SHEARMAN & STERLING LLP

CLIENT PUBLICATION

Privacy & Data Protection | August 9, 2016

HHS Releases Guidance on Privacy and Security Audits and Ransomware

If your organization operates in the healthcare industry, particularly if it qualifies as a covered entity or business associate under the Health Insurance Portability and Accountability Act (HIPAA), you may have noticed the recent flurry of activity from the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR). First, HHS has recently launched phase two of its three-part audit of compliance with HIPAA privacy, security and breach notification rules. Second, HHS has provided guidance on ransomware which states that the presence of ransomware is a "security incident," which triggers breach disclosure obligations. Organizations subject to HIPAA should review its security incident procedures in light of the upcoming audits and the ransomware guidance and even entities outside the healthcare industry may also benefit from reviewing these guidance documents since other agencies and governmental authorities may follow HHS's lead in these interpretations.

HHS OCR Phase Two Audits Focus on Privacy, Security and Breach Notification Rules

Last month, the HHS Office of Civil Rights officially launched phase two of its HIPAA audit program, sending out notification letters to 167 selected covered entities. In an effort to provide the selected covered entities with greater understanding of the audit process, HHS recently posted guidance on its website in the form of a FAQ. According to the FAQ, the purpose of these audits is to provide HHS "an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews, and enable us to get out in front of problems before they result in breaches."

The desk audit program has already begun. Those covered entities selected to participate in desk audits received letters from HHS on July 11th via email. HHS advises covered entities to check their spam and junk mail filter to ensure that communications from HHS are not inadvertently deleted. Although every covered entity is eligible for selection to participate in the desk audits, OCR is endeavoring to select entities that represent a wide range of health care providers, health plans, health care clearinghouses and (for the desk audits commencing in the fall) business associates. The current set of desk audits will examine compliance with specific requirements of HIPAA Privacy, Security and/or Breach Notification Rules. Those selected for audit will receive document request letters from HHS, outlining the specific subject of the audit.

How the desk audit program works. Per HHS's FAQ, the audit process for phase two will employ common audit techniques. HHS will send request to those entities selected for audit to provide certain specified documents and other data. Those audited entities will then be required to submit the requested documents and data through a new secure audit portal on HHS's website within 10 business days of the date of HHS's request. HHS auditors will review the submitted documentation and then share their draft findings with the audited entity. The audited entity

will then have 10 business days to respond in writing to the HHS auditor's draft findings. The auditor will have 30 business days to complete the final audit report following the audited entity's response. The final audit report will describe how HHS conducted the audit, discuss any findings, and include the audited entity's responses to the draft findings. HHS will share a copy of the final report with the audited entity.

Onsite audits. Following the conclusion of all desk audits at the end of this calendar year, HHS will commence a third set of audits which will be onsite and examine a broader scope of requirements from the HIPAA rules than the desk audits. HHS has stated that entities selected for desk audits may be subject to these subsequent onsite audits. Entities selected for onsite audits will be notified via email of their selection and each onsite audit will be conducted over 3 to 5 days onsite, depending on the size of the entity. As with the desk audits, audited entities will have 10 business days to review and provide written comments to the draft findings of the HHS auditor, the auditor will complete a final audit report within 30 business days of the audited entity's response, and HHS will share a copy of the final report with the audited entity.

What happens after the audit. If an audit report indicates a serious compliance issue for an audited entity, HHS may initiate a compliance review. Although HHS will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity, HHS may be required to release audit notification letters and other information about these audits pursuant to a Freedom of Information Act request. HHS will aggregate data from all final reports and will use that information to determine what types of technical assistance should be developed and what types of corrective action would be most helpful. HHS will also develop tools and issue guidance to assist the industry in compliance with HIPAA requirements.

How to Prepare for an Audit

All covered entities and business associates should be prepared for an audit by HHS. Covered entities and business associates should review their privacy, security and breach notification policies and practices. In particular, they should confirm their compliance with the following HIPAA requirements:

- Notice of Privacy Practices. Organizations must provide printed copies of the organization's current privacy notice to patients and make this notice available on the organization's website. These notices must include their effective date as well as: (a) how the organization may use and disclose protected health information (PHI); (b) the patient's rights with respect to PHI and how the patient may exercise these rights, including how the patient may complain to the organization; (c) the organization's legal duties with respect to PHI, including a statement that the covered entity is required by law to maintain the privacy of PHI; and (d) a contact for further information about the organization's privacy policies.
- Written HIPAA policies and procedures. An organization's HIPAA policies and procedures should conform with the administrative, technical and physical safeguards promulgated by HHS and should identify any risks or vulnerabilities in the organization's collection, storage or use of PHI. The organization should implement safeguards for all paper, electronic and verbal PHI, including PHI on mobile devices and storage media.
- Risk assessment. Organizations should both conduct risk assessments and promptly implement appropriate security measures to address any identified risks. These assessments should include, at a minimum, an evaluation of the likelihood and impact of potential risks to PHI, documentation of the organization's security

measures and, where required, the rationale for adopting such measures. Organizations must also conduct periodic follow-up security risk assessments to identify, address and document any deficiencies so as to maintain continuous, reasonable and appropriate security protections. And in light of HHS's new guidance on ransomware (discussed below), organizations should include the threat posed by ransomware attacks in their security assessments.

- Breach Procedures. Organizations must implement notification policies and procedures that conform to HIPAA requirements for breaches of unprotected PHI (including HHS guidelines for breaches affecting 500 or more individuals). Organizations should conduct training for new employees and ongoing training for all staff on how to appropriately respond to a security breach.

Key Takeaways

- *Audit guidance is important for all covered entities and business associates*. HHS has stressed that its guidance for phase two audits "should be helpful to audited entities as well as other covered entities and business associates seeking assistance with improving their compliance with these important requirements of the HIPAA Rules."
- *Your organization may still be selected for an audit*. Phase two audits, including both desk audits and onsite audits, will continue throughout this year. Even if your organization is not selected to participate in a phase two audit, phase three audits are just around the corner.
- *Organizations should be prepared for an audit*. All covered entities and business associates should carefully review their policies and procedures for compliance with HIPAA rules. Particular attention should be paid to compliance with the Security Rule.

Guidance on Ransomware

In addition to the FAQ on the phase two desk audits, HHS Office of Civil Rights released important new guidance on how to protect against and respond to ransomware attacks. Citing cyber-attacks on electronic health information systems as "one of the biggest current threats to health information privacy," the new guidance issued by HHS in July 2016 reinforces activities required by HIPAA to help organizations prevent, detect, contain and respond to ransomware.

And while only organizations subject to the HIPAA Security Rule are obligated to comply with this guidance, other entities which may be targeted by ransomware can also benefit from reviewing these requirements since it is likely that other agencies and governmental authorities will follow HHS's lead.

What is ransomware? Ransomware is a type of malicious software that prevents or limits users from accessing their own system, either by locking the system's screen or by encrypting the user's files. Users are then forced to pay a ransom (hence the term "ransomware") in order to regain access to their system. Though ransomware is a serious threat to any organization, for healthcare entities who deal with medical emergencies on a daily basis, even a few hours of system downtime can be potentially life-threatening. These healthcare entities are then often forced to pay the ransom, thereby encouraging future attacks on similar organizations. And there has indeed been a sharp increase in the number of ransomware attacks on hospitals and other covered entities over the past few years. The

HHS Guidance cites to a recent US Government interagency report which indicates that there have been 4,000 daily ransomware attacks since early 2016, compared to 1,000 daily ransomware attacks reported in 2015. With the threat of ransomware growing, OCR has issued new guidance to better protect patients.

Ransomware attacks are security incidents. The key takeaway from OCR's guidance is that ransomware attacks will generally be considered a security incident under the HIPAA Security Rule. A breach is presumed to have occurred unless the covered entity or business associate can demonstrate a low probability that protected health information has been compromised. Thus, organizations subject to the HIPAA Security Rule that suffer from a ransomware attack must comply with the Security Rule breach notification requirements, including the requirement to notify the affected individuals, the Secretary of HHS and in certain cases the media if it affects more than 500 individuals.

Breach notification requirements may be avoided in certain cases. As noted above, HHS's guidance does allow for organizations to demonstrate that there is a low probability of protected health information having been compromised, thereby avoiding the breach notification obligations. To do this, these organizations must conduct a risk assessment by considering four factors: (a) the nature and extent of the protected health information involved; (b) the unauthorized person who used the PHI or to whom the disclosure was made; (c) whether PHI was actually acquired or viewed; and (d) the extent to which the risk to PHI has been mitigated. Furthermore, HHS's guidance encourages organizations "to consider additional factors, as needed, to appropriately evaluate the risk that the PHI has been compromised." This risk assessment must be thorough, completed in good faith and reach conclusions that are reasonable given the circumstances. Additionally, organizations must maintain sufficient documentation supporting their conclusions.

Organizations must prepare for attacks. In addition, HHS's guidance also requires organizations to proactively implement policies and procedures that will help it respond to and recover from a ransomware attack. These policies and procedures include: (a) implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to ePHI and implementing security measures to mitigate or remediate those identified risks; (b) implementing procedures to guard against and detect malicious software; (c) training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and (d) implementing access controls to limit access to ePHI to only those persons or software programs requiring access.

OCR further reminds organizations that "the Security Rule includes requirements for all covered entities and business associates to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of all of the ePHI the entities create, receive, maintain or transmit and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level." It is therefore incumbent on organizations to address the threat posed by ransomware in their risk assessments. It is not enough to simply respond to ransomware and report them as security incidents; organizations must be prepared to prevent, detect and contain them as security threats.

Key Takeaways

- *Ransomware attacks pose a serious threat, and they are increasing*. Ransomware attacks are often successful and they are increasingly targeting hospitals and other entities in the healthcare industry. For many covered entities and business associates, the question is "when" and not "if" they will be attacked with ransomware.
- *Ransomware attacks are considered a security incident under the HIPAA Security Rule*. When a covered entity or business associate suffers a ransomware attack, a breach is presumed to have occurred unless that organization can demonstrate a low probability that protected health information has been compromised. This will trigger a requirement for the victim entities to notify individuals whose information is involved in the breach "without unreasonable delay" and in no case later than 60 days following the discovery of the breach. Breach notification rules may also require notice to the HHS Secretary and the media.
- *Organizations must prepare for attacks*. HHS's new guidance requires all covered entities and business associates to implement policies and procedures addressing ransomware attacks. All such organizations should carefully review their policies and procedures to ensure compliance with this new guidance.
- *Organizations in all sectors can benefit from reviewing the HHS requirements.* Once a major agency like HHS defines an obligation to detect, prevent, combat and report ransomware attacks, other regulatory agencies may also follow suit in issuing similar guidance.

CONTACTS

Richard C. Hsu
Menlo Park
+1.650.838.3774
richard.hsu@shearman.com

Jeewon Kim Serrato
Washington, DC
+1.202.508.8032
jeewon.serrato@shearman.com

Robert Masella
New York
+1..212.848.5125
robert.masella@shearman.com

Alan Seem
Menlo Park
+1.650.838.3753
alan.seem@shearman.com

Benjamin Petersen
Menlo Park
+1.650.838.3600
benjamin.petersen@shearman.com

401 9th Street, NW | Suite 800 | Washington, DC | 20004-2128