Virtual Mentor
American Medical Association Journal of Ethics
March 2011, Volume 13, Number 3: 163-166.

JOURNAL DISCUSSION
Reassessing "Minor" Breaches of Confidentiality
Timothy Hotze

Dimick C. No harm done? Assessing risk of harm under the federal breach notification rule. *J AHIMA*. 2010;81(8):20-25.

Breaches of privacy have gained increasing attention in recent years, as more and more information about each of us becomes readily accessible online—either through our own efforts or without our knowledge. The presumed security of much of that information can be compromised and, once it is, the information can be spread easily and rapidly through digital networks. In one widely reported recent incidence, the security of account information at the popular blog network Gawker was breached [1], creating the risk for a form of "online identity theft"—someone other than the account holder could post comments under the account holder's name. More ominously, if the Gawker account holder employed the same password for accounts on other sites (e.g., e-mail or bank accounts), the security of those accounts could also be compromised.

Other recent media coverage has been given to financial information stolen from personal bank or credit card accounts [2] and computer networks on a major stock exchange [3]. In light of such large and public breaches, it is natural for individuals to prize personal (and especially private) information and for all of us to wonder how our private information might be compromised in the future.

Fundamentally, a breach of privacy is a breach of trust. We trust that a bank will keep our accounts secure and will not allow unwarranted access to our money. We trust that our login credentials to a website will be kept secure so that no one can act as a digital doppelganger and comment on a blog, posing as us. In the case of a bank, if a breach of trust does occur, the damage, and therefore the remedy, are most likely to be financial: a customer might reasonably expect the bank to cover damages from a theft of data, and some banks might offer credit monitoring services after such a loss to protect against continuing financial harm.

Unlike financial harm, a loss of trust between patient and doctor can be much harder to quantify or repair. The confidentiality between patient and doctor has long been observed and was codified in the first AMA *Code of Medical Ethics* [4]. The trust that comes with confidentiality facilitates the patient's describing (often very private) matters. Keeping symptoms, diagnoses, and treatment confidential is essential to maintaining trust in the profession and ensuring that patients return for ongoing treatment or when new symptoms develop.

There have been a number of legislative moves in recent years to help codify what information should be considered protected or confidential, as well as how and under what conditions that information may be shared. The 1996 Health Insurance Portability and Accountability Act (HIPAA) established guidelines for protecting personally identifiable patient information. More recently, the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, encouraging medical practices to implement electronic health records, spurred the Breach Notification for Unsecured Protected Health Information Rule [5]. This rule states that HIPAA violations must be reported to both the patient and the Department of Health and Human Services (DHHS); the violation need not be disclosed, however, if there was no significant risk of financial, reputational, or other harm to the patient [5].

Although the rule provided some examples, no set of examples could be inclusive enough to be instructive in all cases. In his article *No Harm Done*, Chris Dimick notes that the rule has caused many organizations to go into "overkill mode" [5], resulting in large jumps in the number of HIPAA violation investigations, many of which may not be necessary by the letter of the law.

Dimick offers interviews with a number of privacy officers at various health care organizations across the country. Although the specifics differ in each case, the organizations highlighted in the article share several experiences and characteristics. First, all suggest or state directly that since the rule has taken effect they have been confronted with more cases and have learned from experience, now treating risk-of-harm assessments differently.

All the health systems surveyed also follow officially sanctioned organizational procedures for assessing risk. These procedures might include e-mails or other correspondence surrounding the incident and comments or questions raised when the incident was brought to the attention of the privacy officer. All those Dimick interviewed also advocated ensuring that some key questions, such as the type and quantity of information revealed, be answered before the matter could be considered closed.

As a brief but relatively complete example, in a sidebar, Dimick republished the three determinants of risk delineated by Milwaukee's Aurora Health Care: "harm based on content and recipient" (who received access to protected health information and what information they received), "assessment of harm by the patient" (notifying the patient before deciding whether or not a formal report, which must be forwarded to DHHS, should be created), and "harm based on assurances received" (where a minor, but technically impermissible, disclosure occurs but where assurances are made that the information will not travel further and will be destroyed) [6].

Without a doubt, creating formal processes to document how risk was assessed is essential, both to protect a health care organization and to ensure that relevant facts of a case are examined, both for the sake of the patient and for the health care

organization; yet the focus of both this example and several others seems to confuse the letter and the intent of the law.

Many of the privacy officers suggest disclosing the breach of information to the patient unless it is absolutely clear that no harm was committed. In the cases that are disclosed to the patient, it may be determined, based on the patient's reaction, that no harm was done and that no further investigation (or reporting) need occur. While this is a sensible solution, and it is certainly right to ask the patient whether he or she feels harm occurred, it also suggests a reversal of priorities.

Using the patient as a "harm meter," rather than respecting him or her as a human being who may have been harmed by a breach of trust, suggests that the *real* concern is not the patient or trust, but instead, having to undergo a formal investigation and sending a subsequent report of a breach to the federal government.

The reason for defining protected information in HIPAA and the privacy rule that resulted from the HITECH Act are designed to protect the patient [7] and define, legally, the confidentiality of a patient-doctor relationship that has, over time, grown to include many health care professionals.

Given the focus on patient-centered communication in the context of a patient-doctor encounter [8, 9], it is somewhat disheartening to believe that when it comes to breaches of privacy with confidential patient information, we cannot maintain this patient-centered approach. Protecting an organization against harm resulting from an accidental breach of information is important, as is creating a formal process to evaluate the degree of harm and next steps. However, there is absolutely no reason that concern for the patient cannot and should not be the at the heart of these efforts.

References

1. Stelter B. Hackers disrupt sites run by Gawker Media. *New York Times*. December 12, 2010. http://www.nytimes.com/2010/12/13/business/media/13gawker.html?_r=1&src=busln. Accessed February 15, 2011.
2. HSBC admits huge Swiss bank data theft. *BBC News*. March 11, 2010. http://news.bbc.co.uk/2/hi/business/8562381.stm. Accessed February 15, 2011.
3. Naraine R. Nasdaq confirms servers hacked via web-facing application. *ZD Net*. February 7, 2011. http://www.zdnet.com/blog/security/nasdaq-confirms-servers-hacked-via-web-facing-application/8087. Accessed February 15, 2011.
4. American Medical Association. *Code of Ethics of the American Medical Association; May 1847*. 1st ed. Chicago: American Medical Association Press; 1897. http://www.ama-assn.org/ama1/pub/upload/mm/369/1847code.pdf. Accessed February 15, 2011.

5. Dimick C. No harm done? Assessing risk of harm under the federal breach notification rule. *J AHIMA*. 2010;81(8):20-25.
6. Dimick, 23.
7. Blumenthal D. Launching HITECH. *N Engl J Med*. 2010;362(5):382-385. http://www.nejm.org/doi/full/10.1056/NEJMp0912825. Accessed February 15, 2011.
8. Swenson SL, Buell S, Zettler P, White M, Ruston DC, Lo B. Patient-centered communication: do patients really prefer it? *J Gen Intern Med*. 2004;19(11):1069-1079.
9. Cooper LA, Roter DL, Johnson RL, Ford DE, Steinwachs DM, Powe NR. Patient-centered communication, ratings of care, and concordance of patient and physician race. *Ann Intern Med*. 2003;139(11):907-915.

Timothy Hotze is a senior research assistant in the Institute for Ethics at the American Medical Association in Chicago. His research interests include reducing health care disparities, ensuring equal access to care, and how technological change affects medical ethics.

Related in VM
Use of Electronic Patient Data in Research, March 2011