HIPAA Privacy & Security Updates—Phase Two of HIPAA Audits & Recent Enforcement Settlements

From Dorothy Cociu, COIN Editor and HIPAA Privacy & Security Consultant & Trainer

As usual, the Department of Health & Human Services (HHS) and the Office of Civil Rights (OCR) has been very busy with HIPAA Privacy & Security Enforcement. As stated in Privacy & Security CE courses earlier in 2016, HHS announced a series of desk audits, which began earlier this year. Phase Two of those audits began in July, when the first 167 emails were sent to 167 covered entities. As you'll recall, I previously reported that HHS also announced in September, 2015 that they would begin auditing Business Associates, due to the large number of enforcement actions and settlement agreements with Business Associates. As Agents are Business Associates to the employer clients, they can expect to be included in the Desk Audit Process.

The desk audits are an interesting way to perform exponentially more audits than field audits… It's fairly easy to press a button and send emails to hundreds of covered entities at once and sit back and wait for the items to be selected, then review for the highest offenders…. According to OCR, the desk audits focus examinations on documentation of entity compliance with certain requirements of the HIPAA Rules. They selected these provisions for focus "because our pilot audits, as well as our enforcement activities, have surfaced these provisions as frequent areas of noncompliance."

Upon receipt of the email request for information, the selected covered entities must respond to their request through a unique link for each organization to submit documents via OCR's secure online portal. Entities have 10 days to respond to the document requests. ***According to OCR's July 14, 2016 Email Update, desk audits of business associates will follow this fall,*** which may include agents***.***

Requirements selected for desk audits include (Privacy Rule)notices of privacy practices, provision of notice–electronic notice, right to access, (Breach Notification Rule) timeliness of notification, content of notification, and (Security Rule) security management process—risk analysis and security management process, risk management.

So what does all this mean? Agents and their clients should have all of their HIPAA Privacy & Security protocols in place, as well as their forms, notices, policies and procedures, and a complete risk analysis and risk management written plan in place. Remember, they can go back 6 years for federal rules, and 7 years for state rules.

Penalties, Enforcement & Case Settlement Updates

Every month, I receive several email updates from HHS/OCR on their enforcement and settlement results. This summer has been no exception.

June 30, 2016, HHS/OCR announced Business Associate's Failure to Safeguard Nursing Homes Residents' PHI Leads to ***$650,000 HIPAA Settlement.*** Catholic Health Care Services of the Archdiocese of Philadelphia agreed to settle potential violations of the HIPAA Security Rule after a theft of a CHCS mobile device compromised the PHI of hundreds (412) of nursing home residents. The settlement includes a monetary penalty to $650,000 plus a corrective action plan. "Business Associates must implement the protections of the HIPAA Security Rule for the electronic protected health information they create, receive, maintain, or transmit from covered entities" said OCR Director Jocelyn Samuels. "This includes an enterprise-wide risk analysis and corresponding risk management plan, which are the cornerstones o f the HIPAA Security Rule." An investigation found that a theft of an IPhone occurred, which was not encrypted and not password protected. At the time of the incident, SHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident, an they had no risk analysis or risk management plan.

On July 18, 2016, Oregon Health & Science University (OHSU) agreed to settle potential violations when OCR found widespread and diverse problems at OHSU, which resulted in a ***$2,700,000 settlement*** and corrective action plan. *Two unencrypted laptops and an unencrypted thumb drive thefts with over 3,000 individuals at risk of harm, as well as a cloud-service storage without a business associates agreement.*

Another settlement on August 4, 2016 resulted in a ***$5.55 Million settlement*** and corrective actions plan with Advocate Health Care Network for ePHI violations which affected over 4 million individuals. *PHI, credit card information, DOB's and other information were on an unencrypted laptop.*

On August 18, 2016, OCR announced an initiative to investigate breaches with fewer than 500 individuals.##