Special Report

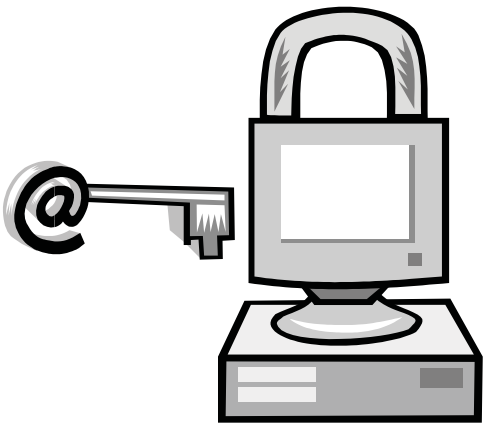
The HITECH Act

Privacy and Data Breach Notification Provision

An Overview of the HITECH Act

On February 17, 2009, President Obama signed into law the $787 billion stimulus package known as the American Recovery and Reinvestment Act (ARRA). Contained within ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which includes a multi-billion-dollar stimulus for the adoption of electronic health records. In addition, the HITECH Act imposes on entities a number of legal obligations designed to supplement and broaden HIPAA privacy and security requirements as well as various state privacy breach notification rules.

The purpose of this article is threefold. First, it provides an overview of the HITECH Act and highlights some of the key new obligations imposed by the Act. Second, the article addresses where the HITECH Act fits in the universe of breach notification laws. Finally, the article outlines, beyond obligations arising from the HITECH Act, general steps entities should take to reduce the likelihood of, prepare for and respond to a privacy breach.



The Extension of HIPAA Obligations to Business Associates

The HITECH Act contains provisions designed to safeguard "protected health information" (PHI) above and beyond current HIPAA requirements. One of the primary ways in which the HITECH Act accomplishes this is by extending HIPAA security and privacy obligations to cover "business associates" of entities that are presently covered by HIPAA (e.g., healthcare providers who transmit health information electronically, health plans and healthcare clearinghouses).

The term "business associate" is fully defined in the regulations promulgated under HIPAA, but generally includes entities that access, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose unsecured PHI. Such entities may include, but are not limited to, companies that provide claims administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, legal support, accounting, financial services and IT consulting.

In the past, these entities may have had contractual obligations to notify HIPAA-covered entities of PHI disclosure and security incidents. Now, business associates face civil and even criminal penalties for HIPAA violations under the HITECH Act.

HITECH Act Notification Requirements

The HITECH Act also imposes on HIPAA-covered entities, business associates and certain other entities (described below) notification requirements in the event of a privacy breach. The Act defines a breach as the "unauthorized

EQUIFAX NAVIGANT CONSULTING VEDDER PRICE P.C.

August 2009

acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."

In such a situation, the entity is required to provide notification within a given amount of time ("without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach") and via particular methods (written, telephonic, Web site or media notification depending on the number of affected individuals, the possibility of imminent misuse of the disclosed PHI and whether the entity has current contact information for those individuals). In certain large breach situations, the entity is also required to provide immediate notice to the Secretary of Health and Human Services, and annual notice for all other breaches.

The notification procedures outlined in the HITECH Act are triggered when there is a disclosure of 'unsecured' PHI

Regardless of the method of breach notification, notice of the breach is to include:

1) A brief description of what happened, including the date of the discovery of the breach, if known.
2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number and disability code).
3) The steps individuals should take to protect themselves from potential harm resulting from the breach.
4) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses and to protect against any further breaches.
5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site or postal address.

These breach notification requirements will also apply to entities that are neither covered entities nor business associates, with respect to breaches of security of "personal health records." A personal health record (PHR) is an electronic record containing individually identifiable information received from or on behalf of the individual who is the subject of the record "that can be drawn from multiple sources and that is managed, shared, and controlled by or primary for the individual." Noncovered entities and nonbusiness associates who (i) offer products or services through the Web site of a vendor of PHR, (ii) offer products or services through the Web site of covered entities that make PHR available to individuals and/or (iii) access information in a PHR or send information to a PHR are required to notify an individual of the security breach in the same manner as described above and, additionally, to notify the Federal Trade Commission.

Examples of such entities include companies with Web-based applications that help consumers manage medications, a bricks-and-mortar company advertising dietary supplements online, companies that provide online medication or weight tracking programs and companies that provide online applications through which individuals can connect blood pressure cuffs, blood glucose monitors or other devices so that the results can be tracked through their personal health records. Entities that provide services to PHR vendors are required, upon discovery of a security breach, to provide notice to the PHR vendor, and the PHR vendor is required to notify the individual.

Technology and Methodology Guidance

The notification procedures outlined in the HITECH Act are triggered when there is a disclosure of "unsecured" PHI. The Act directed the Department of Health and Human Services to issue guidance specifying technologies and methodologies entities can use to render PHI unusable, unreadable or indecipherable to unauthorized individuals. The Department of Health and Human Services issued such guidance on April 17,

2009, and noted therein that "while covered entities and business associates are not required to follow the guidance, the specified technologies and methodologies, if used, create the functional equivalent of a safe harbor, and thus, result in covered entities and business associates not being required to provide the notification otherwise required by [the HITECH Act] in the event of a breach." Covered entities and business associates thus have added motivation to adopt the technologies and methodologies advanced by the Department of Health and Human Services.

The Interaction between the HITECH Act and Preexisting Breach Obligations

Although it imposes legal obligations on covered entities and business associates, the HITECH Act, in conjunction with the guidance provided by the Department of Health and Human Services, is beneficial to entities in that it lays out a protocol to follow in the event of a breach involving PHI. Unfortunately, however, entities' response obligations are not limited to adherence to the HITECH Act.

Most states (44 at the time of publication of this paper) have enacted legislation that sets forth notification requirements in the event of breach involving personal identification information. A few states also have notification laws that apply specifically to health data. These notification requirements may differ from those provided for in the HITECH Act, and state notification requirements often differ from one another. This means that, when impacted individuals are located in multiple states, the entity providing notice often finds itself having to proceed under multiple state notification statutes.

Failure to abide by these obligations can result in civil litigation and/or action by the FTC or other government and law enforcement agencies

In addition to the HITECH Act and various state notification laws, entities must also comply with the HIPAA Privacy Rule, which requires covered entities to mitigate the harmful effects of a breach, as well as common law obligations to take reasonable steps to protect personal information pre- and post-breach. Failure to abide by these obligations can result in civil litigation and/or action by the FTC or other government and law enforcement agencies.

As the Department of Health and Human Services notes:

> [W]hile adherence to this guidance may result in covered entities and business associates not being required to provide notifications in the event of a breach, covered entities and business associates still must comply with all other federal and state regulatory obligations that may apply following a breach of PHI, such as state breach notification requirements, if applicable, as well as the obligation on covered entities at 45 CFR 164.530(f) of the HIPAA Privacy Rule to mitigate, to the extent possible, any harmful effect that is known to the covered entity as a result of the breach of PHI by the covered entity or business associate.

In short, the obligations of covered entities and business associates to safeguard PHI and other personal identification information does not begin and end with the HITECH Act, and entities should remain cognizant of the existence of other legal obligations.

Privacy Breach Reduction; Preparation and Response

Protecting confidential and proprietary information is absolutely necessary, not only to satisfy the HITECH Act and other existing legal obligations, but to maintain sound customer relationships and public goodwill. No entity wants to find itself obligated to disclose to its customers, government agencies or especially major media outlets that the personal health information of its customers or others has been disclosed and compromised.

As information becomes increasingly decentralized with the advancement of technology, preventing data breaches is becoming more and more difficult. Since January 2005, the Privacy Rights Clearinghouse has recorded well over 1,000 data breaches involving more than 250 million records. These breaches have occurred in every field, including the healthcare industry. Perhaps more concerning is a recent report by the Identity Theft Resource Center of San Diego that suggests the problem is getting worse. The Center found that, in 2008, businesses, governments and educational institutions reported nearly 50 percent more data breaches than in 2007. It is thus imperative that steps be taken before a breach occurs to manage information in a secure fashion, and to be prepared to appropriately and quickly respond in the event of a data breach.

HITECH Act Compliance and Data Protection

The first step in safeguarding PHI and other personal information is to make sure policies and security procedures are in place to reduce the likelihood of a data breach. Due to preexisting HIPAA requirements, most in the healthcare industry should already have in place such policies and procedures. However, in light of the HITECH Act, covered entities and business associates should do the following:

- Update data security to meet the guidelines and methodologies provided by the Department of Health and Human Services.
- Audit existing data security technology, as well as identity theft and record management policies and programs, for potential security and compliance gaps.
- Update contracts with business associates to address HITECH Act requirements.

Preparing for a Data Breach

As detailed above, entities that have suffered a data privacy breach have obligations under the HITECH Act, state statutes and common law to react promptly and properly. This is often easier said than done.

Breach investigation and containment is often complex, particularly in the case of hacking or other data theft situations. Once it is determined how the breach occurred, entities must still make determinations such as who was affected, how many individuals were affected, where those individuals reside and whether there exists current contact information for those individuals. Entities must determine their notification obligations, based, not only on the HITECH Act, but on varied state laws as well, and then carry out those obligations. Contact procedures should be created for those affected individuals who have questions, and, if the breach could lead to possible identity theft, the entity will want to arrange for credit monitoring to prevent further harm from the breach.

Breach investigation and containment is often complex, particularly in the case of hacking or other data theft situations

Each of the tasks in this incomplete list of post-breach activities and obligations requires time and effort. Thus, to the extent that an entity can prepare in advance for a data breach, it should do so. This includes:

- Implementing and/or updating security breach response plans.
- Contracting in advance for credit monitoring and other breach-related services to avoid having to negotiate rates from a position of weakness (namely, post-breach).

Incident Management and Response

While implementing technology and security procedures can lessen the likelihood of a breach, breaches may still occur. If a breach does occur, entities should immediately conduct a preliminary investigation as to how the breach occurred, and take the necessary steps to ensure that the breach is contained and corrective action is employed. If the situation involves potential employee or third-party misconduct, a legal investigation and possibly a "cyber" investigation may be required. If business associates or other third parties are involved in the security breach, steps must be taken to ensure that the third party is taking proper steps to contain the breach and retrieve or destroy disclosed information, and that third-party going-forward obligations are quickly agreed upon.

Once the breach has been contained (or even in conjunction with the containment process), the company must assess the risks associated with the breach. This includes, among other things, determining:

- The type of information involved in the breach.
- Who was affected by the breach (employees, customers, patients, etc.).
- The number of individuals affected by the breach.
- The location of individuals affected by the breach.
- Whether current contact information exists for the individuals affected by the breach.
- The foreseeable harm to the affected individuals given the nature of the breach.

This last determination requires an examination of issues such as:

- Whether the information disclosed was protected by means such as passwords or encryption.
- Whether this means satisfies the security guidelines issued by the Department of Health and Human Services in response to the HITECH Act.
- The nature of the personal information disclosed (PHI, credit card numbers, social security numbers, etc.).
- Steps already taken to minimize the damage.
- The number and nature of the recipients of the disclosed information.

If it is determined that notification is required, that notification should be prepared in accordance with the HITECH Act if PHI is involved, as well as with various state laws, and steps should be taken to deal with the associated effects, including arranging for credit monitoring and setting up a system of communicating with customers who have questions. If the entity is required to provide notification to a government agency, such as the Department of Health and Human Services or the FTC, or to state law enforcement, the entity should seriously consider retaining legal counsel.

Finally, the issue of data protection is not one that will disappear any time soon, and entities should learn from past incidents and continually look for ways to improve their data security.

Contributing Authors

Equifax Personal Information Solutions

Equifax (NYSE: EFX) delivers secure, proven and comprehensive Data Breach Response capabilities to the market. These capabilities include credit monitoring services, notification letter generation and mailing, call center services and address matching and appending. Equifax brings flexibility in terms of products, services, pricing and fulfillment to clients today. Equifax offers proactive data breach planning services as well as a quick response when organizations are reacting to a breach situation.

As one of three national credit reporting companies, Equifax has maintained the reputation for securely storing, managing and protecting critical consumer data for over 100 years; consequently we are called upon more than 5 million times per month to verify consumer identities to prevent fraud. Equifax employs more than 7,000 employees around the globe.

Dodge McFall

678-795-7654 Dodge.McFall@equifax.com

Richard Blumberg

678-795-7645 Richard.Blumberg@equifax.com

Dodge McFall is Senior Vice President of Business Development for Equifax Personal Information Solutions. Mr. McFall is responsible for managing Equifax's relationships with affinity partners and resellers to drive increased visibility of Equifax products and solutions across key sectors. While at Equifax, Mr. McFall has spearheaded the launch of an initiative to promote adoption and integration of data protection/intrusion programs within corporations as part of business continuity planning.

Richard Blumberg is a National Account Consultant with Equifax Consumer Services LLC based out of Atlanta, GA. He works with the public and private sector in the areas of data breach support and has assisted over 500 organizations in setting up proactive data breach response plans as well as handling pending data breach events. Richard also works with organizations to set up and manage identity theft solutions as an employee benefit.

Navigant Consulting

Navigant Consulting (NYSE: NCI) is a recognized leader in assisting companies by addressing disruptive business events with clear thinking, independence and the experience that delivers proven results. Our Data Governance and Computer Forensics practices are a cornerstone of the firm. Navigant Consulting provides data security, privacy and governance services that immediately assist clients faced with potential data breach, as well as assistance with establishing and implementing governance and compliance programs for data security and data privacy. We are also actively engaged in conducting forensic investigations including investigations related to electronic data access, security and computer forensics.

John D. Loveland

202-481-7513 JLoveland@navigantconsulting.com

L. Aaron Philipp

512-493-5404 Aaron.Philipp@navigantconsulting.com

John D. Loveland is a Managing Director in the Discovery Services practice for Navigant Consulting. He is based in Washington, D.C. and runs the practice's operations in the Mid-Atlantic region. He brings over 18 years executive-level management consulting, electronic discovery and computer forensics expertise to the firm. Mr. Loveland specializes in providing strategic advice and expert witness services to counsel on matters related to complex e-discovery issues and managing large end-to-end discovery matters. Navigant's Discovery Services practice provides a full suite of services from strategic planning to document evidence preservation and collection and computer forensics to document review and production.

L. Aaron Philipp is a Managing Consultant in the Disputes and Investigations practice at Navigant Consulting. He specializes in cybercrime investigations relating to IP Theft, Securities Fraud and Identity Theft, with a focus on threats originating in Eastern Europe and the former Soviet Union. He is also the author of "Hacking Exposed Computer Forensics."

VEDDER PRICE P.C.

Vedder Price P.C.

Vedder Price P.C. is a full-service law firm with over 250 attorneys located in offices in Chicago, New York and Washington D.C. Vedder Price's Privacy and Data Security Group is a leader in the rapidly evolving field of information management and assists its clients to plan for and prevent data privacy breaches.

Vedder Price counsels companies on compliance with privacy obligations and the development and implementation of security breach response plans and comprehensive record management programs. Vedder Price also has the experience necessary to quickly and effectively respond to privacy breaches in ways that not only comply with varied security breach notification laws but make business sense and best position companies in the event of future litigation or government investigation.

Bruce A. Radke

312-609-7689 bradke@vedderprice.com

Bruce A. Radke is a shareholder at Vedder Price. Mr. Radke is Chair of the Firm's Records Management eDiscovery and Data Privacy Practice Group. Mr. Radke regularly counsels public and sector clients on all aspects of records management and eDiscovery. Mr. Radke also assists clients with various privacy and data security issues, including preparing for and responding to data security breaches, and conducting data privacy audits. His articles and comments have been featured in the *Chicago Tribune*, *The Review of Banking & Financial Services* and the *Privacy & Data Security Law Journal*.

Richard H. Sanders

312-609-7644 rsanders@vedderprice.com

Richard H. Sanders is a shareholder in and the Practice Area Leader of the Health and Association Law Practice Area of Vedder Price P.C. He has served as corporate counsel to health care systems, hospitals, physician groups, home health organizations, provider networks, and managed care organizations. Mr. Sanders is an adjunct professor at Northwestern University School of Law also is a trained mediator and arbitrator and is listed on the panel of the Alternative Dispute Resolution Service of the American Health Lawyers Association. Mr. Sanders is admitted to the Illinois, Indiana and District of Columbia bars, as well as the Seventh Circuit U.S. Court of Appeals and the U.S. Supreme Court. He is a member of the Chicago, Illinois, Indiana, District of Columbia and American Bar Associations and their respective health law sections or committees. He is also the past Chairman of the Healthcare Section Council of the Illinois State Bar Association and a Fellow of the American Bar Foundation.

Jeffrey C. Davis

312-609-7524 jdavis@vedderprice.com

Jeffrey C. Davis is a shareholder at Vedder Price concentrating his practice on representing corporations, financial institutions, public bodies and individuals in technology licensing, records retention, eDiscovery, electronic commerce, data privacy, mergers and acquisitions, regulatory matters, corporate finance arrangements and general corporate matters. He has written and spoken extensively on a variety of topics relating to information technology, data privacy, records retention, e-mail and electronic discovery.

Michael J. Waters

312-609-7726 mwaters@vedderprice.com

Michael J. Waters is an attorney with Vedder Price's Litigation Practice Group. He also counsels all industry sectors in connection with the retention and management of electronic and hard copy data and records. This includes counseling clients on privacy and data security issues and assisting clients in preparing for and responding to data security breaches, as well as advising clients on eDiscovery issues. Mr. Waters' articles on these topics have appeared in publications such as *Antitrust, Privacy & Data Security Law Journal* and *The Illinois Manufacturer*.

1550 Peachtree Street
Atlanta, Georgia 30309

www.equifax.com/databreach

Chicago

New York

Washington, D.C.

www.navigantconsulting.com

Chicago

New York

Washington, D.C.

www.vedderprice.com