ECKERT SEAMANS ATTORNEYS AT LAW

November 2024

Cybersecurity, Data Protection &Privacy Update

U.S. Department of Health and Human Services Issues First Enforcement Action Under HIPAA Security Rule Risk Analysis Initiative

By Matthew H. Meade, Laura A. Decker and Gregory P. Mazmanian

OVERVIEW

Covered Entities that are regulated in whole or in part by HIPAA need to be aware of a recent enforcement action against a county ambulance authority which was clearly designed to put covered entities, big and small, on notice of the importance of paying close attention to the Security Rule requirements under HIPAA.

WHAT HAPPENED

On October 31, 2024, the U.S. Department of Health and Human Services ("HHS"), Office of Civil Rights ("OCR"), the division within HHS tasked with enforcing the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including the Security Rule and Privacy Rule, announced it had reached a settlement with an Oklahoma county ambulance authority that experienced a breach of electronic Protected Health Information ("ePHI") due to a ransomware attack. The impacted ambulance authority files contained the ePHI of approximately 14,273 patients. OCR fined the community ambulance authority $90,000 for a violation of the Security Rule and cited to the community ambulance authority's failure to conduct a HIPAA required Risk Analysis. The media release specifically mentions OCR's **Risk Analysis Initiative** as a basis for the enforcement action:

> "Since 2018, there has been a 264% increase in large breaches reported to OCR involving ransomware attacks. The settlement also marks the first enforcement action in OCR's Risk Analysis Initiative. This enforcement initiative was created to focus select investigations on compliance with the HIPAA Security Rule Risk Analysis provision, a key Security Rule requirement, and the foundation for effective cybersecurity and the protection of electronic protected health information (ePHI).
>
> 'Failure to conduct a HIPAA Security Rule risk analysis leaves health care entities vulnerable to cyberattacks, such as ransomware. Knowing where your ePHI is held and the security measures in place to protect that information is essential for compliance with HIPAA,' said OCR Director Melanie Fontes Rainer. 'OCR created the Risk Analysis Initiative to increase the number of completed investigations and highlight the need for more attention and better compliance with this Security Rule requirement.'"

WHAT THE SECURITY RULE REQUIRES

Covered entities, regardless of size, must be aware of its HIPAA compliance obligations and specific attention should be paid to the Administrative Safeguards section given OCR's Risk Analysis Initiative. The HIPAA

Security Rule[1] provides the requirements that covered entities, including health plans, healthcare providers, health care clearing houses, and business associates, must follow to protect ePHI in order to safeguard against a breach. As this settlement makes clear, even a small emergency medical services entity with just one facility in the county must adhere to the requirements of HIPAA[2]"

To prevent breaches of ePHI, the Security Rule requires covered entities undertake certain proactive measures, and failure to take these steps can lead to fines in the event of a breach. Under the Administrative Safeguards[3] section, the Security Rule requires that covered entities must "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."[4] Additionally, the Security Rule requires that a covered entity to "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [HIPAA required security standards[5]]."[6]

Here, under the agreed upon corrective action plan, OCR required the county ambulance authority to take the following steps to ensure compliance with the HIPAA Security Rule and protect the security of ePHI:

- Conducting an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Implementing a risk management plan to address and mitigate security risks and vulnerabilities identified in their risk analysis;
- Developing, maintaining, and revising, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Training its workforce on its HIPAA policies and procedures.

WHAT AN ORGANIZATION CAN EXPECT IN AN INVESTIGATION

Once an organization reports a HIPAA breach with five hundred (500) or more impacted individuals it should expect to receive a written data request from the regional OCR office. A data request is a list of questions which require responses in writing with accompanying supporting documentation that demonstrate compliance with the requirements under HIPAA. Specific to the Risk Analysis Initiative, below are questions that an entity can expect to receive in an OCR data request:

1. A copy of the most recent comprehensive and detailed enterprise-wide risk analysis performed for or by the Covered Entity prior to the incident, and copies of any conducted after the incident pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(A).
    a. If a written risk analysis was not completed for the relevant period, please state the reason one was not documented.
    b. Did the scope of risk analysis cover personal devices and media used for storing ePHI?
    c. Was the risk analysis updated as a result of the incident?

---

1 *See* 45 CFR §§160 &164. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.
2 *See* 45 CFR § 164.402.
3 *Id.* at § 164.308.
4 *Id.* at § 164.308(a)(1)(ii)(A).
5 *Id.* at § 164.306.
6 *Id.* at § 164.308(a)(1)(ii)(B).

2. Provide a copy of the most recent enterprise-wide risk management at the time of the incident as evidence of security measures implemented to reduce risks and vulnerabilities identified through the risk analysis and/or evaluations. Make sure to include date(s) of completion or estimated date(s) of completion pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(B).

Additionally, a data request from OCR will require that a covered entity provide OCR with its HIPAA policies that ensure compliance with protecting ePHI. Typically, OCR will give an organization thirty (30) days to respond to the data request, but an extension may be requested. After the response is submitted, OCR may continue to follow up with additional questions as they investigate the incident and the safeguards and policies in place prior to the incident and steps taken post incident.

MOVING FORWARD AND HOW WE CAN HELP

All covered entities should confirm that they have met and are continuing to meet the requirements under HIPAA including the Security Rule and Privacy Rule, but special attention should be paid to the Risk Analysis requirement. To assist with Risk Analysis requirement, on November 1, 2024, OCR released its latest version of the Security Risk Assessment ("SRA") Tool. "The [SRA] tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule. The target audience of this tool is medium and small providers ...".[7] Covered Entities should consider utilizing this tool to perform a risk analysis or working with third party experts to complete the risk assessment as soon as possible. If you have questions or would like assistance with HIPAA compliance, including updating or writing policies, please reach out to us below.

RESOURCES

- HIPAA Administrative Simplification, Combined Regulation Text, 45 CFR § 160, 162, & 164, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.
- HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation for $90,000, https://www.hhs.gov/about/news/2024/10/31/hhs-office-for-civil-rights-settles-hipaa-ransomware-cybersecurity-investigation-for-90000-dollars.html.
- HIPAA for Professionals, https://www.hhs.gov/hipaa/for-professionals/index.html.
- The HIPAA Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/index.html.
- The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
- The Security Risk Assessment Tool, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

ECKERT SEAMANS ATTORNEYS AT LAW

This Cybersecurity, Data Protection & Privacy Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Laura Decker at 215.851.6623 or ldecker@eckertseamans.com, or Gregory Mazmanian at 215-851-8439 or gmazmanian@eckertseamans.com, a member of our Cybersecurity, Data Protection & Privacy Practice Group, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.

[7] *See* https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.