July 19, 2016

HHS Issues New Guidance on Ransomware

On July 11, 2016, the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") issued guidance on ransomware attacks. The guidance clarified that a ransomware attack involving electronic protected health information ("ePHI") is presumptively a HIPAA breach unless, as with other types of attacks, the covered entity or business associate can demonstrate that there is a "low probability that the PHI has been compromised" based on the factors provided in the breach notification rule and additional factors particularly relevant to ransomware. Notably, the guidance does not state whether there are instances in which an affected covered entity or business associate should pay the ransom to attempt to regain access to seized information.

Ransomware is a unique type of malicious software that denies access to a user's data by encrypting the data with a key known only by the hacker who deployed the ransomware. A ransomware attack is usually followed by the perpetrator's demand that the user pay a ransom to receive the decryption key. According to the guidance, since early 2016, there have been, on average, 4,000 ransomware attacks each day.

The guidance states that "whether or not the presence of ransomware would be a breach under the HIPAA rules is a fact-specific determination." Under the HIPAA rules, a breach is defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information." 45 C.F.R. § 164.402. According to OCR, "when ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (*i.e.*, unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule. In order to overcome the presumption of breach (and avoid notification required under the HIPAA rules), the covered entity or business associate must conclude, after conducting a risk assessment, that there is a low probability that the PHI has been compromised despite the ransomware attack. The HIPAA Privacy Rule requires that this risk assessment consider at least the following four factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI actually was acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

   45 C.F.R. § 164.402.

The guidance encourages entities "to consider additional factors, as needed, to appropriately evaluate the risk that the PHI has been compromised." Specifically, the guidance suggests two additional factors particularly relevant to ransomware attacks:

1. Whether there is a high risk that the data will be unavailable; and

2. Whether there is a high risk that data's integrity has been compromised.

If analysis under these factors suggests that there is more than a low probability that PHI has been compromised, the guidance requires that entities "provide notification to individuals without unreasonable delay, particularly given that any delay may impact healthcare service and patient safety."

The guidance also suggests that an entity's implementation of "robust contingency plans, including disaster recovery and data backup plans," may help it demonstrate that the ransomware attack had limited impact upon data integrity. After implementing contingency plans, "[t]est restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities." However, the guidance makes clear that integrity of PHI data is only one aspect in determining whether there is a low probability of compromise. The entity must also consider other aspects, such as whether PHI has been exfiltrated.

Because the HIPAA breach notifications apply to only "unsecured PHI," there has been some question as to whether a breach notification is required for ransomware attacks on encrypted data. According to the guidance, if the PHI is encrypted in a manner consistent with OCR's *Guidance to Render Unsecured Protected Health Information, Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, then the entity is not required to conduct a risk assessment to determine if there is a low probability of compromise, and a breach notification is not required. However, the guidance warns that additional analysis may be required to ensure that all affected PHI was encrypted in a manner that rendered it "unreadable, unusable and indecipherable to unauthorized persons." As an example of a situation in which additional analysis would be required, the guidance points to entities that use full-disk encryption as the only method of protecting PHI on employee laptop computers. If ransomware infected a laptop that already was powered on and authenticated, the seized data would not be encrypted. In that case, despite some manner of encryption, a breach would be presumed and notification would be required, unless the entity otherwise could demonstrate "a low probability of compromise of the PHI," under the factor-based risk assessment described above.

As covered entities and business associates consider modifications to their data security procedures in light of the OCR ransomware guidance, it is important to remember that state laws, with increasingly robust standards, may impose additional requirements. If you have any questions, please contact a member of our privacy & data security team or your usual Ropes & Gray advisor.