FAILURE TO ENCRYPT LAPTOP AND FAILURE TO COMPLY WITH TECHNICAL ASSISTANCE FROM OCR LEADS TO $65,000 SETTLEMENT

On December 30, 2019, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") announced a resolution agreement with an ambulance company ("Company") covered entity that provides both emergency and nonemergency transportation services. The Company employs only 64 workers. The Company will pay $65,000 and enter into a Corrective Action Plan ("CAP") to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

THE SETTLEMENT

The Company filed a breach report with OCR in 2013 when an unencrypted laptop fell off the bumper of an ambulance. The unencrypted laptop held the protected health information ("PHI") of 500 individuals. OCR investigated and uncovered multiple failures to comply with HIPAA's requirements. Such failures included:

- Lack of a risk analysis;
- Failure to provide security training to the Company's workers; and
- Failure to implement policies to comply with the HIPAA Security Rule, including failure to have a HIPAA security training program.

OCR indicated that it provided technical assistance to the Company, but the Company did not implement such technical assistance.

THE CAP

The Company entered into a two-year CAP with HHS. The CAP requirements include the completion of a risk analysis. The Company is also required to adopt, implement and train its workforce on adequate policies and procedures. The CAP additionally includes a requirement for the Company to install "HIPAA compliant encryption software on all of its computers." This is notable given encryption's status as an addressable rather than a required safeguard within the HIPAA regulations.

COMPLYING WITH TECHNICAL ASSISTANCE FROM OCR

A covered entity's alleged failure to comply with OCR's technical assistance or other recommendations has been a common theme in recent HIPAA settlements. See our previous articles here and here.

Implementing technical assistance received from OCR provides one means for a covered entity to address compliance concerns to OCR's satisfaction, sometimes in lieu of engaging in a protracted negotiation with OCR over a fine or penalty. Failure to comply with technical assistance could be interpreted by OCR as a covered entity's disregard or inability to comply with HIPAA requirements, absent mitigating factors. When a covered entity undertakes efforts to implement such technical assistance, there may be instances where a number of individual factors could impede, delay or prevent a covered entity from complying with such technical assistance, such as a good faith misunderstanding or financial difficulties. If a covered entity determines that it is unable to comply with technical assistance from OCR, it may be worthwhile for the covered entity to seek assistance from legal counsel to communicate with OCR to find alternate solutions to address OCR's concerns or to negotiate an alternative resolution.

PRACTICAL TAKEAWAYS

In light of this settlement, covered entities should keep the following in mind:

- While OCR automatically investigates breaches that affect over 500 individuals, reporting any breach to OCR can trigger an investigation into a covered entity's HIPAA compliance that can extend beyond the scope of the breach. Such investigations may uncover additional compliance issues, in addition to those that led to a breach. It is advisable for covered entities to take the time to assess HIPAA compliance more broadly whenever a reportable breach occurs in order to address issues, mitigate harm and prevent further breaches.
- Encryption, especially encryption of portable devices like laptops, flash drives and cellular phones, can help prevent the compromise of PHI. This is especially important with devices that contain or connect to systems containing enormous amounts of PHI. Encryption is an

"addressable" standard and not technically a "required" standard under the HIPAA Security Rule. This means that a covered entity must implement encryption or an equivalent alternative measure whenever reasonable and appropriate. If a covered entity determines that encryption is not reasonable or appropriate, it must document: the determination and its reasons for such determination; whether an alternative safeguard was implemented; and if not, why such alternative safeguard was not implemented. This documentation should include discussion of the factors that were considered and the results of the risk assessment on which the decision was based. Additionally, covered entities should confirm that lack of encryption does not impact any cybersecurity insurance coverage.

- A covered entity's workforce is the front line for preventing, identifying and addressing security incidents, especially when they are related to lost or stolen devices. A security awareness and training program should be specifically tailored to the covered entity's security framework, business operations and identified risk areas.
- A risk analysis should be conducted at least annually, and a risk management plan based on the risk analysis results should be drafted, implemented and monitored.
- Violations of the HIPAA Security Rule may give rise to HIPAA privacy breaches. Security policies and procedures should be in place, available to appropriate workforce members and reviewed and updated at least annually, particularly to address items identified as part of the annual risk analysis and risk management plan.

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;
- Stephane Fabus at (414) 721-0904 or sfabus@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.