Ransomware and HIPAA - What You Need to Know Now

Friday, 3:30pm. Your helpdesk technician calls and, in a slightly panicked tone, tells you that the firm has a ransomware outbreak. You ask a series of questions: Whose computers are affected? Did they encrypt client information? Can you tell if any data was taken from the network? He replies that he only knows of three infected computers. He is running a larger scan now to determine the extent of the outbreak.

Then you remember that your firm has recently signed Business Associate Agreements (“BAA’s”) with two large healthcare clients that provide you with their electronic Protected Health Information (“ePHI”). You hope and pray that none of that information is affected.

He calls back an hour later. The fuller scope of the ransomware attack is becoming clear. Sixteen computers at the firm have been impacted, including several in the practice that handles healthcare clients and the ePHI.

According to a US government interagency report, there have been 4,000 daily ransomware attacks since early 2016, a 300% increase over the 1,000 daily attacks reported in 2015. What does this have to do with your obligations under HIPAA and HITECH? In early July of this year, Health and Human Services (“HHS”) clarified whether or not a ransomware attack counts as a breach or security incident. HHS explained that a security incident is defined as the “attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system (45 C.F.R. 164.304). Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R. 164.308(a)(6).”

What does this mean for a law firm that has signed a BAA? Your first step is to alert your Security Officer (a required role under HIPAA), and your Privacy Officer (not a required role, but one strong recommended for firms), who will know where and how ePHI is stored, whether it’s encrypted, and your next steps. As a Business Associate, you would already need to have created a full data backup plan, another requirement under HIPAA. Your HIPAA Privacy or Compliance Officer would then work with your Director or IT to determine the probability that the ransomware-affected PHI has been compromised by performing the four-factor risk assessment (45 C.F.R. 164.402(2)) m. Based on the four-factor risk assessment results, you would understand which, if any, of your ePHI, is impacted, and if you need to follow your Breach Notification plan.

If, however, like most law firms who are Business Associates under HIPAA, you don’t have a Compliance Officer or Privacy Officer who understands your HIPAA obligations, this is the perfect time to put your HIPAA Compliance Program into place. This includes designating the required roles and corresponding responsibilities under HIPAA, gaining a thorough understanding of your firm’s obligations regarding ePHI, and performing a full risk analysis on your ePHI-related processes and technical infrastructure. While this sounds overwhelming, there are several short-term projects that your firm can undertake to cover significant ground.

Kraft Kennedy’s experts understand not only HIPAA compliance requirements, but also the law firm environment, and we are uniquely positioned to help you put the right program into place.
Author Karen Hornbeck is Director of Information Governance at Kraft Kennedy. To learn more, please contact info@kraftkennedy.com.