Stolen Laptop with Unencrypted Medical Data = $1.5 Million Fine

by Alice Leiter [1]
September 24, 2012

The federal law protecting the privacy of your medical records has historically been all bark and little bite; however, changes [2] to the law in 2009 expanded and strengthened its ability to crack down on privacy violators. The government hasn't shied away from using its beefed up enforcement power, as evidenced by the $1.5 million fine it dropped on a Massachusetts group last week for putting patients' medical records at risk.

The Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) announced [3] recently it had fined the Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates (MEEI) for privacy violations relating to the Health Insurance Portability and Accountability Act (HIPAA). This is excellent news for both privacy advocates and consumers. It indicates that OCR's recent commitment to HIPAA enforcement and penalties is alive and well.

As required by law, MEEI told OCR that an unencrypted laptop containing the personal health information of some 3,500 patients and research subjects was stolen. OCR found that MEEI had demonstrated a "long-term, organizational disregard for the requirements of the [HIPAA] Security Rule," including a failure to conduct a thorough risk analysis of the confidentiality of electronic protected health information (ePHI) maintained on portable devices and to implement sufficient security measures. In addition to paying the fine, MEEI is required to follow a corrective action plan, which includes reviewing, revising and maintaining policies and procedures to ensure compliance with the Security Rule.

The MEEI action is the fourth this year in a series of enforcements following changes to HIPAA by the Health Information Technology for Economic and Clinical Health (HITECH) Act to ensure covered entities and business associates are complying with security and privacy rules. This is a welcome sign that OCR is taking its enforcement authority more seriously.

An electronic health information environment depends upon patient trust to succeed, but the very real danger of breach undermines consumer confidence. It is encouraging to see OCR taking swift, thorough and very public action against HIPAA violators.

-
- hipaa
- enforcement

Copyright © 2013 by Center for Democracy & Technology.
The content throughout this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL:
https://cdt.org/blogs/alice-leiter/2409stolen-laptop-unencrypted-medical-data-15-million-fine

Links:
[1] https://cdt.org/personnel/alice-leiter
[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html
[3] http://www.hhs.gov/news/press/2012pres/09/20120917a.html