Codify
BY AAPC

Health Information Compliance Alert

Toolkit: Use This HIPAA Audit Checklist To Gear Up For Phase 2

Pay special attention to 5 key areas of PHI safeguards.

With the next series of HIPAA audits starting right now, you don't have time to procrastinate in making sure that you're compliant and ready for the **HHS Office for Civil Rights**' (OCR) scrutiny. And if you're selected for a HIPAA audit, OCR will give you mere days to respond and provide requested documents.

That's why you need to run through this checklist now to make sure you're ready for the Phase 2 HIPAA audits. According to a recent report by Cincinnati-based attorney **Paulette Thomas** of **Baker & Hostetler LLP**, the checklist below highlights areas of concern for compliance, and you should evaluate these aspects of your privacy and security plan:

- **Policies and Procedures:** Review and revise your privacy, security, and breach notification policies to ensure that they're current and compliant with the HIPAA Omnibus Final Rule.
- **Individual Right to Access Protected Health Information (PHI):** Review your processes and documentation of requests to ensure timely responses to the individual.
- **Notice of Privacy Practices (NPP):** Review your NPP to ensure that it meets current requirements regarding content and posting (including website posting), and distribution.
- **Workforce Training and Education:** Review your training materials to ensure that they're current and have documentation evidencing training and education on the Privacy and Security Rule standards.
- **Privacy Safeguards:** Review the uses and disclosures of PHI to ensure that you're using and/or disclosing the minimum necessary amount of PHI. Also, review your safeguards for PHI, including these key areas:

  o Use of paper shredders;
  o Copy machines that store data;
  o Physically securing PHI in locked cabinets;
  o Use of whiteboards; and
  o Incidental disclosures.

- **Security Risk Assessment, Analysis, and Management Plan:** Compile documentation evidencing that you've conducted and implemented the risk assessment, the risk analysis, and the risk management plan. Keep in mind that:

o Your risk management plan should include a timeline for implementation of specific security controls for identified risks and vulnerabilities;
o You should conduct a security risk assessment and analysis if it has been some time since you completed one; and
o You should review documentation of specific controls in place to comply with addressable security standards, including the rationale for alternative security measures in place.

- **Transmission security:** Review the security measures you have in place to protect electronic PHI (ePHI) when it's in transit.
- **Encryption and Decryption:** Inventory your devices that contain and transmit ePHI and ensure that the devices are encrypted. If you haven't encrypted all devices, you should have a risk management plan detailing the compensating controls currently in place to mitigate risk of compromise.
- **Device and Media Controls:** Review your policies and procedures for the use, reuse, disposal, storage, and backup of devices and systems containing ePHI.
- **Facility Security Plan:** You must have a facility security plan in place wherever PHI is located. You should

maintain a current inventory of where PHI is located, and have a process in place when purchasing new IT equipment or when acquiring a new business and its existing IT equipment.

- **Breach Notification:** Ensure that your breach notification policy complies with the Breach Notification Rule standard. You should also:

o Make sure that your breach notification policy includes the requirement to notify individuals in a timely manner.
o Maintain documentation of prior breach notifications to demonstrate that you provided notification to individuals in the form of notification letters and substitute notices.
o Review incident response procedures and documentation for security incidents, including response, mitigation, investigation, and determination of a breach requiring notification.

- **Business Associates (BAs):** OCR will request a list of BAs from audited CEs. Compile the list of BAs and the associated BA agreements (BAAs).