Illinois Association of Defense Trial Counsel
Springfield, Illinois | www.iadtc.org | 800-232-0169
IDC Quarterly | Volume 20, Number 1 (20.1.46)

Health Law

By: Roger R. Clayton, Mark D. Hansen and Jesse A. Placher
Heyl, Royster, Voelker & Allen

What Every Litigator Needs to Know About the HITECH Breach Notification Rules

The Health Information Technology for Economic and Clinical Health Act ("HITECH") was enacted as part of the American Recovery and Reinvestment Act of 2009. Section 13402 of HITECH imposes certain notification requirements upon entities covered by the Health Insurance Portability and Accountability Act ("HIPAA"), Public Law 104-191.Specifically, HITECH requires HIPAA-covered entities, defined in 45 C.F.R. 160.103, and their business associates to provide notification when breaches of unsecured protected health information occur. When a breach occurs, business associates of HIPAA-covered entities must inform the covered entities of any breach. Covered entities must then notify the individuals whose information has been breached or is reasonably believed to have been breached.

What Constitutes a Breach?

Pursuant to HITECH, a breach occurs when there is an unauthorized acquisition, access, use or disclosure of unsecured protected health information that compromises the security and privacy of the information. "Unsecured" protected health information is information that is still accessible. If a covered entity has technology or methodology that makes the information secured, meaning that it is inaccessible, unreadable and indecipherable, there is no need for notification. Examples of securing protected health information include encryption of electronic information and shredding of hard copy materials.

Also, if the information that has been disclosed does not contain harmful information, resulting in no risk of injury to the patient, there is no need for notification. To determine whether the information would be detrimental to the individual, a "harm threshold" must be met. The "harm threshold" is determined by a fact-specific risk assessment of the unauthorized information. The main factor to consider in the risk assessment is whether the identity of the individual can be determined from the information; if not, there is no risk of harm to that person. Likewise, if the individual can be identified, but the services cannot, there is likely no injury. The covered entity should also take all possible mitigation actions to ensure the information is destroyed by the unauthorized receiver or not viewed and returned by the unauthorized receiver. If the covered entity is positive that the information was destroyed or not viewed and returned, notification is unnecessary.

Exceptions to a Breach

There are three exceptions to a breach under HITECH. The first applies to workforce members of the covered entity when the disclosure was made in good faith, within the scope of the disclosing individual's authority and does not result in any further violation. For example, if one employee of the covered entity accidentally receives a piece of mail with confidential information, shreds the mail without reading it, and notifies the person who gave it to her, the exception would apply. As such, there is no obligation to notify.

The second exception applies to inadvertent disclosures from one person authorized to view the information to another also authorized to view the information, but with less authority. Both persons need to be employed by the covered entity or be business associates, such as a physician with staff privileges and a nurse employee of a hospital. An example might include when an employee who does billing for the hospital and may view only limited portions of a patient's information, receives the entire medical chart from a doctor who may view the entire record. In this situation, the doctor has full authorization and the billing clerk has limited authorization. The doctor and billing clerk both have some level of authorization under the same covered entity, so if the billing clerk does not review the material, there is no breach.

The third exception involves situations in which the covered entity has a good-faith belief that the unauthorized person who received the information could not have reasonably been able to retain such information. For example, the mailing of a patient's examination results to the wrong person, but the mail being returned unopened by the post office.

Notification Requirements

When a breach occurs, the HIPAA-covered entities must notify the individuals without unreasonable delay, and no later than 60 days. The time for notification begins to run upon the discovery of a breach. A covered entity's employee's knowledge of the breach will be imputed to the covered entity, while a business associate will need to notify the covered entity for it to be considered to have knowledge. It is important for a covered entity to impose strict reporting requirements on its employees, and to determine who is considered a business associate rather than an employee.

Covered entities should provide written notice to the individual, or next of kin if deceased. If the matter is urgent, an entity may also notify the individual by telephone. If there are ten or more people whose information has been breached, the covered entity should notify by a conspicuous posting on its website or in media print or broadcasting. If five hundred or more people are affected, the covered entity must give notice to a prominent media outlet within its state or jurisdiction. A HIPAA-covered entity must also notify the Secretary of the Department of Health and Human Services if there has been a breach of information of five hundred or more people. Finally, the entity must annually notify the Secretary of all breaches.

The notifications should include: 1) a brief description of the breach, including the date of the breach and date of discovery of the breach, 2) the type of public health information involved, 3) steps that the individual should take to protect himself, 4) a brief description of what the entity is doing to investigate and mitigate the breach, and 5) contact procedures for the individual to get in touch with the covered entity. The notification should also be written in "plain language."

Non-Covered Entities

The Federal Trade Commission ("FTC") also has a health breach notification rule that applies to entities not covered by HIPAA. For instance, a public health relation vendor may provide services on his own and through a covered entity. If a breach is made by this vendor, he will need to notify the covered entity for HITECH purposes, but will need to provide individual notice to his private clients under the FTC Rule. The FTC breach notification requirement guidelines are similar to those imposed under HITECH, and can be found at 16 C.F.R. §318.1-318.9.

Conclusion

Willful violations of any provision of HIPAA, including breach notification requirements, are punishable by a minimum fine of $10,000, up to $50,000 per violation. Therefore, as counsel for covered entities, it is imperative to advise your clients to create and enforce notification requirements to avoid costly penalties.

About the Authors

Roger R. Clayton is a partner in the Peoria office of *Heyl, Royster, Voelker and Allen* where he chairs the firm's healthcare practice group. He also regularly defends physicians and hospitals in medical malpractice litigation. Mr. Clayton is a frequent national speaker on healthcare issues, medical malpractice and risk prevention. He received his undergraduate degree from Bradley University and law degree from Southern Illinois University in 1978. He is a member of the Illinois Association of Defense Trial Counsel (IDC), the Illinois State Bar Association, past president of the Abraham Lincoln Inn of Court, past President and board member of the Illinois Association of Healthcare Attorneys, and past president and board member of the Illinois Society of Healthcare Risk Management and co-authored the Chapter on Trials in the IICLE Medical Malpractice Handbook.

Mark D. Hansen is a partner in the Peoria office of *Heyl, Royster, Voelker & Allen*. He has been involved in the defense of cases involving catastrophic injury, including the defense of complex cases in the areas of medical malpractice, products liability, and professional liability. Mark has defended doctors, nurses, hospitals, clinics, dentists, and nursing homes in healthcare malpractice cases. He received his undergraduate degree from Northern Illinois University and law degree from University of Illinois College of Law. Mark is a member of the Illinois Association of Defense Trial Counsel and is a co-chair of the Young Lawyers Committee, former ex officio member of the Board of Directors, and has served as chair for various seminars hosted by the IDC. He is also a member of the Illinois Society of Healthcare Risk Management, the Abraham Lincoln American Inn of Court, and the Defense Research Institute.

Jesse A. Placher is a 2007 Fall Associate in the Peoria office of *Heyl, Royster, Voelker & Allen*. He received his undergraduate degree from the University of Virginia in 2004 and law degree from Southern Illinois University in 2007. During law school, he was a member of the SIU Trial Team and was awarded the Order of the Barristers in 2007. Following graduation, he joined the firm's Peoria office in August 2007.

About the IDC

The Illinois Association Defense Trial Counsel (IDC) is the premier association of attorneys in Illinois who devote a substantial portion their practice to the representation of business, corporate, insurance, professional and other individual defendants in civil litigation.
For more information on the IDC, visit us on the web at **www.iadtc.org**.

Illinois Association of Defense Trial Counsel, PO Box 3144, Springfield, IL 62708-3144, 217-585-0991, idc@iadtc.org