Reinhart

OCR to Increase Investigations of Small PHI Breaches

The United States Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") recently announced that it will increase the frequency with which it will investigate breaches of unsecured protected health information ("PHI") involving fewer than 500 individuals. While OCR has historically focused on investigating breaches involving more than 500 individuals, the announcement signals the start of increased action by OCR involving smaller scale breaches.

OCR's announcement explained that OCR's regional offices have started working on an initiative to find the root cause of breaches involving fewer than 500 individuals. Although the regional offices will retain discretion as to which breaches to investigate and prioritize, the goal of the initiative is to address systemic noncompliance, taking into account factors such as size, involvement of theft or improper disposal of PHI, unwanted intrusions into IT systems, the type of PHI involved and repeated breaches from the same entity.

The announcement comes on the heels of some of the largest OCR settlements to date. For example, Downers Grove, Illinois-based Advocate Health Care Network recently made headlines in August for agreeing to a $5.55 million settlement to resolve OCR claims arising out of a 2013 breach that potentially exposed the PHI of approximately 4 million individuals. Smaller breaches can also result in significant penalties. The Catholic Health Care Services of the Archdiocese of Philadelphia, a business associate, agreed to a $650,000 settlement with OCR this year in connection with a breach involving 412 individuals caused by the theft of an unencrypted mobile device.

Breaches are likely to become even more prevalent in the coming years as health care providers and their employees increasingly conduct work activities from electronic devices and hackers scour networks for valuable PHI. Multiple breaches in 2016 were caused by employees losing unencrypted cell phones or other devices that contained PHI. All health care providers, not just large organizations, must put in place the necessary safeguards and be diligent about educating employees regarding the appropriate use of work devices and best practices to ensure the security of PHI.

It is very important for all health care providers to recognize that OCR routinely pursues smaller organizations for failure to comply with the Health Insurance Portability and Accountability Act ("HIPAA"). Organizations that follow the steps

POSTED:

Nov 22, 2016

RELATED PRACTICES:

Health Care

https://www.reinhartlaw.com/practices/health-care

RELATED PEOPLE:

Robert J. Heath

https://www.reinhartlaw.com/people/robert-heath

listed below will be well-prepared if a breach were ever to occur.

1. Culture of Compliance. Be prepared before an incident occurs. Strive to create a "culture of compliance," which includes regular privacy and security training, annual privacy/security risk assessment, and regular reviews of privacy and security processes and procedures.
2. Risk Areas. Ensure that your risk assessment, risk management plan, and accompanying policies and procedures are current and compliant. Because of the frequency with which breaches involve the loss of unencrypted mobile devices, consider implementing a policy addressing mobile device security (e.g., user authentication, encryption, remote wiping, application use, removal of mobile devices from facilities, etc.). A third party audit may help to shed light on an organization's weak spots, such as staff training, lack of encryption and other areas.
3. Legal Counsel. Involve your legal counsel throughout this process and, preferably, well before a breach occurs. Legal counsel should be engaged to analyze current policies and procedures, assist as you formulate a breach notification policy and engage a third party consultant to conduct a risk assessment.

If you have any questions about the OCR audit program and its impact on your organization, or if you have any questions about how to comply with the HIPAA privacy and security rules, please contact Rob Heath or your Reinhart attorney.