Report on
PATIENT PRIVACY
Volume 11, Number 1 • January 2011

Practical News and Strategies for Complying With HIPAA

'Harm' Concept for Breach Violations Is Broadening, May Encompass 'Dignity'

The memory cards contained data for nearly three years of procedures for patients — those who had endoscopic procedures at Mountain Vista Medical Center, a 178-bed hospital in Mesa, Ariz. Patients' names, dates of birth, as well physician information and the endoscopic images themselves, were stored on "compact memory cards" embedded in two endoscopy devices.

And they were missing. While there was no evidence that the loss was caused by a person with nefarious intent — the memory cards could simply have been misplaced, it seemed — on Dec. 11, 2010, the hospital issued a press release, posted a notice on its website and sent a letter to the 2,284 affected patients offering one year of free credit monitoring services.

But was the hospital required to take these actions? It is not clear the breach created a substantial risk of harm to patients, the standard for notification contained in the interim final rule now in force while final regulations are in development (RPP 8/10, p. 1).

The Mountain Vista incident typifies how the harm standard is being interpreted, with covered entities erring on the side of caution and perhaps notifying when they don't have to. Their concern is understandable, as the definition of "harm" is under debate, with some arguing for a more expansive definition that addresses "dignity," expert say.

The Mesa hospital's situation illustrates another phenomenon in the health care privacy and security world—protected health information is everywhere and all of it is vulnerable to loss. While hospitals and other CEs may take pains to secure PHI in patient records, they may neglect medical devices and other equipment, such as copier machines, that also store PHI. (For strategies on ensuring such devices protect data, see story, p. 4).

Hospital Removed Cards, Retrained Staff

Mountain Vista officials learned the memory cards were missing on Oct. 13, and subsequently launched a "thorough investigation," concluding they had "no evidence that information involved in the incident has been accessed or improperly used," according to the hospital's press statement.

Still, the hospital decided to notify patients, stating that "every precaution is being taken to reduce the risk of misuse of the information," and recommending that patients "take proactive steps to protect their credit," including by monitoring credit ratings and taking advantage of a free credit monitoring service Mountain Vista offered for one year.

The hospital said it also has "revised its security involving the storage of the compact memory data cards, has modified the endoscopy machines to no longer use the compact memory data cards, and has retrained the endoscopy unit employees on confidentiality and security procedures."

The Dec. 11 notification was just under the wire of the 60-day time limit for notification under the HITECH Act, so it would appear that the hospital was making the notifications in compliance with the federal law, although this is not stated outright. Timely notification also must be made to the HHS Office for Civil Rights (OCR) if more than 500 individuals are affected.

In response to a question about this from *RPP*, Mountain Vista spokeswoman Audrianne Schneider stated that "the notification and communication regarding this issue complies with all applicable federal and state requirements."

A few organizations, such as Health Net, have gotten into trouble for failing to notify required state officials, including in Arizona (RPP 12/10, p. 1).

Some states do not have a harm standard, and require notification to either the attorney general, department of insurance, or both, only when certain types of data are missing. Although the spokeswoman said "state requirements" were complied with, she also said they didn't apply.

"Because Social Security numbers or other financial identifiers were not involved, state agency reporting in Arizona and other affected states is not applicable," Schneider said in an e-mail. She also said the hospital would not answer any further questions about the incident.

Anxiety Drives Some Notifications

continued

Lisa Sotto, who heads the privacy and information management practice for the New York-based law firm Hunton & Williams, LLP, says CEs are "being conservative" and perhaps notifying patients when not absolutely necessary.

"There is a constant anxiety about whether to notify," Sotto says. "People don't want to be nailed for not notifying. They are notifying and moving on."

If Social Security numbers are breached, CEs will notify—no questions asked. But "once you are in the gray zone it depends on how conservative folks are," she says.

"Everybody is a little nervous about how HHS is going to interpret that standard. There is not a lot of precedent there," Sotto explains.

CEs that have breaches are conducting risk assessments to determine whether patients need to be notified, whether OCR should be as well and what state laws might also apply. Sotto says it's not uncommon for entities to notify patients even if the harm standard isn't met, but to notify OCR only when it's required. "There is no question these are tough issues," Sotto says.

FTC: 'Dignity' Could Be Harmed

A related — and broadening — harm standard is also being used by the Federal Trade Commission. In years past, it didn't really matter to health care entities what the FTC thought; that has changed as the FTC has become increasingly active in health care privacy and security investigations, some of which have resulted in joint settlements with HHS.

In September, Rite Aid Corp. paid $1 million to settle an HHS and FTC investigation of the firm's illegal disposal of prescription bottles containing PHI (*RPP 8/10, p. 12)*; in a similar settlement with HHS and FTC, CVS Caremark Corp. paid $2.25 million in February 2009 (*RPP 3/09, p. 3).*

FTC more recently has shifted its enforcement strategy to a "harm-based approach" that is "designed to target harmful uses of information — those presenting risks to physical security or economic injury, or causing unwarranted intrusions in our daily lives — rather than imposing costly notice and choice for all uses of information," David Vladeck, FTC director of the bureau of consumer protection, explained in congressional testimony last summer.

Appointed in June 2009, Vladeck's mention of "unwarranted intrusions in our daily lives" is part and parcel of his interest in broadening the concept of harm to include consumers' "dignity interests," which Sotto predicts will spill over into more FTC health care investigations.

Many health care attorneys have been warning in blog posts and client updates that Vladeck is taking an aggressive and activist role and may significantly expand FTC's authority and its interpretation of threats to privacy.

Another factor pushing officials toward a dignity standard is their discussions with their European counterparts; U.S. government privacy and security policies are increasingly being influenced by other countries, and there is much more interaction than ever before at high-level meetings and through other means.

Sotto herself recently moderated an American Bar Association webinar that featured Jennifer Stoddard, Canada's privacy commissioner. At the start of the webinar, Sotto asked participants to name their top three "game changers" or issues in the privacy and security area.

Stoddard first noted that "we need to do better enforcement," stating that "increasingly European commissioners are getting more" enforcement authority; she said she would "ask for greater powers" this year when the Canadian data privacy law comes up for review.

Then she spoke of needing to move beyond a harm standard. "In the coming years we are going to have to look at proof of harm for privacy breaches [and how] this has led to very few sanctions around the world, either in lawsuits or regulatory actions," Stoddard said. Companies may be violating regulations "and nothing happens, because, I think, we are overreliant on the proof of harm [standard]."

"We have to move beyond that and try and find a way of sanctioning — meaningfully — breaches that may eventually harm people, but the proof of harm [itself] may not be necessary. So this, I suggest, is moving from the harm principle to the dignity principle," Stoddard said.

European nations today take a much stronger stance about the value and importance of privacy; the preamble to the European Union Data Protection Directive states that privacy is among the "fundamental rights and freedoms" for all mankind. The directive, agreed to in 1995, required all European member states to enact their own laws for the protection of personal data.

Thus far, the U.S. has viewed privacy more as a consumer or patient protection, Sotto says, and has enacted laws that protect data by sector—medical, financial, consumer, etc. Yet this, too, is showing signs of changing, as national data breach bills have been introduced and are expected again in this new Congress (RPP 12/10, p. 1).

Battle Is Waging Over the Standard

The harm standard was greeted enthusiastically by CEs in the U.S., and their support has not wavered, despite the difficulties in interpretation, Sotto says. Retaining the harm standard "is very important," she says.

Kirk Nahra, a partner in the Washington, D.C., law office of Wiley Rein LLP, points out that regardless of whether the harm standard exists, is modified or removed entirely, CEs may still decide it is in their best interests to notify patients. CEs "are not precluded from notifying anybody whenever they want to," Nahra says.

But, he says, "a rule that forces disclosure every time is a bad rule. You want to encourage people to give notice every time there is a risk of harm."

Yet, as committed as some CEs are to maintaining the standard, patient groups may fight just as hard to remove it, insisting that all breaches be made public and affected patients notified, believing that there is an inherent conflict of interest when a CE makes the notification decision, says Cliff Baker, an advisor to Patient Privacy Rights.

Baker, also the chief strategy officer for Heath Information Trust Alliance, a health information consulting firm that also created a widely used security framework, says OCR really has little choice other than to acquiesce to the concerns of six members of Congress on the House Ways and Means and Energy and Commerce Committees, which drafted the HITECH Act.

The congressmen argued in an October 2009 letter to HHS that the standard violated congressional intent and should be repealed "at the soonest appropriate opportunity (RPP 10/09, p. 4).

"For me, that [letter] summed it up very well," Baker tells *RPP*. "Enforcing a requirement that has this ambiguous harm standard attached to it is difficult, and you dilute the objective" of the notification.

Contact Sotto at lsotto@hunton.com, Nahra at KNahra@wileyrein.com and Baker at cliff.baker@meditologyservices.com. ✧