Cooley

January 23, 2015

As of early December 2014, 1,170 security breaches under the Health Insurance Portability and Accountability Act (HIPAA) involving 31 million records had been reported to the U.S. Department of Health and Human Services (HHS) since mandated reporting of such breaches began in September 2009. The number of complaints of medical record security breaches in 2014 also reached a new high. A spokeswoman for the HHS Office of Civil Rights (OCR) noted that "OCR's strong enforcement of the HIPAA privacy, security, and breach notification rules, remains very much on track."

On January 17, 2013, HHS released the long-awaited "Omnibus Rule" mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, which amends a wide range of privacy, security, and breach notification requirements under HIPAA. HITECH and the Omnibus Rule represent the most comprehensive set of changes to HIPAA since its inception. Some of the changes under the Omnibus Rule include: imposing new rules governing uses and disclosures of Protected Health Information (PHI); enhancing patient rights to access and to restrict disclosure of their PHI; expanding certain HIPAA obligations to business associates and their subcontractors; modifying breach notification standards; and broadening permissible enforcement approaches.

HHS is required to perform periodic audits of covered entities' and business associates' compliance with HIPAA and HITECH. OCR enforces HIPAA and HITECH and in 2011, OCR established a pilot audit program to assess the controls and processes covered entities and business associates have implemented to comply with the law. Through this program, OCR developed a protocol for compliance and measured the efforts of 115 entities. A compliance report issued last year sheds light on what covered entities and business associates can expect from OCR going forward. OCR is ramping up its enforcement efforts and will soon begin its second round of compliance audits.

Given recent changes to the law, heightened enforcement efforts, and the continuation of the audit program, we recommend that organizations take the following steps to ensure they are in compliance with existing HIPAA and HITECH obligations and to reduce their liability:

1. **Perform a risk assessment audit.** Become familiar with the HIPAA and HITECH requirements applicable to your organization. Review your existing policies and practices for consistency with your organization's obligations under HIPAA and HITECH, and work with counsel to perform a risk assessment to determine where compliance efforts need to be improved. Cooley has developed risk assessment tools for this purpose.
2. **Review and update policies and procedures as necessary.** Proactively identify and address HIPAA and HITECH compliance risks by using what is discovered in your organization's risk assessment to update your policies and procedures as necessary. Again, your counsel can be helpful here. Cooley has developed comprehensive policies and procedures and other tools to facilitate HIPAA and HITECH compliance.
3. **Encrypt PHI at rest and in transmission.** Although encryption is not required by HIPAA and HITECH, encryption is highly recommended to meet HIPAA and HITECH compliance standards and is required for certain sensitive information by some states. A breach of encrypted data does not trigger notice obligations under HIPAA and HITECH. However, based on the observations from the first round of audits and in recent HIPAA and HITECH breach settlements, OCR considers encryption to be very important. Therefore, encryption is an area that is expected to be a focus of the next round of audits.
4. **Prepare breach response protocol before breaches occur.** Another focus area of the next round of audits will be breach compliance. HITECH and the Omnibus Rule outline breach notification obligations and penalties for failing to adhere to those requirements. Organizations should ensure that a breach notification policy is in place that accurately reflects legal requirements and that employees are aware of procedures that must be taken in case of a potential breach. Effective breach response is more likely when the company has a solid response plan already in place. Cooley attorneys can help you implement an effective breach response plan.
5. **Ensure adequate insurance is in place to cover breach events and related liability.** While not required under HIPAA or HITECH, insurance coverage for breaches and other privacy and security related liability is highly recommended. Costs for these types of incidents can quickly become very high. Based on research conducted by the Ponemon Institute, the average cost per one lost or stolen record in the United States is $215, and the average cost to a company for each breach incident is $3.5 million.

Proactive HIPAA and HITECH compliance efforts can ensure that your organization is able to successfully complete a potential OCR audit and mitigate the risk of future losses due to HIPAA and HITECH violations and breaches. Cooley's Health Care Team has prepared an Audit Toolkit that can assist clients in assessing compliance with HIPAA and HITECH and determine areas for improvement. Contact us for further information on this topic.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Phil Mitchell **New York**	**phil.mitchell@cooley.com** **+1 212 479 6581**

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.