UNAUTHORIZED ACCESS TO EPHI ON WEB SERVER LEADS TO $875,000 SETTLEMENT

The United States Department of Health and Human Services Office for Civil Rights ("OCR") announced a settlement with a research university ("University") which has agreed to pay $875,000 to settle potential violations of the HIPAA Privacy, Security and Breach Notification Rules, as well as to take corrective action after an unauthorized third party gained access to a web server that contained electronic protected health information ("ePHI").

In January 2018, the University notified OCR of a breach of ePHI that affected 279,865 individuals and occurred in November 2017. This breach occurred when a hacker gained access to a web server by uploading malware. The web server contained ePHI, including patients' names, Medicaid numbers, health care provider names, dates of service, dates of birth, addresses and treatment information.

In addition to this breach, the University later reported that a hacker had previously accessed the same web server as early as March of 2016. The University did not report this breach at the time, because it was not aware that ePHI was stored on the web server in 2016.

OCR found indications that the University was noncompliant in a multitude of Privacy, Security and Breach Notification Rules. These include:

- Impermissible uses and disclosures of PHI;
- Failure to conduct an accurate and thorough risk analysis;
- Failure to perform an evaluation establishing the extent to which the covered entity's security policies and procedures meet the requirements of the Security Rule;
- Failures to implement audit controls, security incident response and reporting; and
- Failure to provide timely breach notification to affected individuals and HHS.

In addition to the $875,000 settlement, the University has agreed to comply with a Corrective Action Plan ("CAP") for a period of two years. The CAP includes obligations to:

- Conduct a comprehensive risk analysis of any security threats that may involve ePHI;
- Create a risk management plan according to the risk analysis findings;
- Develop, maintain, and distribute policies and procedures to comply with the Federal standards that govern the privacy and security of PHI;
- Report any noncompliance of the policies and procedures to OCR after training all members of the workforce; and
- Appoint a person or entity to monitor the compliance of the CAP.

PRACTICAL TAKEAWAYS

As a result of this settlement, covered entities should consider the following:

- A risk analysis must be conducted by a covered entity to discover any security threats and vulnerabilities of all ePHI created, received, maintained, or transmitted by the entity. The results of the risk analysis must be addressed through a risk management plan to mitigate any security threats and vulnerabilities identified in the risk analysis.
- Further, data governance is key to proactively managing ePHI. HIPAA-covered entities accumulate data that is considered ePHI from a number of disparate sources, and it is possible that not all sources of ePHI are properly identified and categorized by the covered entity. Sound data governance practices help ensure that the covered entity understands where ePHI resides on its systems, and can properly assess security incidents as potential breaches of ePHI when appropriate.

THIS IS AN ADVERTISEMENT
© 2002-2024. Hall, Render, Killian, Heath & Lyman, P.C. All Rights Reserved.

- Covered entities should have a process to routinely audit uses and disclosures of PHI to ensure impermissible uses and disclosures are detected and reported in accordance with HIPAA requirements.
- Covered entities, regardless of their size, must have policies and procedures to comply with the HIPAA Privacy, Security and Breach Notification Rules. It is especially important to address any threats and vulnerabilities to ePHI.

If you have any questions or would like additional information about this topic, please contact:

- Charise Frazier at (317) 977-1406 or cfrazier@hallrender.com;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com; or
- Your primary Hall Render contact.

Special thanks to Summer Associate, Liliann Stoll, for her assistance with this alert.

Hall Render blog posts and articles are intended for informational purposes only. For ethical reasons, Hall Render attorneys cannot—outside of an attorney-client relationship—answer specific questions that would be legal advice.

THIS IS AN ADVERTISEMENT
© 2002-2024. Hall, Render, Killian, Heath & Lyman, P.C. All Rights Reserved.