COMPLIANCE ALERT

EPIC Insurance Brokers & Consultants

HEFTY HIPAA PENALTY FOR FAILURE TO ENCRYPT MOBILE DEVICES

December 1, 2019

QUICK FACTS

- The Health Insurance Portability and Accountability Act (HIPAA) contains stringent privacy and security rules that group health plans, as covered entities, must follow to safeguard participants' protected health information (PHI).
- The Department of Health and Human Services (HHS), through the Office of Civil Rights (OCR), enforces the privacy and security rules and can assess fines against non-compliant covered entity group health plans.
- The OCR continues to address HIPAA complaints and monitor covered entities to ensure that they meet their HIPAA obligations.
- Plan sponsors should ensure that the devices used to manage or store sensitive PHI are properly secured, and encrypted. They should also ensure that individuals handling PHI or using the devices have proper HIPAA training.

THE CASE

One of the largest health systems in New York, The University of Rochester Medical Center (URMC), has agreed to pay $3 million in fines to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS). URMC will also take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules.

URMC filed breach reports with the OCR in 2013 and 2017 relating to two separate incidents involving unencrypted mobile devices (a lost flash drive and a stolen laptop). As a result of the filings, the OCR investigated URMC and discovered several failures on the health system's part. The OCR's inquiry revealed that URMC failed to (1) conduct an enterprise-wide risk analysis; (2) implement the reasonable and appropriate level of security measures sufficient to reduce risks and vulnerabilities; (3) utilize device and media controls; and (4) employ reasonable and appropriate encrypt and decrypt mechanisms to safeguard electronic protected health information (ePHI).

In 2010 the OCR investigated URMC because an unencrypted flash drive went missing. The HHS provided technical assistance and guidance to the health system at that time, but URMC continued to authorize the use of unencrypted mobile devices. Now, URMC will not only need to pay a monetary fine, but also undergo a corrective action plan. URMC's resolution agreement includes two years of the OCR monitoring their compliance with the HIPAA rules.

COMPLIANCE ALERT

EPIC Insurance Brokers & Consultants

KEY TAKEAWAYS FOR EMPLOYER PLAN SPONSORS

To avoid HIPAA violations and hefty penalties, covered entities should consider taking steps to protect ePHI (and all protected health information) by encrypting all mobile devices, including flash drives, laptops and cell phones that may hold such information. The consequences of violating HIPAA depend on the level of negligence, the number of records potentially exposed by the breach, and the unauthorized disclosures' posed level of risk.

Should a covered entity violate HIPAA, the OCR may issue guidance, a corrective action plan, and civil monetary penalties. The HIPAA penalties, which were recently revised, are structured as follows:

Culpability Level	Minimum penalty per violation	Maximum penalty per violation	All such violations of an identical provision in a calendar year
No Knowledge	$117	$58,490	$1,754,698
Reasonable Cause	$1,170	$58,490	$1,754,698
Willful Neglect - Corrected	$11,698	$58,490	$1,754,698
Willful Neglect - Not Corrected	$58,490	$1,754,698	$1,754,698

HIPAA COMPLIANCE FOR EMPLOYERS

EPIC's Compliance Team assists employer health plan sponsors in understanding and meeting their HIPAA obligations, including help with training members of their workforce who deal with health plan PHI. If you have any questions regarding HIPAA compliance, please contact a member of your EPIC benefits consulting team.

EPIC Employee Benefits Compliance Services

For further information on this or any other topics, please contact your EPIC benefits consulting team.

425 California Street, 24th Floor
San Francisco, CA 94104
415.356.3900