May 3, 2016

OCR Cyber-Awareness Monthly Update

April 2016 Topic: Is Your Business Associate Prepared for a Security Incident?

Despite the requirements of HIPAA, not only do a large percentage of covered entities believe they will not be notified of security breaches or cyberattacks by their business associates, they also think it is difficult to manage security incidents involving business associates, and impossible to determine if data safeguards and security policies and procedures at their business associates are adequate to respond effectively to a data breach.

As such, covered entities and business associates should consider how they will confront a breach at their business associates or subcontractors, respectively. For example, since the Office of Personnel Management (OPM) had a data breach in 2015, OPM has been drafting new contract rules on reporting security incidents for health insurance companies with whom they work.

Covered Entities Should Consider:

1. Defining in their service-level or business associate agreements how and for what purposes PHI shall be used or disclosed in order to report to the covered entity any use of disclosure of PHI not provided for by its contract, including breaches of unsecured PHI, as well as any security incidents.

   HIPAA defines **security incidents** as attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *(See the definition of security incident at 45 CFR 164.304)*. HIPAA also identifies **breaches** as, generally, an impermissible acquisition, access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information. *(See the definition of breach at 45 CFR 164.402).*

   According to the US-CERT, cybersecurity incidents could include the following types of activity, but are not limited to:

   - Attempts (either failed or successful) to gain unauthorized access to 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.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

2. Indicating in the service-level or business associate agreements the time frame they expect business associates or subcontractors to report a breach, security incident, or cyberattack to the covered entity or business associate, respectively. Keep in mind; incident-reporting should be done in a timely manner, and covered entities are liable for untimely HIPAA breach reporting to affected individuals, OCR, and the media, as applicable. The quicker the incident is reported, the faster a covered entity or business associate can respond, possibly:

   - Minimizing the damages caused by the security incident.
   - Protecting and preventing further loss of electronic patient health information.
   - Preserving evidence for forensic analysis, if necessary.
   - Regaining access to and secure information systems.

3. Identifying in the service-level or business associate agreements the type of information that would be required by the business associate or subcontractor to provide in a breach or security incident report. The report should include:

   - Business associate name and point of contact information.
   - Description of what happened, including the date of the incident and the date of the discovery of the incident, if known.
   - Description of the types of unsecured protected health information that were involved in the incident.
   - Description of what the business associate involved is doing to investigate incident and to protect against any further incidents.

4. Finally, covered entities and business associates should train workforce members on incident reporting and may wish to conduct security audits and assessments to evaluate the business associates' or subcontractors' security and privacy practices. If not, ePHI or the systems that contains ePHI may be at significant risk.

Resources:

- **Office of Management and Budget (OMB):** https://policy.cio.gov/ - *(Federal Information Technology contracts)*

- **Office for Civil Rights (OCR):** http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html - *(HIPAA Breach Notification guidance)*

- **United States Computer Emergency Readiness Team (US-CERT)**: https://www.us-cert.gov/ - *(Cybersecurity Incident practices)*