Shumaker

DECEMBER 6, 2019 | PUBLICATION

Client Alert: OCR Blitzkrieg: Wider Investigation of Smaller Breaches

INDUSTRY SECTOR

Health Care

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

On the heels of its first business associate settlement with a business associate and a hat trick of multi-million dollar settlements with covered entities involving electronic Protected Health Information ("**PHI**"), on August 18, 2016 the Office for Civil Rights ("**OCR**") announced that it has begun an initiative to more widely investigate the root causes of breaches affecting fewer than 500 individuals. The goals of the initiative are to better evaluate covered entities' compliance programs, obtain corrective action of any deficiencies and to better understand compliance issues of HIPAA covered entities more broadly.

Currently, OCR Regional Offices investigate all breaches involving PHI of more than 500 individuals and other breaches as time permits. Under the new initiative the OCR Regional Offices will increase their efforts to identify and obtain correction action to address entity and systemic noncompliance related to smaller breaches. They will have the discretion to prioritize which smaller breaches to investigate and will consider:

1. The size of the breach;

2. Theft of or improper disposal of PHI;

3. Breaches that involve unwanted intrusions to IT systems (such as hacking);

4. The amount, nature and sensitivity of the PHI involved; and

5. Instances where numerous breach reports from a particular covered entity or business associate raise similar issues.

Voluntary actions and technical assistance have been and are commonly used by OCR to resolve noncompliance, however, in announcing the initiative, OCR pointed out that it has entered into recent settlements where it investigated smaller breach reports. These include:

1. A 2013 settlement with Hospice of North Idaho involving a corrective action plan and a penalty of $50,000 after an investigation of a PHI breach involving 441 individuals resulting from the theft of an unencrypted laptop;

2. A 2014 settlement with QCA Health Plan involving a corrective action plan and a monetary penalty of $250,000 after an investigation of a PHI breach involving 148 individuals, also resulting from the theft of an unencrypted laptop; and

3. A 2015 settlement with St. Elizabeth Medical Center involving a corrective action plan and a monetary penalty of $218,400 after an investigation of two PHI breaches involving a combined 1093 individuals resulting from unsecured PHI on a former employee's laptop and a USB drive, and employee use of an internet application without analyzing the risks of doing so.

Covered entities and business associates can expect the number of OCR investigations and settlements to continue to climb. The OCR smaller breach initiative follows a September 2015 report of the Office of Inspector General that encouraged OCR to strengthen its oversight. OCR has entered into more settlements in the first eight months of 2016 than it did in all of 2015.

To avoid costly penalties and onerous corrective action plans, covered entities and business associates should identify and address the root cause of identified deficiencies to ensure they are not an indication of entity wide or systemic noncompliance. If we can assist you or if you have questions, please contact Kelly Leahy at (614) 628-6815 or kleahy@shumaker.com.

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer

Shumaker