Health Care Compliance Association Audio Conference
Privacy Matters: Creating a Systematic Investigation and Reporting Process for Privacy Complaints

Health care organizations are under increased pressure to improve the privacy and security of protected health information (PHI). Notably, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is reviewing various organizations' compliance with the Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules and breach notification standards under the Health Information for Economic and Clinical Health (HITECH) Act. During the course of 2012, OCR plans to conduct privacy and security audits of 150 health care entities and potentially their business associates. The OCR audits can ultimately lead to increased government scrutiny and possible fines for entities with inadequate safeguards for PHI. To avoid such implications, entities must ensure that they have a defined process to protect PHI and report breaches in accordance with the HIPAA Privacy and Security Rules and HITECH Act.

To assist organizations with OCR audits, the Health Care Compliance Association recently held an audio conference titled, "Privacy Matters: Creating a Systematic Investigation and Reporting Process for Privacy Complaints." The conference speaker, Eva Maria Wood, the Director for Ethics & Compliance Program Assessment for the Hospital Corporation of America, offered providers guidance to improve privacy investigations and risk assessments in preparation for OCR audits. This brief will summarize how organizations should prepare for OCR audits by establishing an internal process to investigate privacy and security matters, conducting risk assessments, and appropriately reporting breaches.

Internal Investigations

One component of OCR reviews will be to determine how the entity investigates privacy and security violations. Accordingly, organizations are encouraged to create an incident response team (IRT) that can detect and respond to HIPAA complaints. The IRT should consist of executives and staff members who have expert knowledge in protecting the privacy and security of PHI. Thus, the IRT may include the organization's Chief Executive Officer, Compliance Officer, Privacy Officer, Security Officer, Risk Director, and General Counsel. The team can also include the director and manager of the personnel involved in the alleged violation. Above all, the members of the IRT must be unbiased in conducting IRT activities.

Once established, the IRT would be responsible for investigating credible allegations of HIPAA violations by interviewing and reviewing documentation related to the complaint. Specifically, the IRT should ensure that an unbiased party carries out the interviews. Further, interview questions must be open-ended and objective to obtain all relevant information. Based on findings from the investigation, the IRT will determine the root cause of the complaint and develop a corrective action plan (CAP) to mitigate privacy and security risks. The CAP should also include sanctions for all responsible parties.

Particularly for OCR audits, the IRT must thoroughly document the team's activities. This documentation should include detailed notes from interviews, findings from medical record reviews, audit results, and CAPs. Organizations can also establish an intake form for IRT investigations to capture important information about the event including, but not limited to:

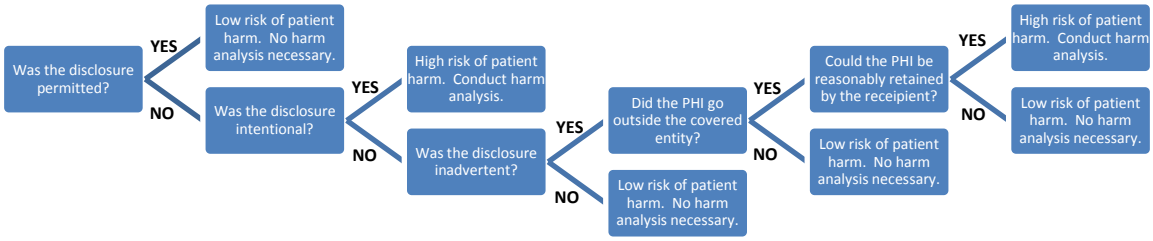
- Complainant's name;
- Patient's name;
- Location of the alleged violation; and
- Summary of the dispute.

An organization may use the IRT as the focal point of the organization's HIPAA compliance efforts if faced with an OCR audit. The IRT would supply OCR with information on the organization's privacy and security investigations and related activities. By documenting all IRT activities, the organization can evidence attempts to mitigate HIPAA risks and resolve any alleged violations.

Risk Assessments

To prepare for OCR audits and improve the privacy and security of PHI, organizations should conduct risk assessments to determine their risks for unauthorized disclosures of PHI. When a disclosure is identified, organizations can use a decision tree to determine the resulting harm to the patient. This decision tree will also assist the organization in determining the appropriate response to an unauthorized disclosure of PHI. An example of a decision tree is provided below in Diagram 1.

Diagram 1: Sample Decision Tree for PHI Disclosures[1]



As illustrated above, not all disclosures of patient information pose serious risks of harm to the patient. For example, when a disclosure is permitted by the entity or the recipient is unable to interpret that PHI, the disclosure poses a low risk of harm to the patient. However, if PHI is disclosed to an individual outside of the organization, the disclosure can pose a high risk of harm to the patient. For disclosures that are likely to cause the patient significant harm, organizations should conduct a patient harm analysis to assess the level of harm to the patient.

The patient harm analysis allows the organization to pinpoint the consequences of the disclosure and determine the appropriate action to alleviate the harm to the patient. When conducting this analysis, the organization should closely assess the disclosure. Organizations should determine who received the disclosed information, and what relationship, if any, the individual has with the patient. For instance, a patient can suffer significant harm if the organization discloses information about the patient's substance abuse history to the patient's employer. The organization should also consider the potential

[1] The sample decision tree is based on information from the HCCA audio conference titled "Privacy Matters: Creating a Systematic Investigation and Reporting Process for Privacy Complaints."

reputational or economic harm to the patient. For example, when sensitive health information is disclosed, such as a terminal illness or sexually transmitted disease, the patient can face significant reputational harm. Moreover, disclosures can pose personal financial risks to the patient if his or her social security number or other identifying information is disclosed. Once the extent of the patient's harm is determined, the organization should take steps to mitigate the harm and take the appropriate disciplinary action against the responsible party. When responding to any breach, the organization should also ensure that adequate safeguards are established to prevent future breaches.

Breach Reporting

Another component of the OCR audit is to ensure that entities properly report breaches to the affected patient(s), government, and media outlets when necessary. OCR will review organizations' responses to breaches and the subsequent steps taken to resolve and report breaches. Therefore, organizations must become familiar with the HITECH breach reporting requirements and update their policies and procedures accordingly.

The HITECH Act established breach notification requirements that entities must follow regardless of the size and impact of the breach. Specifically, organizations must send a notification letter to the affected patient(s) within 60 days from discovery of the breach. The notification letter must provide the patient with the following information:

- Description of the breach, including the date of the breach and the date it was discovered.
- Description of the type of PHI disclosed.
- Details on what the organization has done to investigate, mitigate, and remediate the breach.
- List of steps the affected individual should take to protect themselves from further harm.
- Offer to pay for credit monitoring services if there is potential for financial harm.
- Contact information for the organization, including a toll-free number, email address, and a web or postal address.

Further, the HITECH Act requires entities to report all breaches to HHS. If fewer than 500 patients are affected by the breach, organizations must report the breach to HHS within 60 days after the end of the calendar year. However, if the breach affects 500 or more patients, the report to HHS must be made within 60 days after discovery of the breach. The HITECH Act also requires organizations to notify major media outlets if a breach affects 500 or more patients within the same state or jurisdiction. For example, if a breach involves 600 patients, 300 of whom reside in Georgia and 300 others who reside in Tennessee, the organization would not notify the media. However, if a single breach involves 600 patients who all reside in Georgia, the organization must report that breach to the media. Organizations should review all reporting requirements to ensure strict compliance with the HITECH Act and document their reporting activities in preparation for OCR audits.

Conclusion

As evidenced by the ongoing OCR audit program, the privacy and security of PHI is a growing focus for the federal government. The audits will be based mostly on documentation that demonstrates the organization's compliance with privacy, security, and breach notification standards. Accordingly, health care organizations must reevaluate their policies and procedures related to breaches and unauthorized disclosures of PHI. Organizations should also ensure that all breach responses are documented thoroughly and accurately. This documentation is not only useful to the organization in conducting investigations and resolving privacy and security complaints, but also can eliminate the penalties and

additional government audits that may flow from OCR audits. With adequate preparation to prevent and respond to breaches, organizations can better ensure the privacy and security of PHI.