NOVEMBER 07, 2019

FAILURE TO ENCRYPT HARDWARE RESULTS IN $3 MILLION FINE

On November 5, 2019, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") announced that a New York Medical Center ("Medical Center") will settle potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") by paying a civil penalty of $3 million and entering into a Corrective Action Plan. The Medical Center is a HIPAA covered entity that includes hospital and academic medicine components.

According to OCR, the Medical Center had experienced several issues with lost or stolen unencrypted devices. OCR investigated the Medical Center in 2010 in a matter relating to an unencrypted flash drive and had provided technical assistance to the Medical Center. In the course of receiving that technical assistance, the Medical Center identified a lack of encryption as a high risk to its electronic protected health information ("ePHI"). Despite identifying this risk, the Medical Center continued to allow the use of unencrypted mobile devices. In 2013, the Medical Center notified OCR of the breach of unsecured ePHI, specifically the loss of an unencrypted flash drive. In 2017, the Medical Center notified OCR that an unencrypted personal laptop that contained Medical Center ePHI had been stolen, which resulted in the Medical Center impermissibly disclosing the ePHI of 43 patients.

OCR did not consider the risk analysis conducted by the Medical Center to be an accurate and thorough analysis of all potential risks and vulnerabilities to the confidentiality, integrity and availability of all of the ePHI the Medical Center was responsible for safeguarding. Further, OCR determined that the security measures implemented by the Medical Center to reduce risks and vulnerabilities to a reasonable and appropriate level were insufficient. OCR further found that the policies and procedures governing hardware and electronic media, including receipt and removal and movement of such hardware and electronic media in, out and within the Medical Center were also insufficient. Finally, OCR determined that the Medical Center did not implement mechanisms that were sufficient to either (1) encrypt and decrypt ePHI, or (2) document why encryption was not reasonable and appropriate while implementing an equivalent alternative measure to safeguard ePHI.

The Corrective Action Plan requirements include conducting a risk analysis, developing and implementing a risk management plan and updating policies and procedures and training materials.

PRACTICAL TAKEAWAYS

As a result of this enforcement action, covered entities and business associates should take note of the following:

- OCR will scrutinize determinations that encryption is not reasonable or appropriate for a covered entity to protect ePHI, especially the encryption of mobile devices. An entity subject to the HIPAA Security Rule must thoroughly document the reasons it has determined that encryption is not reasonable or appropriate.
- Entities that have received technical assistance from OCR need to ensure that they actually implement the technical assistance. Repeat HIPAA incidents or violations, even after several years have passed, can be interpreted by OCR as a pattern of noncompliance.
- A security risk analysis will likely not be found to be effective by OCR if the covered entity or business associate does not take steps to actually mitigate risks and vulnerabilities identified by the risk analysis. Once a security risk analysis is created, a risk management plan should be developed. OCR also issued a penalty last month that was based in part on insufficient risk analyses. This highlights the importance of conducting a meaningful security risk analysis and actually taking steps to address the threats and vulnerabilities identified.

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

- Mark Swearingen at (317) 977-1458 or mswearingen@hallrender.com;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com; or
- Your regular Hall Render attorney.

For more information on Hall Render's HIPAA, Privacy & Security services, click here.