Codify
BY AAPC

Health Information Compliance Alert

Business Associates: Take 4 Actions Now To Ensure Your BAs Are Prepared For Security Incidents

Consider conducting security audits to evaluate your BA's security and privacy practices.

Are your business associates (BAs) ready to respond to a HIPAA breach? When it comes to answering this question, what you don't know can hurt you.

According a May 3 Cyber-Awareness Monthly Update from the **HHS Office for Civil Rights** (OCR), covered entities (CEs) and BAs should think about how they'll handle a vendor's or subcontractor's breach.

Problem: Not only do a large percentage of CEs believe they will not be notified of security breaches or cyberattacks by their BAs, they also think it's difficult to manage security incidents involving BAs and impossible to determine if data safeguards and security policies and procedures at their BAs are adequate to respond effectively to a data breach, OCR states.

Solutions: The OCR offers the following tips on making sure that your BAs or subcontractors are prepared for a HIPAA breach or security incident:

1. Include Specifics in Your BAAs

You should consider defining in your service-level or BA agreements (BAAs) how and for what purposes your BA will use or disclose PHI. This is important so that your BA can report to you any PHI use or disclosure that's not provided for in your BAA or vendor contract, including breaches of unsecured PHI and any security incidents.

According to a the **United States Computer Emergency Readiness Team** (US-CERT), cybersecurity incidents may include activity such as:

- Attempts (either failed or successful) to gain unauthorized access to electronic PHI (ePHI) or a system that contains ePHI;
- Unwanted disruption or denial of service to systems that contain ePHI;
- Unauthorized use of a system for the processing or storage of ePHI data; and
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

2. Identify a Timeframe for Breach Reporting

OCR also advises that you define in your BAA the timeframe in which you expect your BA or subcontractors to report a breach, security incident, or cyberattack. Keep in mind that CEs are liable for untimely breach reporting to affected individuals, as well as to OCR and the media.

Rule of thumb: The quicker the incident is reported, the faster a CE or BA can respond, OCR points out. Reporting an incident rapidly can help minimize damages caused by the security incident, protect and prevent further loss of ePHI, preserve evidence for forensic analysis (if necessary), and regain access to and secure your IT systems.

3. Define What You Expect in the Incident Report

Consider identifying in your BAAs the type of information that's required in a breach or security incident report. Your BA or subcontractor should include in such reports:

- BA name and contact information;
- Description of what happened, including the date of the incident and the date of discovery, if known;
- Description of the types of unsecured PHI involved in the incident; and
- Description of what the BA is doing to investigate the incident to protect against any further incidents.

4. Conduct Security Audits on Your BAs

CEs and BAs alike should train their workforce members on incident reporting. You may also want to conduct security audits and assessments to evaluate your BAs' or subcontractors' privacy and security practices. "If not, ePHI or the systems that contain ePHI may be at significant risk," OCR warns.

Resource: To sign up for the OCR's cyber-awareness updates, visit https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-SECURITY-LIST&a=1.