It's 2 AM: Do You Know Where Your Patients' Information Is?

D. Brent Wills, Esquire
Gilpin Givhan PC
Montgomery, AL

On September 17, 2012, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced that it had entered into a resolution agreement (i.e., settlement) with Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates (collectively, MEEI) which required MEEI to pay $1.5 million to OCR and enter into a three-year corrective action plan with the agency. The agreement related to the theft of a laptop belonging to an MEEI-affiliated physician while the physician was lecturing in South Korea in 2010. Although the laptop included certain data security features, it was not encrypted. The laptop reportedly held protected health information (PHI) for more than 3,600 of MEEI's patients.

Unfortunately, the MEEI breach involves facts that are becoming all too familiar as hospitals and other "covered entities" struggle to maintain the privacy and security of their patients' personal information, as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] For example, the following are among the largest hospital breaches so far in 2012:

- Emory University Hospital in Atlanta, GA, misplaced ten unencrypted backup computer disks containing PHI for more than 300,000 individuals. The disks contained old data from software the hospital deactivated years ago. Although the disks were stored in an office that was locked at night, they went missing from an unlocked storage cabinet.
- At Howard University Hospital in Washington, DC, an employee of a business associate of the hospital downloaded patients' PHI to a personal laptop computer, in violation of the hospital's data security policies. The laptop was subsequently stolen from the employee's vehicle. Even though the laptop was password protected, it was not encrypted. The laptop contained PHI for more than 34,000 individuals.
- Memorial Healthcare System in Hollywood, FL, discovered that two employees had stolen PHI for nearly 10,000 patients with the intent to use it to file fraudulent tax returns.

Like MEEI, all three hospitals reported the incidents to OCR pursuant to requirements in the Health Information Technology for Economic and Clinical Health Act (HITECH), part of the 2009 federal stimulus legislation.[2] All three now appear on OCR's website listing of "major" breaches that affect 500 or more individuals (the so-called Wall of Shame). Undoubtedly, all three hospitals have already suffered considerable economic and noneconomic losses in dealing with their respective breaches. Moreover, OCR presumably will investigate each of the breaches, and, if the MEEI breach is an indicator, one or more of the hospitals may be subject to significant civil monetary penalties (CMPs) to boot.

Why Should Hospitals be Worried?

Data breaches are occurring at an alarming rate in all industries, but particularly in the financial sector and in healthcare. OCR data indicates that since September 2009, when the HITECH breach notification requirement became effective, the agency has received nearly 60,000 notifications[3]—that is, 60,000 breaches reported in roughly 1,000 days. Frighteningly, the number of breaches reported during 2011 increased nearly one-third from 2010.[4] In addition, the author recently learned from an OCR spokesperson that, during 2012, a particular regional office of OCR is receiving an average of four major breach notifications per month.

The potential costs and legal risks associated with data breaches are substantial. Any breach that occurred on or after February 18, 2009, is subject to the CMP scheme established by HITECH.[5] Whereas maximum CMPs for HIPAA violations were previously capped at $25,000, HITECH authorized penalties up to $1.5 million per violation.[6] Not surprisingly, OCR has been quick to flex its HITECH enforcement muscle to negotiate a number of resolution agreements that have often entailed substantial resolution payments; for example, in addition to the $1.5 million payment from MEEI, OCR has received resolution payments this year in the amounts of $1.7 million and $1.5 million, respectively, from the Alaska Department of Health and Social Services (Alaska DHSS) and Blue Cross Blue Shield of Tennessee (BCBSTN). Significantly, these three resolution agreements represent the first publicized enforcement actions taken by OCR against covered entities that reported data breaches pursuant to HITECH's requirements (i.e., self-reported potential HIPAA violations). HITECH also authorizes state attorneys general (AGs) to pursue CMPs with respect to data breaches and other HIPAA violations that affect their constituents.[7] Several AGs have seized upon this power, including Massachusetts

AG Martha Coakley, who earlier this year entered into a $750,000 settlement with a Boston hospital to resolve federal HIPAA and state law claims relating to a 2010 data breach. It is noteworthy that there was no showing, in any of these cases, that PHI was inappropriately accessed or misused.

Even if no penalties or settlement payments result, however, data breaches may still be very costly. For example, in the wake of a breach, a hospital may need to engage legal counsel, information technology consultants to assist with internal investigations and corrective actions, and a public relations firm to help notify the individuals affected by the breach (and, in some cases, the media) and to help with damage control for the hospital's public image. The hospital may also incur significant costs to correct any security problems that contributed to the breach (e.g., updating or upgrading technology, policies and procedures, or physical safeguards). Consider, also, that OCR investigates every major breach notification it receives. The cost of dealing with an investigation—again, even where no penalties result—may be substantial. As an example, reports indicate that, whereas BCBSTN ultimately paid $1.5 million to OCR pursuant to its resolution agreement, it spent nearly $17 million to conduct an internal investigation, implement corrective actions, notify the affected individuals, and deal with OCR.[8] Ironically, BCBSTN may have gotten off light: studies have determined that data breaches—especially those that entail media notifications and government investigations—may cost hospitals as much as $500 per affected individual.[9] None of this accounts, of course, for lost time and productivity, or for other, indirect economic harm a breach may cause to a hospital's brand and reputation.

What's more, while cyber espionage gets headlines, OCR statistics show that a substantial majority of breaches result from simple breakdowns in everyday privacy and security practices. Specifically, breaches most frequently result from theft or loss, inadequate safeguards, or improper disposal of PHI, and they most frequently involve PHI in paper format or electronic PHI stored on unencrypted portable electronic devices, such as laptop computers, flash drives, and smart phones. The MEEI, Alaska DHSS, and BCBSTN breaches, for example, all resulted from theft of unencrypted portable devices. Indeed, in its enforcement actions against MEEI and Alaska DHSS, OCR put portable devices front and center, identifying various alleged deficiencies and calling for a number of corrective actions specifically targeting such devices.[10] By comparison, only a very small percentage of breaches reported to OCR have involved computer hackers. This is not to say, of course, that hackers are not a threat to a hospital's e-PHI; on the contrary, they are a major threat. What it does say is that the data breach problem is far more than just "an IT issue."

Other studies have determined that more than 80% of physicians (and presumably most clinical and administrative staff, as well) use smart phones or other portable electronic devices in their work. This, in and of itself, should not be surprising. But consider that the majority of those devices are not encrypted or lack necessary data security safeguards. As the MEEI, Alaska DHSS, and countless other breaches exemplify, any physician or medical staff member, any management personnel, or any other hospital workforce member walking around with an unencrypted laptop, smart phone, or jump drive that contains patients' PHI may be a breach waiting to happen. Worse, other studies have suggested that the street value of a medical identity may be up to fifty times greater than the value of a Social Security number. Criminals are wise to this. A significant market has developed for stolen PHI; as illustrated earlier, a common tactic is to use stolen patient information to file fraudulent tax returns.

Perhaps it is not surprising, then, that, more often than not, data breaches are caused by insiders. This means that someone in a hospital's workforce, or in the workforce of the hospital's business associate, either does not have a proper understanding of his or her responsibilities in regard to PHI or, more and more frequently, has intentionally violated those responsibilities. Again, the illustrations at the beginning of the article reflect classic cases: in one case, a contractor failed to follow the hospital's policy; in the other, a hospital employee simply stole patients' PHI.

In sum, data breaches are happening to everyone, everywhere. Not even the healthcare elite are excluded. MEEI, for example, is the primary ophthalmology and otolaryngology teaching hospital for Harvard Medical School, and it has experienced large breaches both before and since the breach that led to its resolution agreement with OCR. Likewise, in addition to the Emory University Hospital breach referenced above, Stanford University Hospital has experienced multiple large breaches during the last two years, including a breach last year that impacted nearly 20,000 emergency room patients. Similarly, both the UCLA Health System and the M.D. Anderson Cancer Center have reported or experienced multiple large breaches, the latter on three separate occasions in 2012 alone. All these breaches involved either theft or loss of an unencrypted portable electronic device or inappropriate access, use, or disclosure of PHI by a member of the hospital's workforce or a business associate.

What Comes Next?

With the advent of telemedicine, cloud computing, and mobile health, among other advances, the healthcare industry is constantly turning out new and improved technologies. New technologies, however, mean new challenges for hospitals and other covered entities in regard to information privacy and security. From OCR's perspective, each new challenge presents a new opportunity for enforcement.

In addition, OCR, pursuant to a Congressional mandate in HITECH, recently commenced its first-ever HIPAA compliance audits. OCR entered an agreement last year with KPMG to develop an audit protocol and conduct an initial "pilot" round of 115 compliance audits expected to be completed by the end of 2012.[11] OCR recently published the HIPAA audit protocol, but it has not published any specific audit results. Further, the future of the audit program remains unclear; OCR's contract with KPMG only covers the initial round of audits. OCR has indicated informally that compliance audits will continue beyond 2012, but it has not addressed, for example, whether, when, or to what extent there will be an expanded rollout of the program. Whatever the

future of the HIPAA audits, however, the program is only one piece in a larger enforcement trend.

It is also expected that OCR will soon publish its long-awaited "omnibus" final HITECH regulation (HITECH Final Rule) that will finalize and implement many of the Act's provisions. Among other things, the HITECH Final Rule will finalize and implement important changes to the HIPAA privacy rule, including expansions to individuals' rights to access their own PHI, new restrictions on certain uses and disclosures of PHI that involve financial remuneration, new requirements relating to the use of PHI in connection with fundraising, and important changes to business associate agreements and notices of privacy practices. All these new compliance obligations, again, represent new enforcement opportunities for OCR. Hospitals and other covered entities must be in compliance with most of the requirements of the HITECH Final Rule within 240 days after the rule is published.[12]

Finally, class action lawsuits are gathering steam. Stanford Hospital and its business associate, Multi-Specialty Collection Services, for example, are facing a $20 million class action suit in regard to the 2011 data breach mentioned above. Likewise, Emory Hospital is facing a $200 million class action suit involving more than 200,000 plaintiffs in regard to its breach reported earlier this year. Moreover, although HIPAA does not provide for individual causes of action, HITECH directed OCR to develop procedures whereby individuals who notify OCR about violations (i.e., whistleblowers) may receive a percentage of any penalties or other amounts the government ultimately recovers.[13] OCR missed its February 2012 target date to promulgate regulations to implement the whistleblower mandate, but there is nothing to indicate that OCR will not move forward with this initiative.

What Should Hospitals Do?

The discussion above indicates, loud and clear, that the government has taken on a distinctly enforcement-oriented mindset in regard to HIPAA. Given the very high likelihood that most or all hospitals will experience a data breach, combined with the potential for future compliance audits, and potentially even whistleblower and class action lawsuits, it behooves hospital management to take on an enforcement-oriented mindset as well—i.e., "Not if, but when."

In preparing to deal with OCR, a hospital's primary objective should be to demonstrate that violations, if any, resulted from reasonable cause, and not willful neglect. Under the HITECH penalty scheme, this could be the difference between a $1,000 per-violation penalty, or no penalty at all,[14] and a *minimum* $50,000 per-violation penalty, up to an aggregate maximum of $1.5 million per violation. In this regard, OCR guidance indicates that putting policies and procedures and other basic safeguards in place and demonstrating a good-faith effort to comply are indicators of reasonable cause, whereas failure to put such safeguards in place is an indicator of willful neglect.[15] This is consistent with OCR's resolution agreements to date; these have focused heavily on covered entities' failure to implement very basic protections, particularly security risk analysis, compliance programs and policies and procedures, workforce training and accountability practices, physical safeguards, and audit and monitoring mechanisms. Also, as mentioned above, recent enforcement activity suggests that OCR is zeroing in on information safeguards on portable electronic devices.

Moreover, at least in general, OCR appears to be interested as much in a covered entity's overall HIPAA compliance process as it is in particular breaches and deficiencies. Hospital management must take the initiative to conduct a security risk analysis to identify the particular security risks and vulnerabilities associated with its patients' PHI and develop reasonable and appropriate safeguards to address those risks and vulnerabilities. The hospital must also regularly update its security risk analysis and evaluate whether its existing safeguards are effectively protecting its patients' PHI; if not, the hospital must promptly take corrective action. In addition, each step in the process must be consistent with the others. A top notch compliance program and set of policies and procedures is not worth much—from OCR's perspective—to a hospital that does not train its workforce or hold them accountable for noncompliance. The process must also be constantly adapting to reflect changes in the hospital's workforce and operations, changes in laws and technology, and security risks and vulnerabilities identified by the hospital. Finally and perhaps most importantly, hospital management must thoroughly document the steps the hospital takes to follow its compliance program and policies and procedures. In an enforcement battle with OCR, thorough documentation of compliance may be a hospital's most valuable weapon.

In addition, as part of a hospital's HIPAA compliance process, management must thoroughly vet the hospital's information technology vendors and other business associates. Management should closely examine a prospective vendor's privacy and security practices, for example, and confirm that the vendor does not appear on the Wall of Shame. Management should also ensure that the hospital's vendor and business associate agreements include rights to indemnification and other protections sufficient to compensate the hospital in the event of a data breach or other information security incident.

A hospital's compliance process must also address encryption. While technically not required by HIPAA, OCR has clearly indicated a strong preference for encrypting e-PHI on multiple fronts. In its resolution agreement with MEEI, for example, OCR

emphasized MEEI's failure to address whether, in its particular circumstances, encryption was a reasonable and appropriate e-PHI safeguard. In addition, OCR exempts e-PHI encrypted pursuant to standards established under HITECH from the Act's breach notification requirements.

Finally, hospitals should be aware that HIPAA and HITECH provide an affirmative defense against CMPs for covered entities that correct potential violations within thirty days, absent evidence of willful neglect.[16] Thus, a hospital's HIPAA compliance program and policies and procedures, and its overall HIPAA compliance process, should require the hospital to take steps to correct any breach of PHI or other potential HIPAA violation within thirty days, or as soon as reasonably practicable.

1 42 USC § 1320d-5 and -6; *see also* 45 CFR Part 160 and Part 164, Subparts, A, C, D, and E.

2 *See* Division A, Title XIII and Division B, Title IV, American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, at § 13402 (HITECH).

3 *See* David Holtzman, OCR, Breach Notification for HIPAA Covered Entities and Business Associates, *available at* http:/csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-4_dholtzman_ocr-hitech-breach-notifcation-rule.pdf.

4 *See* Brian T. Horowitz, *Health Care Data Breaches Increase by 32 Percent: Ponemon Report*, Health Care IT News (December 1, 2011), *available at* www.forbes.com/sites/andygreenberg/2010/11/08/data-spills-cost-u-s-hospitals-6-billion-a-year/?boxes=Homepagechannels.

5 *See* HITECH, at § 13410(d)(2), *codified at* 42 USC § 1320d-5(a)(3).

6 *See Id.*

7 *See* HITECH, at § 13410(e)(1), *codified at* 42 USC § 1320d-5(e).

8 Press Release, Blue Cross, HHS Reach Settlement in 2009 Hard Drive Data Theft (Mar. 13, 2012), *available at* www.bcbst.com/about/news/releases/default.asp?release=426.

9 *See* Andy Greenberg, *Data Spills Cost U.S. Hospitals $6 Billion A Year*, Forbes (Nov. 8, 2010), *available at* www.forbes.com/sites/andygreenberg/2010/11/08/data-spills-cost-u-s-hospitals-6-billion-a-year/?boxes=Homepagechannels (reporting on 2010 study published by Ponemon Institute).

10 *See* Resolution Agreement by and between OCR and MEEI dated September 13, 2012, at 1-2, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf and Resolution Agreement by and between OCR and Alaska DHSS dated June 25, 2012, at 6, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.pdf.

11 *See* Audit Pilot Program, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html.

12 *See* HITECH, at § 13405.

13 *See* HITECH, at § 13410(b)(2).

14 OCR retains discretion to waive penalties due to reasonable cause and not willful neglect. *See* 42 CFR § 160.412; *see also* Enforcement IFR, 74 Fed. Reg. at 56129. Penalties are mandatory, however, for violations that involve willful neglect. *See* 42 CFR § 160.404(b)(2)(iv).

15 *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40868, 40879 (July 14, 2010).

16 *See* 45 CFR § 160.410(a)(3).