Published on *The National Law Review* https://natlawreview.com

# Stolen Laptop and Lack of Understanding of HIPAA Leads to $2.5 Million Settlement

Article By:

Health Law

This week the U.S. Department for Health and Human Services Office for Civil Rights (OCR) announced a settlement for an impermissible disclosure of unsecured electronic protected health information (ePHI) and the covered entity's lack of understanding of HIPAA requirements. The covered entity, the first wireless health services provider to face such a settlement, must pay $2.5 million and begin implementation of a corrective action plan that involves OCR scrutiny of its HIPAA Security Rule compliance.

## Impermissible Disclosures

In January of 2012, the covered entity filed a breach report indicating a workforce member's laptop containing the ePHI of 1,391 individuals was stolen from a vehicle outside of the person's home. Another incident in February of 2012 led to covered entity filing an additional report regarding the unsecured breach of the ePHI of 2,219 individuals. In May of 2012, OCR notified the covered entity that OCR was investigating the covered entity's compliance with HIPAA's Privacy, Security, and Breach Notification Rules.

## Lack of Understanding of HIPAA Requirements

OCR's announcement also highlights that not understanding HIPAA's requirements creates risk for entities subject to HIPAA. OCR found that the covered entity had insufficient risk analysis and risk management processes in place at the time of the laptop theft. OCR's investigation also revealed that the covered entity's policies and procedures for implementing HIPAA Security Rule standards were still in draft form and not yet effective. Finally, the covered entity had also failed to produce any policies or procedures regarding safeguards for ePHI, including for mobile devices such as the one stolen.

## Settlement

The covered entity and OCR entered into a Resolution Agreement, which includes a two-year corrective action plan requiring the covered entity to:

1. Conduct a risk analysis of security risks and vulnerabilities, subject to OCR approval;

2. Develop and implement a risk management plan to address and mitigate the security risks and vulnerabilities identified in the risk analysis, subject to OCR approval;

3. Revise its policies and procedures, as necessary, based on implementation of the risk management plan and requirements of the Security Rule, and submit such updated policies for OCR approval;

4. Implement secure device and media controls with proper encryption protocols and provide certification to OCR that all laptops, flash drives, SD cards, and other portable media devices are encrypted (together with a description of the encryption methods used), which shall also be subject to OCR approval;

5. Review and revise its training program relating to the use, security, encryption, handling of mobile devices, and out-of-office transmissions, which shall also be subject to OCR review and approval;

6. Notify OCR of any workforce member's failure to comply with the covered entity's policies and procedures (not just policies and procedures related to Security Rule compliance); and

7. Submit annual reports detailing the corrective actions taking during the year.

This settlement reinforces the importance for covered entities and business associates to not only ensure that policies and procedures are updated, effective, and HIPAA-compliant, but also to properly execute and enforce its policies and procedures (including by educating its workforce to safeguard and prevent the disclosure of unsecured ePHI). It is clear that OCR expects HIPAA policies and procedures to be continuously reviewed, analyzed, and updated/refreshed as an interactive compliance program, rather than untouched binders on a shelf representing a compliance snapshot in time.



National Law Review, Volume VII, Number 117