the nature of the safeguards will vary with the size of the entity and the type of activities that the entity undertakes. Examples of appropriate safeguards include requiring that the entity shred documents containing protected health information prior to disposal, keep doors to medical records departments (or to file cabinets housing such records) locked, and limit which personnel are authorized to have the key or pass-code.

After interviewing the various physicians and nurses who were present in the ED during the bus emergency, you identify two prime suspects for the privacy breach. One suspect is an ED physician who is employed by an ED physician contracting company and provided to the hospital under a business associate arrangement. In his spare time, the suspect physician has provided expert testimony in lawsuits on behalf of clients of the personal injury law firm that received the list of injured bus passengers. The second suspect

is an operating room nurse employed by the hospital who volunteered to help in the ED the afternoon of the bus accident. The nurse's husband is out of work due to a disability resulting from a slip and fall in the local supermarket, and the personal injury law firm that received the list of bus passengers is representing the husband in a lawsuit against the supermarket.

HIPAA Criminal Penalties

A person who knowingly discloses individually identifiable health information to another person commits a crime punishable by fines up to \$50,000 and imprisonment up to one year, or both (42 U.S.C. §1320d-6[b][1] [2010]). The criminal penalties jump to fines up to \$250,000 and imprisonment up to 10 years, or both, if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm (42 U.S.C. §1320d-6[b][3] [2010]).

HITECH clarified that, for purposes of this crime, a person (including an employee or other individual) shall be considered to have illegally disclosed individually identifiable health information if the information is maintained by a covered entity (such as a hospital) and the individual disclosed such information without authority (HITECH §13410[a], codified at 42 U.S.C. §1320d-6[a][3] [2010]). If either the suspect physician or nurse knowingly disclosed the list of injured bus passengers to the personal injury law firm for personal gain, the person would face up to 10 years in prison, longer than the maximum sentence for an armed bank robber (2009 Federal Sentencing Guidelines Manual §2B3.1 [first offense]).

HIPAA Civil Monetary Penalties

HITECH significantly increased the civil monetary penalties for HIPAA violations. Prior to HITECH, a HIPAA violation was like a speeding ticket. The general penalty for a HIPAA violation was \$100 per violation, and the total amount of fines for all such violations of an identical requirement or prohibition during a calendar

FEATURE STORY

year could not exceed \$25,000. Furthermore, fines could not be imposed if the person did not know, and by exercising reasonable diligence would not have known, that such person violated the provision.

HITECH established categories of violations that reflect increasing levels of culpability, requiring that a penalty determination be based on the nature and extent of the harm resulting from the violations. HITECH significantly increased financial risk of HIPAA violations in two respects: The penalty per violation of \$50,000 for uncorrected willful violations is 500 times greater than the prior \$100 “speeding ticket,” and the calendar year maximum jumped 60-fold to \$1.5 million. HITECH also eliminated the affirmative defense for violations in which the covered entity did not know, or by reasonable diligence would not have known, of the violation, and such violations are now punishable under the first tier of penalties.

If the privacy violations for the 30 bus passengers are considered willful and not corrected, the offending party could hit the calendar year maximum of \$1.5 million ($\$50,000 \times 30 = \$1,500,000$) in a single incident. Even unknowing violations can add up if a large number of patients are affected. HITECH applies these fines not only to the hospital, but also to business associates of the hospital, such as the ED physician contracting company if it is found to be the offending party.

This increased financial exposure means both hospitals and their business associates should place greater emphasis on HIPAA compliance.

Improved Enforcement

HITECH provides significant new incentives to improve enforcement of HIPAA. Congress ordered the secretary of HHS to establish by Feb. 17, 2012, a new methodology under which an individual harmed by a HIPAA offense may receive a percentage of the civil monetary penalty or monetary settlement collected with respect to such offense (HITECH §13410, codified at 42 U.S.C. §17939[c] [2010]). Although there remains no private right of action for HIPAA violations, the new methodology will provide monetary incentives for harmed individuals to complain to federal regulators in the hope of sharing in the penalties. HITECH also requires the secretary of HHS to provide for periodic audits to ensure that covered entities and business associates comply with HIPAA (HITECH §13411, codified at 42 U.S.C. §17940 [2010]). These enforcement provisions will change the healthcare industry’s previously nonchalant approach to HIPAA compliance.

The investigation of the disclosed list of bus passengers continues. The personal injury law firm cooperates in the investigation, and produces evidence that the ED physician did in fact send the list of bus passengers to a paralegal at the law firm. The ED physician contracting company

HITECH ENHANCED HIPAA PENALTIES

HIPAA Violation Category	Each Violation	Minimum—30 Violations	Maximum—All Violations
Did not know (and by exercising reasonable diligence would not have known)	\$100-\$50,000	\$3,000	\$1,500,000
Reasonable cause	\$1,000-\$50,000	\$30,000	\$1,500,000
Willful neglect—Corrected within 30 days	\$10,000-\$50,000	\$300,000	\$1,500,000
Willful neglect—Not corrected	\$50,000	\$1,500,000	\$1,500,000

Source: 74 Fed. Reg. 56123 (Oct. 30, 2009) amending 45 C.F.R. Section 160.404(b).

EXAMPLE OF BREACH NOTIFICATION

HIPAA HOSPITAL
100 Main Street
Town, State 99901

July 9, 2010

[NAME OF AFFECTED INDIVIDUAL]
[ADDRESS]

Re: HIPAA Notification

Dear _____

On May 14, 2010, a bus carrying a high school girls' soccer team and their supporters to their state tournament game collided with a beverage truck on a nearby highway, and the bus overturned. Many injured bus passengers were treated at HIPAA Hospital.

On May 21, 2010, we discovered that certain unsecured protected health information relating to the injured bus passengers was sent to a local law firm that specializes in personal injury lawsuits. The types of information that were involved in the breach were names, addresses, phone numbers, and primary diagnosis of the injured bus passengers.

We immediately commenced an investigation, contacted the law firm in question, and instructed the law firm to cease making calls to family members of the injured passengers or otherwise using the protected health information. The law firm complied with our demands and cooperated with our investigation. We have not received any other reports of misused information and we know of no other steps you would need to take to protect yourself from potential harm from the unauthorized disclosure.

Our investigation determined that an emergency department physician provided to HIPAA Hospital by ACME Physician Contracting Company was solely responsible for the unauthorized disclosure. The offending physician has been terminated by ACME and is subject to criminal investigation for his actions. We continue to work with law enforcement investigating this breach of protected health information.

Protecting the privacy of our patients is extremely important to us. HIPAA Hospital has modified its privacy and security procedures to further restrict access to protected health information and enhanced privacy training to protect against further breaches.

HIPAA Hospital sincerely apologizes for the inconvenience or concern this incident has caused our patients and their families. If you have any questions or would like additional information, please contact Mr. John Doe, Chief Privacy Officer, HIPAA Hospital, via e-mail at JohnDoe@HIPAAHospital.org or call toll-free (800) 555-1234.

A HIPAA horror story can be avoided by following sound HIPAA compliance procedures that will mitigate culpability and reduce any potential civil monetary penalties.

terminates the employment of the physician and assures the hospital that it will indemnify the hospital for damages suffered by the hospital as a result of the incident. The HIPAA financial risk appears to be under control, yet the hospital still faces a major public relations problem.

Breach Notification

HITECH requires HIPAA covered entities to notify affected individuals within 60 days following the discovery of a breach of unsecured protected health information (HITECH §13402, codified at 42 U.S.C. §17932 [2010]). Covered entities also must notify the secretary of HHS in all cases (45 C.F.R. §164.408 [2010]), and must notify the media if the breach of protected health information involves more than 500 residents of a state or jurisdiction (45 C.F.R. §164.406 [2010]). In the case of a breach of unsecured protected health information by a business associate of a covered entity (such as the ED physician contracting company), the business associate must notify the covered entity of the breach (45 C.F.R. §164.410 [2010]).

Breach notification is not required for all violations of HIPAA privacy and security protections, just those violations resulting in the unauthorized acquisition, access, use, or disclosure of protected health information. For example, breach notification of the failure to keep medical records cabinets locked or the failure to encrypt wireless

transmissions is required only if such failure actually results in the unauthorized use of protected health information. HITECH and the implementing regulations also adopt three exceptions to the definition of *breach* for certain harmless uses or disclosures (45 C.F.R. §164.402 [2010]). The first exception is unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if it is made in good faith and within the scope of authority and does not result in further unauthorized use or disclosure. The second exception is any inadvertent disclosure by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same entity and does not result in further unauthorized use or disclosure. The third exception is a disclosure where the covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information, such as mail returned unopened.

The breach notification must be written in plain language and include:

- > A brief description of what happened, including the date of the breach and date of discovery, if known
- > A description of the types of unsecured protected health information that were involved in the breach
- > Any steps individuals should take to protect themselves from potential harm resulting from the breach
- > A brief description of what the covered entity is doing to investigate the breach, mitigate the harm to individuals, and protect against further breaches
- > Contact procedures for individuals to ask questions or learn additional information

You are concerned about sending the breach notification to the affected individuals within 60 days, and coordinating public relations efforts with the local newspaper. The hospital, not the

ED physician contracting company, is responsible for ensuring the breach notification is sent to the affected individuals. Although it may be possible to delegate this responsibility to the business associate in some circumstances, you determine that the hospital should take charge of the notification process in this situation. The sidebar on page V illustrates a sample notification letter.

Follow Sound HIPAA Compliance Procedures

HITECH significantly expands the financial risk of HIPAA violations and extends HIPAA procedures and penalties to business associates. Hospitals, physicians, and their business associates should ensure that HIPAA privacy and security provisions are adopted and up-to-date. Compliance efforts should focus on high-risk areas, including information access management, access control, and impermissible disclosures of protected health information.

Business associate agreements should be revisited to verify that business associates accept the direct HIPAA obligations and indemnify the hospital and physicians for any HIPAA breaches. Covered entities and business associates must provide HIPAA training and appropriate monitoring to confirm continuing compliance. A HIPAA horror story can be avoided by following sound HIPAA compliance procedures that will mitigate culpability and reduce any potential civil monetary penalties. ●

About the author



Scott C. Withrow, Esq., is a founding partner, Withrow, McQuade & Olsen, LLP, Atlanta (swithrow@wmolaw.com).