Making Your Practice HIPAA Compliant

Heather McClane

Indian Health Service

Privacy Officer

HIPAA Privacy Rule

- Privacy Rule went into effect April 14, 2003.
- Privacy refers to the protection of an individual's health care data.
- Defines how patient information can be used and disclosed. (Permitted vs. Required)
- Gives patients privacy rights and more control over their own health information.
- Outlines ways to safeguard Protected Health Information (PHI).

HITECH

- HIPAA and HITECH, are separate and unrelated laws, but they do reinforce each other in certain ways. For example, HITECH stipulates that technologies and technology standards created under HITECH do not compromise HIPAA privacy and security laws.
- It also requires that any physician and hospital that attests to meaningful use, must also have performed a HIPAA security risk assessment as outlined in the Omnibus rule.
- Another example: HITECH established data breach notification rules; HIPAA's omnibus update echoes those rules and adds details such as holding healthcare providers' business associates accountable for the same liability of data breaches as the providers themselves.

Breach

Definition of Breach

- 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 protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Breach Notification Rule

- Individual Notice
- Media Notice
- Notice to the Secretary

http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Administrative Requirements and Burden of Proof

- Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."
- Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Omnibus Rule

- The final rule expands patient rights by allowing them to ask for a copy of their electronic medical record in electronic form.
- Under the final rule, when patients pay out of pocket in full, they can instruct their provider to refrain from sharing information about their treatment with their health plan. Example * If a Medicare beneficiary requests a restriction on the disclosure of PHI to Medicare for a covered service and pays out of pocket for the service, the provider must also restrict the disclosure of PHI regarding the service to Medicare.
- The final rule sets new limits on how information can be used and disclosed for marketing and fundraising purposes, and it prohibits the sale of an individuals' health information without their permission.
- Penalties for noncompliance with the final rule are based on the level of negligence with a maximum penalty of $1.5 million per violation.

Omnibus Rule (cont.)

- The breach notification final rule was amended with a requirement to determine the breach's "risk of compromise" rather than harm. "Compromise" was considered a more objective test than harm. Thus, breach notification is necessary in all situations except those in which the covered entity or business associate demonstrates a low probability that the PHI has been compromised.
- To determine whether there is a low probability that PHI has been compromised, the covered entity or business associate must conduct a risk assessment that considers at least each of the following factors:
- • The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
  • The unauthorized person who used the PHI or to whom the disclosure was made.
  • Whether the PHI was actually acquired or viewed.
  • The extent to which the risk to the PHI has been mitigated.
- Under the final rule, breaches of limited data sets — regardless of their content — must be handled like all other breaches of PHI.
- Providers and covered entities still have a safe harbor, in which an unauthorized disclosure only rises to the level of a breach — thereby triggering notification requirements of the HITECH Act — if the PHI disclosed is "unsecured.“ Unsecured PHI is PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of technology or methodology specified by the secretary through published guidance.

Omnibus Rule (cont.)

- Requirements for methods of breach notification remain unchanged.
- Business associates, or people or organizations that conduct business with the covered entity that involves the use or disclosure of individually identifiable health information, must also provide notice to covered entities no later than 60 days after the discovery of a breach of unsecured PHI.
- Covered entities' Notice of Privacy Practices forms need to inform patients that they will be notified if their PHI is subject to a breach. NPPs must also inform individuals that a covered entity may contact them to raise funds, and the individual has a right to opt out of receiving such communications.
- Business associate agreements and policies and procedures must address the prohibition on the sale of patients' PHI without permission.
- Covered entities must modify and implement policies and procedures that address the new limits on permissible uses of information for marketing and fundraising activities.
- Covered entities' business associate agreements and policies and procedures must address the expanded rights of individuals to restrict disclosures of PHI.

So Where do You Start?

- Gap Analysis

Take a good look at your internal processes, walk through your facility, from front door to back, in every room, follow your PHI from start to finish.

- HIPAA Audit Protocol

Use the OCR HIPAA Audit Protocol annually to ensure you have every policy in place that you need.

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

- Security Risk Assessment – Use the OCR Security Guidance

http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Document and Retain for Six Years

- Document!
- Document!
- Document!
- Document!
- Document!
- Document!
- Document!
- Document!

45 CFR 164.530