COSMOS
Navigate the Compliance Universe

Compliance Today - September 2019
Risks with the breach risk assessment

By Yvonne M. Wolters, MBA, CHPC, CLA

Yvonne M. Wolters (ywolters@swgeneral.com) is the Privacy Officer and Compliance Specialist at Southwest General Health Center in Middleburg Heights, OH.

Determining whether the privacy or security of protected health information (PHI) meets the low-probability-of-compromise threshold can be complex, which is further exacerbated when presented with ethical considerations and the risk for fraudulent activity. Based on the following scenario, this article will provide an analysis of the Breach Notification Rule[1] risk assessment. This analysis will discuss the four-factor risk assessment, the term compromise, factors beyond the minimum four, and defensibility.

Using the following scenario, consider whether your risk assessment proves low probability of compromise to the privacy or security of the (PHI) involved.

Scenario: A patient was recently admitted to the hospital for what he believes is pneumonia. A nurse practitioner (NP) goes into the patient's room to discuss the patient's recent test results. One visitor is in the room with the patient, so the NP asks the patient if it is OK to discuss his test results in front of his visitor. The patient tells the NP it is OK. The NP tells the patient his test shows he is HIV positive and that his pneumonia is associated with the HIV infection. The patient becomes infuriated with the NP, because the patient feels he was not given adequate opportunity to discuss this diagnosis with his visitor on his terms and when he was ready. The patient tells the NP that he believes the NP violated his right to privacy and says he is going to file a complaint with the Office for Civil Rights (OCR). The patient had no idea being in the hospital for pneumonia would result in a positive HIV test.

Breach and risk assessment review

According to the Department of Health and Human Services' Breach Notification guidance, "A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:"[2]

- Nature and extent of the PHI involved;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

The risk assessment is ultimately used to determine the level of compromise to the PHI involved and is used as documentation to demonstrate when a low probability, or low risk, of compromise exists. The Final Omnibus Rule in 2013 revised the breach definition from the previous HITECH definition that assessed the risk of harm

and added the above four factors as an effort to make the risk assessment more objective; meaning, the risk assessment would be performed using facts and without influence by personal feelings, emotions, or opinions. Since all impermissible uses and disclosures of PHI are presumed to be a breach unless low probability of compromise can be proven, incidents that cannot prove low probability of compromise are considered reportable breaches.

Generally, the four-factor assessment to this scenario may look like this:

1. PHI disclosed – Name and diagnosis.
2. Unauthorized person – Visitor who was in hospital room with the patient.
3. Actually acquired/viewed – Yes, PHI was actually acquired.
4. Mitigation steps – No further PHI was disclosed to the visitor and the patient's right to request restrictions was explained to him, as well as how to exercise this right to help prevent future similar disclosures.

Some may deem this incident as low risk of compromise (not a reportable breach) because:

- The four-factor risk assessment, as written above, appears to prove low probability of compromise to the privacy or security of the PHI involved;
- The patient was given an opportunity to object and he did not; in fact, he gave verbal permission;
- The disclosure was to a visitor who, by using professional judgment, appeared involved in the patient's care, which was presumed, based on the fact the person was there with the patient and the patient seemed to be OK with discussing his care in front of the individual; and/or
- The risk was mitigated.

Beyond the minimum four factors

Unfortunately, applying the factors as shown above does not depict the true scenario or the seriousness of the privacy matter and the actual risk to the PHI. Nor does it convey the apparent affect and potential harm the disclosure had on the patient. In fact, the risk assessment could have been done in a different way.

1. Name and new sensitive diagnosis.
2. Visitor who was in hospital room with the patient.
3. Yes, PHI was actually acquired.
4. Unable to mitigate; PHI verbally disclosed to visitor.

The Breach Notification Rule states, at a minimum, to use the four-factor risk assessment. There may be additional factors to consider, which will be situation-dependent. For example, when the incident is a ransomware attack, availability (i.e., whether the information was encrypted) and integrity (i.e., whether the hackers altered the information) should be considered in the risk assessment. To determine what other factors might need to be considered, refer to the additional section of the breach definition, which explains that the term compromise means "it poses a significant risk of financial, reputational, or other harm to the individual."[3] In applying this provision of the Rule, additional factors should be considered in this scenario:

5. Are there applicable privacy or security protections under state laws or other federal regulations?

- In this case, say there are state privacy laws for HIV/AIDS- or AIDS-related diagnosis. Although verbal consent was obtained from the patient, which may address applicable state laws, the patient could argue his right to personal autonomy was violated, because he was not given adequate information in order to make an educated decision about the risks of disclosing the diagnosis. How could he have objected to discussing a diagnosis he did not know he had?

6. Was mitigation actually achievable?
    - The PHI was disclosed verbally. The patient's visitor clearly knows the patient and as such, it is highly unlikely the visitor will forget the diagnosis. If mitigation (the fourth factor of the Breach Notification Rule risk assessment) is not achievable, should the incident be a reportable breach?
7. Was there other potential or actual harm to the affected individual?
    - The relationship with the visitor is unknown (e.g., friend, partner, sibling, parent, coworker). The PHI disclosure may have had a negative impact on the patient's relationship with the visitor, and given the patient's immediate reaction to the disclosure, it is quite possible. The PHI was disclosed to the visitor who is not obligated to keep it confidential and who may be a person prone to gossiping, which may have negative repercussions the patient's personal or work life.
8. Is there a broad reach of potential harm (e.g., complaint, lawsuit)?
    - The patient became clearly upset over the disclosure, stated his privacy was violated, and said he was going to file a complaint with the OCR. It is also possible the patient could seek legal action for this privacy matter under state law or otherwise.

These additional factors not only tell more about the situation, but they are relevant in providing a better understanding of the risk to the PHI and potential harm to the patient. Given the additional factors to consider in this scenario, one may now consider this incident a reportable breach. The risk assessment is not required to be documented when breach notification is provided. However, the risk assessment is often used to determine the level of compromise in the situation, and as such, it may be documented even when the incident is determined to be a reportable breach.

Walking through the risk assessment process for this scenario shows how the determination of whether a privacy incident is a reportable breach can be subjective and open to interpretation influenced by personal feelings, emotions, or opinions. One can now see how this determination is not just a legal decision but an ethical one.

Other factors provided in guidance from the Department of Health and Human Services to help evaluate the level of compromise are as follows and will be situation-dependent:

- Applicable state or other federal laws, regulations, or requirements
- Whether mitigation would actually be effective

Other potential or actual harm to affected individual(s) may include:

- Harassment or prejudice;
- Blackmail;
- Mental pain or emotional distress;

- Secondary uses resulting in fear or uncertainty;
- Physical harm (e.g., disclosed address of victims of abuse);
- Reputational harm (e.g., employment, community standing, personal relationships, religious beliefs);
- Unwarranted exposure leading to humiliation or loss of self-esteem;
- Whether disclosure could result in illegal use of PHI (e.g., Social Security numbers); or
- Likelihood that harm will occur, which will depend on the manner of the actual or suspected breach and the types of data involved in the incident.