OCR Issues New Guidance on Ransomware and HIPAA

Matthew M. Brohm and Elizabeth A. Mulkey

In response to a rising number of ransomware attacks on healthcare systems, the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) has issued new ransomware guidance on the HIPAA obligations of healthcare organizations and business associates.[1] The Fact Sheet provides guidance for covered entities on how to determine whether a ransomware incident is a reportable HIPAA breach, as well as the steps these entities should take to minimize the introduction of malware. We have summarized the guidance below.

Ransomware, a type of malicious software, is used to encrypt a user's data. The hacker using the ransomware will typically make a demand to the user to pay a ransom in order to decrypt the information. However, the hacker may also destroy or transfer the information to another system. According to a recent interagency report cited in the guidance, there have been, on average, 4,000 daily ransomware attacks since early 2016 (which is a 300% increase over the 1,000 daily attacks reported in 2015).

OCR notes that the HIPAA Security Rule requires covered entities and business associates to take steps that can reduce the likelihood of a ransomware attack. For example, entities must conduct a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and put in place procedures to guard against malicious software. Additionally, system users should be trained to recognize and report malicious software. Though an entity may not be alerted to a ransomware attack until after the ransom demand is made, users who recognize indicators of an attack can activate a security incident response plan more quickly.

The HIPAA Security Rule also requires covered entities and business associates to implement policies and procedures to respond and recover from a ransomware attack. Since ransomware can encrypt and delete data, the guidance advises maintaining frequent backups of records and periodically testing to ensure that the backup records are readable. Some ransomware can disrupt online backups, so OCR recommends maintaining backups offline and unavailable from other networks.

This guidance clarifies that ransomware on a covered entity's computer systems is a security incident under the HIPAA Security Rule. A security incident is "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system," and it triggers an entity's response and reporting procedures. Entities must have "reasonable and appropriate" procedures and reporting processes in place to respond to security incidents. Initially, an entity needs to determine the scope of the incident, where it originated, whether the incident is ongoing, and how the incident occurred. Ultimately, a key part of the incident analysis is assessing whether or not there was a breach of PHI.

According to OCR, "whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination."[2] When PHI is encrypted through a ransomware attack, an unauthorized party has taken possession or control of the information, causing an

1 Fact Sheet: Ransomware and HIPAA, Department of Health and Human Services, Office of Civil Rights, available at http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last accessed July 18, 2016).

2 A breach is defined 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." See 45 C.F.R. 164.402.

unpermitted "disclosure." Notably, OCR states that a ransomware incident creates a presumption that a breach has occurred, meaning that an entity must comply with the applicable breach notification provisions ("notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements").[3]

An entity may be able to demonstrate that there is a "low probability that the PHI has been compromised," and a breach notification would not be required. To do so, the entity must conduct a risk assessment involving 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 was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

Entities can consider additional factors in this analysis.For example, if there is a high risk of unavailability or of a risk to the integrity of the data, that may weigh more heavily towards a compromise of the PHI. Again, OCR emphasizes that a robust contingency plan is key to mitigating risk to PHI (the fourth factor in the risk assessment). Without data backup and restoration, an entity may not be able to verify that the risk has been mitigated. When conducting the risk analysis, the entity must do so in good faith, engage in a thorough assessment, reach conclusions that are reasonable given the circumstances, and maintain supporting documentation sufficient to meet the burden of proof on those conclusions.

Overall, this guidance emphasizes best practices to minimize the risk and damage associated with a ransomware attack. Healthcare systems must also have the appropriate security incident procedures in place before an incident occurs; following a robust plan can help mitigate the ultimate risk of compromising PHI. HHS has identified ransomware as "one of the biggest current threats to health information privacy," and with the release of the new guidance, the government has set clear expectations for the safeguards covered entities and business associates must implement.[4]

3 See 45 C.F.R. 164.400-414.

4 Your Money or Your PHI: New Guidance on Ransomware, Jocelyn Samuels, OCR Director, July 11, 2016, available at http://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html(last accessed July 18, 2016).

Authors and Contributors

Matthew M. Brohm
Partner, Atlanta Office
404.873.8740
matt.brohm@agg.com

Elizabeth A. Mulkey
Associate, DC Office
202.677.4906
elizabeth.mulkey@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**