Report on
PATIENT PRIVACY

Volume 14, Number 8 • August 2014

Practical News and Strategies for Complying With HIPAA

Contents

R.I. Hospital Settles With Massachusetts For $150,000 but Faces an OCR Inquiry

It sounds like something out of a 60s-era rock song. But the alleged failure of a Rhode Island medical center to keep track of more than a dozen computer back-up tapes during a "hospital-wide media destruction" has cost it a penalty of $150,000 and resulted in a corrective action plan that requires, among other things, that it hire a private firm to audit how well it is complying with HIPAA.

And that's just what's mandatory under the agreement Womens and Infants Hospital (WIH) made with Massachusetts to settle a suit brought by Martha Coakley, the attorney general (AG) for the commonwealth.

A spokeswoman for WIH tells *RPP* it is still being investigated and thus may face possible sanctions by the HHS Office for Civil Rights (OCR). *And here's the kicker:* there's no evidence the tapes, which contained ultrasounds dating as far back as 1993 that disappeared in either 2011 or 2012, ever fell into the wrong hands and were misused.

Coakley is among the very few AGs who've flexed the muscle granted to them under the HITECH Act to bring state enforcement powers to bear when there is a violation of HIPAA, the federal law protecting the privacy and security of patient information.

The terms to which WIH is subject could easily be applied to any other CE that has patients residing in Massachusetts. The settlement also provides a case study of how a CE can face sanctions through a web of overlapping state laws, with HIPAA requirements layered on top. In many respects, the settlement is far more detailed than OCR's corrective action plans.

Coakley filed suit against WIH in Superior Court in Suffolk County, Mass., on July 22, alleging violations of the Massachusetts Consumer Protection Act and the Security

continued on p. 9

After Hopkins Case, CEs Should Review Photo Policies, Mitigate Any Patient Fears

At UMC Health System, the public system in Lubbock, Texas, that serves as the primary teaching hospital for Texas Tech University Health Sciences Center, cameras are a vital and routine presence in patient care. They help document the progress of patients recovering at its burn center and its level I trauma center.

Special cameras owned by UMC are used that automatically erase stored images once they are uploaded to UMC's medical record, and in certain cases, only nurses credentialed under state regulations may take photographs. Acceding to the needs of its physicians, UMC recently implemented a new program that allows physicians to receive patient photos via text message in a HIPAA-compliant fashion.

But even with so much careful thought as to safeguards, Deborah Dabbs, UMC's compliance coordinator whose responsibilities include the privacy rule and breach investigations, worries about the impact of a multimillion-dollar settlement that has been in national headlines recently between Johns Hopkins Hospital and Healthcare, Inc., and thousands of patients secretly recorded by one of its physicians.

continued

"I think people definitely will be concerned, and every time we pick up a camera now the patient is going to have questions," Dabbs tells *RPP*, adding that she intends for the case to be discussed at a high-level UMC system meeting that brings together legal, privacy, security and corporate health system officials.

Other privacy experts tell *RPP* HIPAA covered entities (CEs) that rely on videos and photos for medical records, teaching, research and other uses should take the time to allay any patient concerns while ensuring they are doing the utmost to preserve their privacy.

In addition to providing notice and obtaining consents, "CEs may wish to consider public relations campaigns proactively describing the limited ways in which they use recording devices, sharing contact information for appropriate staff members who can field questions about such practices, and contact information for filing complaints," says David Harlow, principal with the Harlow Group LLC.

The Hopkins settlement made national news when it was announced July 22, described as "one of the largest settlements on record in the U.S. involving sexual misconduct by a physician." Brought on behalf of 8,000 women, the class action contended Dr. Nikita Levy violated patient privacy and "improperly photographed and/or videotaped his patients without consent or authorization, and stored those images electronically."

The actions of Levy, who committed suicide after being confronted with the allegations and terminated by Hopkins, may or may not put Hopkins on the radar of the HHS Office for Civil Rights. As the suit was making the news, OCR leadership has been in flux (see p. 5).

For OCR, among the factors to be weighed are whether any patients were identifiable. However, the government could decide to bring an action if a CE was found to violate other privacy and security requirements uncovered during an OCR investigation that may have been precipitated by an unrelated complaint.

Dabbs and other HIPAA officials tell *RPP* they believe OCR must make a public statement about whether it is pursuing potential HIPAA violations in this case. Thus far OCR has declined to do so.

CEs can also face potential actions by the state attorney general (AG) in Maryland, as permitted under the HITECH Act. While few state AGs have been active in this regard, Massachusetts AG Martha Coakley last month inked a $150,000 settlement with a hospital that lost track of prenatal images for more than 14,000 patients (see story, p. 1).

Photos Play an Important Role

Harlow tells *RPP* that, in general, "while the need for recordings is limited," the "legitimate uses" of photography "might include tracking progress of a skin lesion over time, healing post-surgery, documenting curvature of the spine, a patient's gait…a million different things."

UMC's burn unit and trauma center count among its 450 beds; it also includes a children's hospital. Dabbs tells *RRC* cameras play an integral and routine part in documenting wounds, pressure ulcers and burns suffered by patients. They are also used for patients being treated for sexual abuse, with those photos taken only by staff credentialed through the state's sexual assault nurse examiner (SANE) program, she says.

"All of those have to be taken by hospital-owned cameras," she says, adding that the cameras are kept securely in nursing stations and other locations around the hospital, including in the trauma center and surgical intensive care units. The emergency room has a special camera that only certain staff are permitted to use.

UMC's medical records system is not yet fully electronic — Dabbs calls it a "hybrid" that still exists on paper as well.

UMC has banned the use of cell phones by employees — a group that does not include physicians — in its Emergency Center. There's just too much temptation to

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com.

Editors, Theresa Defino, Francie Fernald; Executive Editor, Jill Brown; Associate Editor, BJ Taylor; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Tracey Filar Atwood; Production Director, Andrea Gudeon

Subscriptions to *RPP* include free electronic delivery in addition to the print copy, e-Alerts when timely news breaks, and extensive subscriber-only services at www.AISHealth.com that include a searchable database of *RPP* content and archives of past issues.

To order an annual subscription to **Report on Patient Privacy** ($524 bill me; $494 prepaid), call 800-521-4323 (major credit cards accepted) or order online at www.AISHealth.com.

Subscribers to *RPP* can receive 12 Continuing Education Credits per year, toward certification by the Compliance Certification Board. Contact CCB at 888-580-8373.

use the phones, as well as their cameras, especially when patients with "cool" injuries arrive.

Cell phones are allowed elsewhere on UMC's grounds, but no workers, with advanced degrees or otherwise, are permitted to use their phones to take pictures of patients, even if they are not identifiable.

Secure Text Messaging Can Be Used

In fact, it was the need for medical staff and physicians to share their visual impressions of patients' symptoms or injuries that led UMC to implement a secure text messaging application called Cortext, by Imprivata Inc.

Staff can text physicians, and *vice versa*, via UMC's main frame computer, to personal cell phones, laptops, and tablets, says Dabbs. This program was implemented this year and has been working well so far. Its uses are limited, however. For example, it cannot be used by physicians to issue an order and the photos never make it into the medical record, Dabbs adds.

Dabbs says she was aware of the Hopkins physician's actions when they became public, and she read about the settlement, which was also roundly shared among privacy and HIPAA groups on LinkedIn in addition to being highlighted in many media outlets.

Such a case can do great damage to patients' level of trust, says Dabbs, who feels strongly that employees must appreciate the deep trust patients place in them, something she tries to drill home whenever possible. "Trust is one of the issues that I always talk about when I do orientation," she says.

"We know more about that patient than almost anybody else, and we often know it first," Dabbs adds as she recalls her days working at a lab.

If a CE wants to take a photograph or video for marketing, fundraising or other related purposes, a HIPAA authorization is required. These activities fall outside of an exception for treatment, payment and health care operations and also wouldn't fit within standard patient consent procedures.

NPPs Should Mention Photography

Rob Tennant, senior policy advisor for the Medical Group Management Association, says CEs should review their notices of privacy practices (NPPs) to ensure photography is mentioned, especially in light of the Hopkins case, which he called "extreme but very important," especially because news of it is so widespread.

Of course, as appropriate, there will also be a need for obtaining patient consent, he adds. CEs shouldn't just "bury" the issue in the NPP, but when appropriate, begin a dialogue with the patient, explaining, "This is what we do and why we do it," says Tennant.

Harlow agrees, and he recommends that "given the current increased general awareness of and sensitivity to privacy issues, CEs should consider reviewing current policies and implementations of policies regarding recording devices."

Harlow provided a few guidelines for handling photography.

◆ ***Ensure consent is appropriately received.*** For example, "obtaining informed consent for use of photography or other recording devices should be standard in both the research and treatment contexts. In the research context, institutional review board approval should be required in advance as well. Policies should mandate the documentation of informed consent before any recording may be made."

◆ ***Make it easy to complain.*** "If there is a strong culture of compliance, generally, in a practice or institution, then reporting of violations or suspected violations of whatever sort, via an anonymous tip line or other mechanism, may be promoted and used."

◆ ***Look beyond policies and procedures.*** "I don't care how carefully you have plotted out your privacy and security compliance plan," Harlow says. "It has to be implemented by the people in your organization, and if they have not bought in to the whole concept and taken the core principles to heart, then the plan can never truly be operationalized."

◆ ***Customize your approach.*** Make it homegrown, and provide training and education "not just with respect to the 'shalts' and 'shalt nots' in the privacy rulebook."

◆ ***Foster patient empowerment and "patient-centeredness."*** When this is done, "patients speak up immediately if something seems amiss rather than harboring misgivings."

CEs should take care to employ methods that fit "with a broader culture of compliance and patient centeredness and patient empowerment throughout the institution," Harlow concludes. "Unless this is done, an institution runs a greater risk of experiencing a local or general breakdown in the realm of patient privacy."

Don't forget that policies go both ways. Like other CEs, UMC has rules about when patients and their family members can use their own cameras; for example, taping live births, traditionally permitted, is no longer allowed. But like every good rule, this one has an exception. "We have had requests from women whose husbands are overseas serving in the military who want to Skype with their husbands during delivery," Dabbs relates. That, she says, has been permitted.

Contact Dabbs at Deborah.Dabbs@umchealthsystem.com, Harlow at david@harlowgroup.net and Tennant at rtennant@mgma.org. ✧