HHS Office for Civil Rights in Action

OCR Cyber-Awareness Monthly Update
August 18, 2016

OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals

Since the passage of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and the subsequent implementation of the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule, OCR has prioritized investigation of reported breaches of protected health information (PHI).

Importance of Understanding Data Breach Causes

The root causes of breaches may indicate entity-wide and industry-wide noncompliance with HIPAA regulations, and investigation of breaches provides OCR with an opportunity to evaluate an entity's compliance programs, obtain correction of any deficiencies, and better understand compliance issues in HIPAA-regulated entities more broadly.

Smaller Data Breaches Also Count

OCR Regional Offices investigate all reported breaches involving the PHI of 500 or more individuals. Regional Offices also investigate reports of smaller breaches (involving the PHI of fewer 500 individuals), as resources permit.

Recent settlements of cases where OCR has investigated smaller breach reports include Catholic Health Care Services, Triple-S, St. Elizabeth's Medical Center, QCA Health Plan, Inc. and Hospice of North Idaho. [Links to those individual details are displayed on page 2.]

Beginning this month, OCR, through the continuing hard work of its Regional Offices, has begun an initiative to more widely investigate the root causes of breaches affecting fewer than 500 individuals.

Regional Offices will still retain discretion to prioritize which smaller breaches to investigate, but each office will increase its efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these breaches.

Factors OCR Regional Offices Will Consider

Among the factors Regional Offices will consider include:

- The size of the breach;
- Theft of or improper disposal of unencrypted PHI;
- Breaches that involve unwanted intrusions to IT systems (for example, by hacking);
- The amount, nature and sensitivity of the PHI involved; or
- Instances where numerous breach reports from a particular covered entity or business associate raise similar issues.

Regions may also consider the lack of breach reports affecting fewer than 500 individuals when comparing a specific covered entity or business associate to like-situated covered entities and business associates.

For More Information

For more information about OCR compliance and enforcement work with regard to breaches, and with regard to the many other incidents that OCR investigates, please visit: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html.

Following are links to the five data breach settlement cases mentioned on page 1:

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/catholic-health-care-services/index.html

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/triple-s-management/index.html

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/semc/index.html

http://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html

http://www.hhs.gov/about/news/2013/01/03/hhs-announces-first-hipaa-breach-settlement-involving-less-than-500-patients.html