

Jay Cline: Are medical-data breaches overreported?

Healthcare organizations should make better use of the 'significant risk of harm' exemption in the federal law

By Jay Cline

September 20, 2011 09:26 AM ET

Computerworld - The Eli Lilly employee whose programming glitch [exposed the e-mail addresses of almost 700 Prozac users](#) to each other didn't know he was making history. Since that day in June 2001, hundreds more US healthcare organizations have reported medical-data breaches. As a result of those reports, federal and state health agencies have dealt out millions of dollars in fines, and the U.S. Department of Health and Human Services has launched a round of 150 audits. Meanwhile, a cottage industry of breach-notification service providers has arisen, and healthcare organizations can't find enough privacy talent to batten down the hatches.

But is this obsessiveness over health-data privacy warranted? Do medical-data breaches harm people, and does notifying them of the incidents help them?

The answer to these questions might seem like a resounding yes. The thought of our medical records ending up on websites or in criminals' hands makes us nervous. We want to know about these incidents if they happen, even though few of us take any action as a result of being notified.

This large and growing allocation of healthcare resources in an era of cost containment, however, deserves a closer look.

The phenomenon of data-breach notification started in California the same year as the Eli Lilly incident. State legislators Steve Peace and Jim Simitian drafted what became [SB 1386](#), the first data-breach notification act in the world. Passed in 2002, this law remained an outlier until the infamous [ChoicePoint breach](#) of 2005. Nearly every U.S. state passed a breach-notification law in its aftermath, and many other countries are following suit. Most of these laws notably did not include personal medical records in their scope of concern.

That all changed in 2009. In April of that year, Congress passed the [HITECH Act](#) as part of the economic-stimulus package. Included in that act were instructions for the U.S. Department of Health and Human Services (HHS) to issue a series of new rules about improving the protection of personal health information. In August 2009, HHS released its first installment -- an "interim final rule" on notification of health-data breaches. By the end of 2011, HHS is expected to divulge its "final final rule" on medical-data breach notification.

The landmark feature of the interim final rule is a mandate to immediately notify HHS of any data breaches affecting 500 or more people. The rule also requires an annual notification to the department of incidents affecting fewer people. The department posts the notices for the large breaches on its infamous "[wall of shame](#)."

A close look through the wall of shame tells a curious story. More than a handful of incidents don't appear to involve malicious intent or easy-to-use media. A number of entries cite "other," "loss" or "improper disposal" for the type of breach, instead of "theft" or "unauthorized access." A large share also cites "paper" as the medium, instead of easier-to-manipulate electronic media. On the wide spectrum of data breaches, these often fall on the low-impact side.

The department itself implicitly acknowledges this reporting of low-risk breaches. Last month, HHS released its [Annual Report to Congress on Breaches of Protected Health Information For Calendar Years 2009 and 2010](#). The congressionally mandated report details the type and origin of large and small reported incidents, where large incidents are those affecting 500 or more people.

The study counted 252 large-scale breaches affecting 7.8 million individuals. Of these, 37 cases affecting 1.1 million people involved only the loss of electronic devices or paper. Likewise, 29 cases impacting about 600,000 people stemmed from misdirected communications and similar nonmalicious errors.

The report also tallied over 30,000 small-scale incidents affecting just over 50,000 people. Of these small breaches, HHS noted that the majority involved misdirected communications affecting only one individual. These are a lot of seemingly low-impact breaches.

What's going on here?

I think companies are either afraid to be caught not reporting a low-grade breach after the fact, or they don't know about the "significant risk of harm" exemption in the interim final rule.

This exemption allows organizations that have suffered a medical-data breach to determine if that breach poses a significant risk of harm to the persons whose information was included in the incident. The regulations define a [security](#) or privacy compromise as one posing "a significant risk of financial, reputational, or other harm" to the person affected.

That risk determination can conclude that the people who had access to the health data did not pose a threat. It can also conclude that the circumstances of the incident do not pose a risk of harm. In addition, the rule states that organizations suffering an incident

"should also consider the type and amount of protected health information involved." In other words, not all medical-data breaches are created equal.

It would be one thing if our names were posted on a public website, for example, along with a list of other people cited as having mental illnesses, venereal diseases or drug addictions. This not only could be embarrassing, but it could also affect our social prospects and career outlooks. We could suffer both tangible and intangible -- or "dignitary" -- harm.

But what trouble could befall us if our dental records were thrown out with the trash or if our allergy medications were included on the laptops stolen by a petty thief? What harm is caused if the world knows you have a broken finger, had the flu last week or visited the only clinic in town on a certain date last year?

I'll go out on a limb and say there would be no embarrassment and no social or economic impact arising from these incidents. And yet a significant number of organizations appear to be making public notifications of these breaches.

How can this situation be improved?

I think healthcare organizations should band together. They should voluntarily adopt a self-regulatory standard for medical data-breach notification that specifies which types of data incidents do and do not pose a significant risk of harm according to the criteria laid out in the interim final rule.

That standard could take the form of the table below:

TYPE OF BREACH TYPE OF RECORD	GOOD-FAITH ACQUISITION OR NONPUBLIC EXPOSURE Examples: misdirected communications, improperly disposed papers and devices, and devices or papers lost in a private area	PROBABLE OR KNOWN PUBLIC EXPOSURE OF THE DATA Examples: lost devices or papers in a public area, or temporary accidental posting to a website	INTENTIONAL MALICIOUS ACQUISITION OF THE DATA Examples: stolen devices, breached networks, and employee wrongdoing
QUALITATIVE PERSONAL HEALTH INFORMATION Examples: mental or sexual health, addictive behavior, terminal or chronic conditions, children's information	Possible significant risk of harm; the default approach is to not notify unless unusual circumstances warrant caution	Often significant risk of harm; the default approach is to notify unless the known risks have been contained	Always significant risk of harm; always notify
INCIDENTAL PERSONAL HEALTH INFORMATION Examples: routine treatments and prescriptions, common maladies	Rarely significant risk of harm; rarely notify	Possible significant risk of harm; the default approach is to not notify unless unusual circumstances warrant caution	Often significant risk of harm; the default approach is to notify unless the known risks have been contained

Here's an example of how this table could be used. Let's say a dental practice misplaces a box of adult patient records. If it was lost within the practice's office complex, the first column marked "Good-faith acquisition or nonpublic exposure" would be the appropriate choice. Next, since dental treatment is routine and common, and none of the practice's patients in memory had a chronic condition, the second row down marked "Incidental personal health information" would be appropriate. At the cross-section of those two vectors is the recommended analysis: "Rarely significant risk of harm." Conclusion: there's no need to notify.

In spite of national healthcare reform, medical costs continue to escalate unabated. We can protect patient privacy without adding unneeded, costly bureaucracy by reining in overnotification of medical-data breaches.