OCR to step up investigations of small HIPAA breaches

Rick L. Hindmand, James J. Giszczak, Dominic A. Paluzzi | Friday, August 19, 2016

Yesterday, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) announced its new initiative to investigate breaches of protected health information (PHI) affecting fewer than 500 individuals.

Breaches affecting fewer than 500 individuals are sometimes referred to as "small" breaches in light of the different treatment they receive under the HITECH Act and Breach Notification Rule. Breaches involving 500 or more individuals trigger earlier OCR reporting deadlines, and are publicly disclosed on OCR's website. Most significantly, OCR investigates all breaches involving 500 or more individuals. In contrast, breaches involving fewer than 500 individuals typically escape public disclosure and scrutiny by OCR, which investigates smaller breaches only as resources permit.

Even with OCR's traditional focus on breaches involving at least 500 individuals, OCR has publicly disclosed at least five settlements in recent years arising out of investigations involving PHI of fewer than 500 individuals. One of these was the first HIPAA resolution agreement with a business associate, which was announced less than two months ago and provided for a $650,000 settlement payment even though only 412 patients were affected by the breach.

As a result of this change, small breaches will be less likely to slip under the radar. The change will also ratchet up the potential exposure facing HIPAA covered entities and business associates. It is therefore becoming even more important for every covered entity or business associate to maintain robust safeguards to protect the privacy and security of PHI. The following steps are particularly important:

- Conduct enterprise-wide risk analysis accounting for all ePHI maintained within the organization or on its behalf by business associates or subcontractors.
- Implement safeguards based on the risk analysis to reduce the identified risks and vulnerabilities to reasonable and appropriate levels.
- Review and update an incident response plan and HIPAA privacy, security and breach notification policies and procedures.
- Identify all business associate relationships (whether as covered entity, business associate or subcontractor) and ensure that all required HIPAA business associate agreements are in place.

- Make privacy and security priorities within the organization.
- Conduct ongoing privacy and security awareness training with your workforce members and business associates
- Encrypt portable devices containing ePHI where technically feasible, and if not feasible, document this assessment and implement an equivalent alternative measure that is reasonable and appropriate.

For more information, please contact one of the attorneys listed below or another member our Data Privacy and Cybersecurity or Healthcare team.

Rick L. Hindmand

Team member bio

James J. Giszczak

Team member bio

Dominic A. Paluzzi

Team member bio