HIPAA Infractions Result in Huge Penalties

Although the fate of the Affordable Care Act remains undecided, enforcement of the HIPAA privacy & security regula-tions by the Office for Civil Rights (OCR) of the US Dept of Health & Human Services is ongoing, with three settlements & one assessment of penalties already in 2017. The settlements & penalties so far total over $11 million, with one of the settlements equaling the largest ever, at $5.5 million. These four cases provide helpful lessons for covered entities & business associates, as well as warnings that HIPAA compliance might be less expensive than noncompliance.

The smallest settlement so far in 2017 was for $475,000 for paper Protected Health Information (PHI) of over 800 individuals that was "missing" from a health care provider, and for failure to provide breach notices within the regulatory time limits. This is not the first time breach notices were late, but it is the first time OCR has specifically identified late notices as an alleged violation.

The largest settlement so far in 2017 was for $5.5 million. It arose when an employee of a physician practice that was affiliated with the covered entity (a large health care provider) left employment with the affiliate, but the covered entity did not terminate the former employee's access to PHI for over a year, leaving the PHI of about 80,000 individuals available to the individual.

Another large settlement in 2017 was for $2.2 million, & it arose from the theft of a USB device that was left overnight in an insurance company's IT dept & contained the PHI of over 2,200 individuals. OCR alleged that the covered entity failed to conduct an appropriate risk assessment, failed to implement a security awareness & training program for its workforce members, failed to implement an encryption mechanism, & failed to have policies & procedures to comply with the HIPAA security rules.

Finally, a penalty assessment of $3.2 million was imposed against a large medical center that had several HIPAA issues over a period of years, including the loss of an unencrypted phone, theft of an unencrypted laptop from the covered entity's premises and access to PHI given to unauthorized workforce members. OCR found that the covered entity did not act in a timely fashion, despite knowing of the risks presented by the unencrypted devices as early as 2007, and continued to issue such devices until 2013.

Lessons for Covered Entities and Business Associates

These and other recent enforcement actions provide important lessons and reminders, including the following:

- Don't use unsupported software (i.e., out-of-date versions) and apply patches regularly and promptly.
- Continually train your workforce through an aggressive security education and awareness program.
- Train the workforce that idle curiosity (i.e., snooping) is forbidden and a HIPAA violation.
- Pay close attention to Internet scheduling tools, which can present special problems.
- After routine maintenance, always check that firewalls are reactivated and security settings are appropriate.
- Wipe any hard drives (to include copiers and medical devices) before reselling or returning to leasing companies.
- Implement strong policies and procedures and keep them current.
- Implement policy/procedure for taking PHI offsite, handling while offsite and protecting it from others (family members, neighbors, visitors in the home, etc.).
- Never leave a device containing PHI in a vehicle unless the PHI or device is secured (i.e. encrypted).
- Review business associate agreements to make sure they've been updated for legal requirements and any changes in the services to be rendered by the business associate.
- Implement an org info security risk management program and ensure that it goes beyond information technology.

With a total of over $11 million in settlements and penalties already in 2017, this is on pace to be a record year for HIPAA enforcement. Although many covered entities and business associates balk at the cost of HIPAA compliance, HIPAA noncompliance can be even more expensive.

Rick R Ensenbach, CISSP-ISSMP, CISA, CISM, CCSFP
Wipfli LLP
rensenbach@wipfli.com