Can you afford not to investigate a security incident?

By: Alex Mattingly on May 9, 2019 on graydon.law

Many self-funded health plan sponsors are aware that their plans are subject to HIPAA and that they must maintain policies and procedures to comply with the law. But compliance with HIPAA does not stop in the planning phase. As the threat and occurrence of security incidents become more and more common, plan sponsors must be ready to take action when an incident arises. HIPAA's administrative safeguards require covered entities to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes. If the security incident rises to the level of a breach the covered entity also has notification requirements. Failure to satisfy these requirements can have very real consequences to your business.

A **recent HHS settlement** illustrates what can happen if a security incident is not handled properly. In this settlement, a diagnostic medical imaging services company was required to pay $3 million and complete a corrective action plan due to the company's failed handling of a security incident. The company was originally notified of a security incident, exposing PHI of more than 300,000 individuals, by both the FBI and HHS Office for Civil Rights, but inexplicably failed to thoroughly investigate the incident until several months after the notices. Not only did the tardy response violate HIPAA's security incident procedure requirements, but the delayed investigation meant that the company was also unable to timely notify individuals affected by the breach. To make matters worse, the company also failed to have business associate agreements in place with its vendors and had not conducted a risk analysis of potential risks.

This HHS settlement should serve as a reminder to all plan sponsors to revisit their security incident procedures, and should be a wake-up call for those that are not prepared to readily respond. Although no covered entity can be 100% immune from the threat of a breach, preparation today can minimize the extent that a breach will harm your company tomorrow.