King & Spalding
Client Alert

JUNE 14, 2021

For more information, contact:

Marcia Augsburger
+1 916 312 4803
maugsburger@kslaw.com

King & Spalding

Sacramento
621 Capitol Mall
Suite 1500
Sacramento, CA 95814
Tel: +1 916 321 4800

OCR Updates Ransomware Guidance

On June 9, 2021, OCR distributed an update to those on its Privacy List sharing links to alerts and resources for addressing the growing number and size of ransomware incidents. One such resource included a White House memo dated June 2, 2021 from Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology titled, "What We Urge You To Do To Protect Against The Threat of Ransomware" (the White House Memo). The White House Memo describes the following as best practices to significantly reduce the risk of a successful cyber-attack:

Backup your data, system images, and configurations, regularly test them, and keep the backups offline: Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.

Update and patch systems promptly: This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program.

Test your incident response plan: There's nothing that shows the gaps in plans more than testing them. Run through some core questions and use those to build an incident response plan: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?

Check Your Security Team's Work: Use a 3rd party pen tester to test the security of your systems and your ability to defend against a sophisticated attack. Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors.

Segment your networks: There's been a recent shift in ransomware attacks – from stealing data to disrupting operations. It's critically important that your corporate business functions and manufacturing/production operations are separated and that you carefully filter and limit internet access to operational networks, identify links between these networks and develop workarounds or manual controls to ensure ICS networks can be isolated and continue operating if your corporate network is compromised. Regularly test contingency plans such as manual controls so that safety critical functions can be maintained during a cyber incident.

The OCR notice also provided various additional resources, including its Fact Sheet: Ransomware and HIPAA (OCR Fact Sheet), which was designed specifically for entities regulated by HIPAA. The OCR Fact Sheet reminds such entities that "the Security Rule simply establishes a floor, or minimum requirements, for the security of ePHI; entities are permitted (and encouraged) to implement additional and/or more stringent security measures above what they determine to be required by Security Rule standards." Therefore, OCR admonishes, entities must, for example, update the firmware of network devices, especially when firmware updates are available to remediate known security vulnerabilities.

The OCR Fact Sheet also instructs that "[b]ecause ransomware denies access to data, maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack." Additionally, entities should conduct test restorations periodically to verify the integrity of backed up data and their data restoration capabilities. Maintaining backups offline and unavailable from their networks is a practical suggestion for avoiding the removal or disruption of online backups by ransomware attackers.

The OCR Fact Sheet notes that the presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. *See* 45 C.F.R. § 164.308(a)(6) (defining "security incident" as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.) Thus, once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. Such procedures must be, OCR states, what the entities "believe are reasonable and appropriate to respond to malware and other security incidents, including ransomware attacks." Entities seeking guidance on this may review NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

Of course, a security incident is not necessarily a reportable breach; OCR emphasized that this would depend on the facts and circumstances of the attack. Where ransomware is present in a covered entities' or business associates' system, an assessment must be conducted as to whether or not (1) the incident constitutes an impermissible disclosure of PHI in violation of the Privacy Rule, *see* 45 C.F.R. § 160.103, and (2) a breach under 45 C.F.R. § 164.402. An impermissible disclosure would occur, for example, when electronic protected health information (ePHI) is encrypted and held for ransom by the attacker because the ePHI was acquired and disclosed (i.e., unauthorized individuals have taken possession or control of the information), but the disclosure would not rise to the level of a breach if the covered entity or business associate can demonstrate that there is a "… low probability that the PHI has been compromised." See 45 C.F.R. 164.402(2).

In determining whether the probability of compromise of ePHI is low, entities are encouraged to go beyond considering the factors described in the statute. OCR suggested considering, for example, whether there is high risk of unavailability of the data or to the integrity of the data. These, OCR warned, "may indicate compromise."

OCR offered guidance for performing a ransomware risk assessment that incidentally offers suggestions for establishing a low probability of compromise. OCR explained that correctly identifying the malware involved and understanding what it is programmed to do can assist an entity to determine what algorithmic steps the malware is programmed to perform, how or whether a particular malware variant may laterally propagate throughout an entity's enterprise, what types of data the malware is searching for, and whether or not the malware may attempt to exfiltrate data or exploit vulnerabilities, among

other factors. Such an investigation may show that the malware is not designed to compromise ePHI and/or otherwise establish a low probability that the ePHI was compromised.

OCR also tackled the question of whether a reportable breach occurs if the ePHI encrypted by the ransomware was already encrypted. Emphasizing that the determination is fact specific, OCR acknowledged that if the ePHI is encrypted "in a manner consistent with the Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, of 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 breach notification is not required." However, OCR warned, even if the PHI is so encrypted, additional analysis may still be required to ensure that the encryption has in fact rendered the affected PHI unreadable, unusable and indecipherable to unauthorized persons. This includes not only considering the encryption algorithm, but also additional areas such as encryption methodologies (e.g., full disk, virtual disk/volume, folder/file), cryptographic key management, and pre-boot authentication, where applicable, as contemplated by NIST SP 800-111.

Marcia Augsburger is a partner in King & Spalding's healthcare, privacy, and digital health practices, with certifications in healthcare and privacy compliance