No Harm Done? Assessing Risk of Harm under the Federal Breach Notification Rule

By Chris Dimick

Provisions within the HITECH Act require that covered entities notify individuals if their protected health information is breached. However, the current regulation allows an exemption if the risk of harm is slight. Assessing risk can be subjective, and privacy officers have been working to create methods to conduct and document their analyses.

The independent 18-year-old man had moved out of his parents' home and begun taking on the responsibilities of life-including paying his own medical bills. But after a visit to his local hospital, he began to get behind on payments.

The hospital's collection agency mailed out an overdue bill notice but mistakenly sent it to an old address on file, his parents' home. The notice included the amount owed and limited information about the visit.

The mistake was identified internally, and the incident was reported to the privacy officer, who had a decision to make. Did this HIPAA violation carry a significant risk of harm to the patient and thus require that he be notified of a breach to his privacy? Or-because a limited amount of information was disclosed to an immediate relative-was the risk of harm low and no notification required?

For the past 11 months, privacy officers have been debating questions like this and developing processes for determining the risk of harm that comes from a HIPAA violation.

On August 24, 2009, the Department of Health and Human Services (HHS) released the Breach Notification for Unsecured Protected Health Information Interim Final Rule, part of the regulations coming out of the HITECH Act. The rule stated that covered entities must report HIPAA violations to both HHS and the affected patient through a breach notification. However, the interim final rule included a harm threshold provision, allowing the organization to omit notification if it determined that the impermissible use or disclosure posed no significant risk of "financial, reputational, or other harm" to the individual.

The provision was controversial, with consumer advocates, some providers, and even legislators claiming the threshold defied the intent of the law. Others described it as necessary, noting that it was impractical and unhelpful to notify individuals of minor errors unlikely to harm them-such as a misdirected e-mail sent within the organization or a fax mistakenly sent to the wrong clinic.

Regardless of opinion, the interim rule took effect the following month, and covered entities began seeking effective processes for determining risk of harm. HHS provided some guidance on breach exemptions, but privacy officers have found that the definition of harm is unique to each case and each patient. Determining risk can be a subjective process, but organizations are identifying steps and measures that help them evaluate whether a breach notification is necessary.

New Rule Increased Workload

At press time, HHS had not published its final rule on breach notification, although it is expected this summer. There is a chance that the harm threshold could be removed.

Regardless of the final rule, some privacy officers and HIM professionals believe risk-of-harm assessments should always be part of a HIPAA violation investigation. They are an accurate way to record and log a HIPAA violation and can help officials mitigate a breach by determining where harm was committed, according to Peg Schmidt, RHIA, the chief privacy officer with Aurora Health Care in Milwaukee, WI.

The last year has been a busy time for privacy and security officials. The HITECH Act within ARRA instituted several measures designed to tighten up HIPAA and further protect patient privacy. The changes led to a fresh round of privacy training within facilities, which increased the number of incidents reported to privacy officials.

At Ministry Health Care, based in Milwaukee, WI, the number of HIPAA violation investigations has doubled since the breach notification rule was instituted, according to Nancy Davis, MS, RHIA, director of privacy/security officer at Ministry. Davis conducts a breach investigation and risk-of-harm assessment on every HIPAA complaint or concern reported in the 14-hospital organization.

From 2006 to 2008, Davis says Ministry averaged about 40 HIPAA violation investigations a year. In 2009 that number jumped to 98 investigations, with 48 of those reported late in the year following the implementation of the breach notification rule. HHS's interim final rule was the first breach notification requirement Wisconsin providers had seen-the state did not have a similar requirement in place.

"This has really changed my job, quite a bit," Davis says. "Many privacy officers, especially in large systems, are feeling so overwhelmed, because we now have that additional component of the HIPAA investigation-the risk assessment and breach notification."

Many organizations are in "overkill" mode, asking employees to report all HIPAA concerns for fear of missing a case that should lead to a breach notification, Schmidt says. Her cases also doubled since the breach rule was instituted.

Incidents Exempted from Breach Notification

While HHS has not provided comprehensive guidance on determining risk of harm, it did provide the following examples of low-risk HIPAA violations in the breach notification interim final rule that are exempt from breach notification:

- Good faith, unintentional acquisition, access, or use of PHI by a workforce member of a covered entity or business associate
    - ***Example:*** *A staff member receives and opens an e-mail from a nurse containing protected health information about a patient that the nurse mistakenly sent to the staff person.The staffer realizes the e-mail is misdirected and deletes it.*
- Inadvertent disclosure to another authorized person within the entity or its business associates
    - ***Example:*** *A nurse calls a doctor who provides medical information on a patient in response to the inquiry. It turns out the information was for the wrong patient. Such an event would not be considered a breach, provided the information received was not further used or disclosed in a manner not permitted by the privacy rule.*
- Recipient could not reasonably have retained the data
    - ***Example:*** *A nurse hands a patient a medical report but quickly realizes that it was someone else's report and requests its return. In this case, if the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then providing the medical report to the wrong patient does not constitute a breach.*

Subjectivity a Challenge

The way privacy officials conduct breach notification investigations and risk-of-harm assessments has been evolving since the rule was published in August 2009. Experience has led to more refined ways to determine if a breach notification should be sent, and risk-of-harm protocol have adapted. Mitigating subjectivity between cases is the major challenge privacy officers' face when determining risk-of-harm, Davis says.

"When we started, we felt like we were going to want to err on the side of reporting for fear of doing it wrong," Schmidt says. "If we couldn't absolutely come to any decision in a real immediate way, we said, 'Well, we are going to report that.' But as you touched new cases, you learned from each case. We are handling cases differently now than before."

Breach notifications are sent in response to a confirmed HIPAA violation-an inappropriate access, use, or disclosure of patient information. However, not all HIPAA violations require breach notifications. The risk-of-harm assessment allows a privacy official to look at all the evidence and determine if that violation will cause harm to the patient and warrants a breach notification, Davis says.

At Aurora Health Care, which is comprised of 14 hospitals and more than 100 clinics, local privacy officers conduct the leg-work in investigating a HIPAA complaint. If they confirm a violation, then they forward the case to Schmidt, as chief privacy officer, for the risk-of-harm assessment.

Schmidt and her privacy officers follow a documented process in assessing risk. "Low risk" determinations cannot be based on opinion alone. Harm must be assessed in various categories, including the type of PHI released (was there sensitive information?), who the information was distributed to and the circumstances behind the disclosure (was it an unintended recipient or a malicious disclosure?), and any assurances they receive that the information has been destroyed or restricted (the interim rule states that proper assurances of mitigating the disclosure can lower risk of harm).

Using a privacy breach investigation record of some type is considered a best practice, Davis says, as it gives organizations a way to document their risk analysis decision should they be questioned on their breach notification decision either by a patient or the Office for Civil Rights, the federal organization in charge of enforcing HIPAA.

A typical breach investigation record contains a brief description of the privacy complaint or concern, copies of any e-mail correspondence regarding the incident, and a series of questions that help identify the level of risk. Within the investigation record designed by Davis and used at Ministry, the risk assessment section asks questions that include:

- Who impermissibly used the information, or to whom was the information impermissibly disclosed?
- What is the potential for significant risk of financial, reputational, or other harm?
- What is the type and amount of PHI involved?

There are some cases where determining the risk of harm is obvious, Davis says. The release of sensitive personal health information, such as diagnoses, procedures, Social Security numbers, and date of birth, should always be considered harmful and constitute a breach notification.

But other incidents, like the example given at the start of this article, are less cut and dried. In that case, disclosing a hospital bill to the teen's parents might not pose a significant risk of harm. The information disclosed was minimal, and the mistake was a reasonable one.

But what if the 18-year-old did not want his parents to know he was being treated? What if the hospital visit centered on treatment of an STD, and the son was hiding his hospital visit from his parents? The receipt of a bill from a hospital could spark the parents to inquire about the son's health, and he may feel harmed by the disclosure. However, if the bill is for a knee injury the parents know about, the risk of harm would be minimal.

Schmidt says she has learned that the individual in an unauthorized disclosure is just as significant in determining risk of harm as is the content of the disclosure.

"What is maybe considered harmful to one patient is not harmful to a different patient," Schmidt says. "Or what I might argue is harmful as an entity might not be harmful in the patient's eyes. I'm not in the patient's shoes."

Three Ways to Assess Harm

Each individual breach case is unique, and privacy officials should expect to assess each case individually. However, each investigation should follow the same process and criteria. Milwaukee-based Aurora Health Care evaluates three categories during every risk-of-harm assessment.

Harm Based on Content and Recipient

Both the nature of the disclosed information and the individual to whom it was disclosed influence risk of harm. A recipient of PHI who did not seek out the access, who is cooperative and willing to quickly return information, who did not have any adversarial relationship to the individual or likelihood of personally knowing the individual could be considered a "low risk recipient." A covered entity could also be considered a low risk recipient. Questions to consider include:

- What content was disclosed-just identifiers or medical, sensitive information? A bill is different than a dictation.
- Is it likely the recipient will be able to identify the patient whose information they received? Did the disclosure happen in a small community or a big city?
- What is the relationship between the recipient and the patient? Is it a family member in good standing with the patient or one half of a divorcing couple?
- Was the incident an intentional, unauthorized access or an accidental disclosure?
- What is the recipient's attitude when reporting the violation? Do they seem to want to protect the information and return it, or are they holding it over the organization's head as leverage for something else?

Assessment of Harm by Patient

Unless it is absolutely clear there is no harm, privacy officers contact the patient to discuss the incident and listen for his or her reaction as a way to assess harm. This works well for common mistakes. If a patient does not believe there is harm, privacy officers offer an apology but no further reporting to HHS is necessary.

Harm Based on Assurances Received

HHS states that an impermissible use or disclosure might not qualify as a breach if the covered entity obtains satisfactory assurances that the information will not be further used, disclosed, or retained. This is appropriate only in cases that are lower risk with no malicious intent. To gain this assurance:

- Obtain a confidentiality statement. The organization's human resources department can help. If the recipient provides the statement and circumstances are otherwise acceptable, then no patient contact is required.
- Request a certificate of destruction. OCR requires that the organization must be able to demonstrate destruction.

Calling Patients Aids Assessment

Getting into the patient's shoes is a piece of risk assessment some privacy officials are adding to their investigations. In some cases, Ministry Health Care calls patients to discuss the breach and understand how harmful the patient considers the disclosure.

Before Ministry began the practice in March, Davis would err on the side of caution in borderline cases, sending a breach notification just to be safe. But soon her staff realized that in relatively low-risk cases, the patient might be the best person to determine if risk of harm exists.

Ministry only contacts patients when the risk of harm is not obvious, such as disclosures involving minimal information like patient name and the balance owed to the facility.

"We do this in cases where we are really on the fence," Davis says.

For example, Davis has called patients when billing statements for a father have been mailed to his son who has the same name and lives at the same address. Though the risk of harm may seem low in this situation, Davis says a phone call to the father to discuss the situation can help immediately determine the risk of harm.

If the patient believes that he or she has not been harmed, the case is determined to be low risk and no formal breach notification is sent to the patient or HHS. The discussion is documented in the risk assessment.

If the patient cannot be reached and privacy officials are uncertain of the level of harm, Ministry sends a breach notification by default, Davis says.

Davis and her team do not call individuals in cases where the risk of harm is high and a breach notification is likely warranted, such as an intentional unauthorized access or when sensitive personal information is sent to the wrong patient.

The phone calls have reduced the number of breach notifications sent at Ministry, as they have at Aurora, which has a similar practice.

If after reviewing all pieces of the case she remains unsure of the risk, Schmidt says she will contact the patient and discuss his or her view of the harm. In addition to assessing harm, the call also gives staff a chance to formally apologize for the breach and answer any questions the patient may have.

"We decided to call the patients and let them tell us in their own way how harmful this is," Schmidt says. "That seems like a very direct way of knowing if we reached that significant threshold of harm."

Risk-of-Harm Flow Sheet

Using a risk-of-harm analysis flow chart can help determine if the level of risk justifies a breach notification. The HIPAA Collaborative of Wisconsin (HIPAA-COW) offers an extensive white paper on the breach notification rule that includes a flow chart within the harm analysis tool. It may be found at www.hipaacow.org.

NCHICA Tool Scores Risk

While HHS guidance has been limited, several healthcare organizations have developed tools and white papers that can help privacy officials determine risk of harm.

In June the North Carolina Healthcare Information and Communications Alliance (NCHICA) updated its well-used HITECH Act Breach Notification Risk Assessment Tool to reflect experience gained in the previous months by the tool's authors, the NCHICA Privacy/Security Officers Workgroup.

The NCHICA tool provides a way to evaluate risk of harm using a scoring system that ranks incidents from low to high risk. The tool describes the variables of a HIPAA violation-such as recipients, circumstances of release, and disposition of the information-and ranks examples of those variables from 0 to 3. The more harmful the examples in each variable, the higher their corresponding score.

For example, in the "method of disclosure" variable, the incident examples read:

- Unauthorized internal acquisition, access, and/or use without disclosure outside of organization = 0
- Verbal disclosure or unauthorized view only = 1
- Paper/fax = 2
- Electronic = 3

At the end of the exercise, the user adds up the incident's score and places it on a risk-of-harm scale.

The NCHICA tool is not meant to be the sole deciding factor as to whether a HIPAA violation constitutes a breach notification, says J.T. Moser, chief privacy officer at Wake Forest University Baptist Medical Center in Winston-Salem, NC,

and member of the NCHICA Privacy/Security Officers Workgroup.

However, it can be a useful tool, especially for those members of a risk assessment committee, such as IT or marketing, who might not have a deep background on HIPAA or the requirements of the breach rule.

"This tool is not designed to make a decision for the user, it is really to help make the decision," says Moser, who uses the tool at his organization. "It really helps us, because in our process we have compliance, legal, IT, security, and privacy at the table. It helps get a consensus on what we think the risk of harm is since some of it is pre-scored before we get into the room."

In addition, he says, having a tool also helps provide a framework for the discussion and gives the team focus.

Creating Common Ground

The tool not only provides expert guidance for privacy officers in individual organizations, but its wide use also strengthens an individual organization's case for conducting harm assessments if its processes were ever challenged.

"Everybody struggled with how to measure harm and conduct the risk assessment. We wanted to pull all the experts together to figure out how everybody was interpreting the laws so we could go back and say that if some event occurred at hospital A, we would be measuring it the same way at hospital B across the street," said Larry LaBanc, information security official at Novant Health System, based in Winston-Salem, NC, and member of the NCHICA Privacy/Security Officers Workgroup.

"This is a common ground to start with to help everybody make those assessments in the same manner and weigh the risks with the same values."

This evaluation also offers a recordable methodology for risk- of-harm assessment, something privacy officers can revisit long after as supporting documentation for their eventual breach notification decision, LaBanc says.

Even if the final rule removes the risk-of-harm assessment piece, the NCHICA tool is still a good way to document a breach investigation.

"It creates a common place to collect your thoughts, show how you scored things, the environment at the time," he says. "We have to make sure that we are memorializing these investigations so that we can go back and see where we were and what facts were available to us at the time that caused us to make those decisions."

The tool, which can be adapted in any state to help determine risk of harm, is available on NCHICA's Web site at www.nchica.org.

Good Reasons to Get It Right

Creating a solid, fact-based risk-of-harm analysis protocol is essential, Davis says. The stakes for protecting patient information are much higher today, with increased HIPAA enforcement and electronic systems enabling the easy exchange of protected health information.

Privacy officials should not assume certain cases are low risk without conducting a proper investigation, she warns.

Conducting risk analyses does not necessarily lead to more breach notifications, Schmidt says. Several times she has received a case that at first glance she thought would require breach notification only to conclude it was low risk once the risk assessment was completed. The assessment helped her feel confident that notification was not necessary.

Additionally, a well-documented breach notification investigation is vital if OCR or a patient challenges a HIPAA violation investigation.

"If I were to have to respond two years later to an OCR complaint, I would feel much better knowing that I have the documentation of that [past] incident," Davis says.

Potential fines from OCR aside, instituting a fair and reasoned process is something healthcare facilities owe to patients, Schmidt says.

"This is your facility's reputation at stake in the community," she says. "That is a more compelling reason to be doing the right thing, in addition to the regulatory requirements.

"You want your patients' trust, so that can't be ignored."

Chris Dimick (chris.dimick@ahima.org) is staff writer for the *Journal of AHIMA*.

Article citation:
Dimick, Chris. "No Harm Done? Assessing Risk of Harm under the Federal Breach Notification Rule" *Journal of AHIMA* 81, no.8 (August 2010): 20-25.
