Health Information Compliance Alert

Ransomware: When Ransomware Attacks, Here's What You Must Do

Does your breach represent a 'low probability' of compromised data?

With more than 4,000 daily attacks since early 2016 (up 300 percent from 2015), ransomware is one of the biggest current threats to health information privacy. And, with the release of much-anticipated guidance on the topic,

HHS's Office of Civil Rights finally appears to be taking it seriously with the release of new breach reporting guidance.

But while the new guidance is meant to help health care entities better understand and respond to the threat of ransomware, it also provides a serious heads up to providers and insurers that no breach of data is too small. That is, almost no breach of data is too small.

Organizations must notify affected individuals per HIPAA regulations ASAP and then determine if patient information was acquired or viewed, the extent to which data loss was mitigated, and to whom the disclosure was made. But what does that mean exactly?

The Demands

HIPAA-covered entities and business associates are required to develop and implement security incident procedures and response and reporting processes that are "reasonable and appropriate" to respond to malware and other security incidents.

The new OCR guidance reinforces activities HIPAA already requires that can help organizations prevent, detect, contain, and respond to threats, including:

- Conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and establishing a plan to mitigate or remediate those identified risks;
- Implementing procedures to safeguard against malicious software;
- Training authorized users on detecting malicious software and reporting such detections;
- Limiting access to ePHI to only those persons or software programs requiring access; and
- Maintaining an overall contingency plan that includes disaster recovery, emergency operations, frequent data backups, and test restorations.

Hold on to Your Breaches

The new guidance makes clear that HIPAA defines a breach as "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."

Unless the covered entity or business associate can demonstrate that there is a "low probability" that the PHI has been compromised, a PHI breach has occurred, the OCR guidance explains.

Demonstrating that there is "low probability" that the breach has compromised PHI is tougher than it seems. OCR requires that a risk assessment considering at least the following four factors be conducted:

- "the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- the unauthorized person who used the PHI or to whom the disclosure was made;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI has been mitigated."

Bottom Line: The risk assessment to determine whether there is a low probability of compromise of the PHI must be

thorough, completed in good faith, and reach conclusions that are reasonable given the circumstances.

To Notify or Not to Notify?

Not sure whether it's a breach or not? Consider these examples from the OCR guidance:

Low probability of breach: A laptop that has a full disk encryption solution is properly shut down and powered off and then lost or stolen. In this case, the data on the laptop is "unreadable, unusable and indecipherable to anyone other than the authenticated user," the guidance explains.

Higher probability of breach: An authenticated user powers on and uses the laptop. He then clicks on a link to a malicious website that infects the laptop with ransomware. In this case, the likelihood of a breach is higher because the PHI was decrypted and thus "unsecured PHI" when the ransomware accessed the file.

Editor's Note: To read the OCR's guidance on ransomware, go to: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.