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 should 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 practice administrator can help. If the recipient provides the statement and circumstances are otherwise acceptable, then no patient contact is required.

Request a certificate of destruction, if applicable. OCR requires that the organization must be able to demonstrate destruction.