You Can Run, but You Can't Hide: OCR Announces Increased Investigation of Small HIPAA Breaches

September 9, 2016

Since the issuance of the HIPAA Breach Notification Rule (45 CFR 164.402 et. seq.), HIPAA covered entities have been obligated to report breaches to the Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services. Breaches involving the protected health information of 500 or more individuals must be reported immediately to OCR and are displayed on the "wall of shame" of OCR's website. Smaller breaches are reported annually to OCR. Historically, OCR has prioritized its resources toward investigation of larger breaches with fewer investigations of smaller breaches.

All of that is about to change. In August 2016, OCR announced that its Regional Offices will expand initiatives to investigate smaller breaches. OCR will investigate breaches occurring at covered entities or at business associates, even though only covered entities have a direct obligation to report to OCR. The Regional Offices will have discretion to decide which smaller breaches to investigate, taking into account factors such as the following:

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

OCR has stated that even covered entities that habitually report statistically few breaches will now be on its radar screen. If that reporting pattern is below the norm for comparable entities, OCR's suspicion may be raised about the non-reporting entity's ability to recognize and remediate breach events. Under the Breach Notification Rule, all improper disclosures of or access to unsecured protected health information are presumed to be a reportable breach, unless the covered entity can affirmatively demonstrate that there is only a low risk that the protected health information has been compromised—all as defined in the rule.

This all means that HIPAA covered entities need to take their breach reporting responsibilities even more seriously than before. It also means that HIPAA covered entities and business associates must enhance their focus on the safeguards that can prevent a breach, detect one when it does occur, and respond immediately to remediate and mitigate its effects. These safeguards range from highly sophisticated cybertechnology applications to very low tech precautions relating to human behavior. It won't take a major hack to get OCR interested in a covered entity's or business associate's HIPAA compliance anymore.

For further information please contact Joanne Lax (248-203-0816 or jlax@dykema.com), Kathrin Kudner (734-214-7697 or kkudner@dykema.com), Josh Sutin (210-554-5309 or jsutin@dykema.com), or your Dykema relationship attorney.

Attorneys

Thomas B. Alleman

Sherrie L. Farrell

Jonathan S. Feld

Jennifer Fraser

J. Daniel Harkins

Kathrin E. Kudner

Mark G. Malven

Donna K. McElroy

Daniel R. Stern

Leonard C. Wolfe

Practice Areas

Health Care

Privacy and Data Security