

**LYNDON GROUP**



## **Protecting Your Business**

### **What You Need To Know About HITECH Regulations and Risks**

**Eric L. Nelson**  
**Practice Leader – Privacy and Information Security**

# Protecting Your Business

## What You Need To Know About HITECH Regulations and Risks

### Background

According to the Los Angeles Times, more than 120 workers at the UCLA Medical Center looked at celebrities' medical records and other personal information without permission between January 2004 and June 2006.

State public health officials reported that 127 workers peeked into celebrities' medical records without permission, leading to several firings, suspensions and warnings. The violations included the patient records of Farrah Fawcett, Britney Spears, California First Lady Maria Shriver and other celebrities.

The report also detailed the case of one employee who looked at the records of about 900 patients "without any legitimate reason" and viewed Social Security numbers, health insurance information and addresses, from April 2003 to May 2007.

In July of this year, the LA Times reported that the Kaiser Permanente hospital in Bellflower, CA was fined \$187,500 for failing a second time to prevent unauthorized access to confidential patient information. State officials said Kaiser Permanente Bellflower Medical Center compromised the privacy of four patients when eight employees improperly accessed records.

According to the article, the hospital was previously fined \$250,000 in May for failing to keep employees from snooping in the medical records of Nadya Suleman, the woman who set off a media frenzy after giving birth to octuplets in January.

The fine was the first penalty imposed and largest allowed under a new state law, AB 1298, enacted in 2008 after the violations of privacy at UCLA Medical Center.

California was the first state in the country to pass a data breach notification law with the passing of AB 1298, California again led the nation in privacy by expanding the scope of protecting confidential computerized information to include medical and health information. Approximately 46 states have since implemented legislation relating to the protection of an individual's personal information.

### ARRA and Electronic Health Records

On February 17, 2009, the American Recovery and Reinvestment Act (ARRA), commonly referred to as the Stimulus Act, was signed into law by President Obama. The ARRA includes the Health Information Technology for Economic and Clinical Health (HITECH) Act, which provides over \$19 billion to help the healthcare industry streamline healthcare and reduce costs through the use of health information technology.

The ARRA provides financial incentives through the Medicare B program to help physicians purchase and implement qualifying electronic health records (EHRs) in a meaningful way. Medicare physicians who implement and report meaningful use of EHRs in 2011 will be eligible for an initial incentive payment up

to \$18,000 and payments in subsequent years with a maximum incentive payout of \$44,000 (see chart below). Incentive payments will be reduced in subsequent years, eventually phasing out in 2016.

Physicians who do not use an EHR system before 2015 will not receive any incentive payments and are subject to a reduction in Medicare reimbursements by 1% in 2015, 2% in 2016 and a minimum of 3%, in subsequent years.

<b>EHR - Medicare Incentives Schedule for Physicians</b>					
<b>Incentive Payment Year</b>	<b>2011</b>	<b>2012</b>	<b>2013</b>	<b>2014</b>	<b>2015</b>
2011	\$18k	-0-	-0-	-0-	-0-
2012	\$12k	\$18k	-0-	-0-	-0-
2013	\$ 8k	\$12k	\$15k	-0-	-0-
2014	\$ 4k	\$ 8k	\$12k	\$12k	-0-
2015	\$ 2k	\$ 4k	\$ 8k	\$ 8k	-0-
2016	-0-	\$ 2k	\$ 4k	\$ 4k	-0-
2017 +	-0-	-0-	-0-	-0-	-0-
<b>TOTAL</b>	<b>\$44k</b>	<b>\$44k</b>	<b>\$39k</b>	<b>\$24k</b>	<b>-0-</b>

### **Privacy and Security Requirements**

The HITECH Act was intended to provide assurance to the public that the privacy and security of their patient information is protected. The HITECH Act significantly expands the scope of the HIPAA Privacy and Security rules, including civil and criminal penalties, to business associates – e.g., entities providing services to health care providers, health insurers and other HIPAA “covered entities (CEs)”.

Currently, business associates must sign a contract with a covered entity that requires certain HIPAA provisions by contract. The new legislation will obligate a business associate by law to follow all HIPAA security provisions and not just the minimum included in current business associate contracts.

The HIPAA Security Rules relating to administrative, physical and technical safeguards of electronic PHI (plus new security requirements under the HITECH Act that apply to covered entities ) now apply directly to business associates in the same way that those standards apply to covered entities .

Non-covered HIPAA entities, such as Health Information Exchanges, Regional Health Information Organizations and personal health record (PHR) vendors are now required to have business associate agreements with covered entities (including physicians) if they provide the electronic exchange of patient health information.

### **Additional provisions of the HITECH Act**

#### ***Increased enforcement and penalties***

The legislation substantially increases the civil penalty amounts based on the level and intent of a breach of privacy, e.g., whether the violation was made without knowledge; due to reasonable cause and not willful neglect; or due to willful neglect. The tiers of penalties include:

- Violations determined to be made without knowledge: Penalties start at \$100/not to exceed \$25,000 per calendar year.
- Violations based on reasonable cause: Penalties start at \$1,000/not to exceed \$100,000 per calendar year.
- Violations based on willful neglect: Penalties start at \$10,000/not to exceed \$250,000 per calendar year.
- Violations based on willful neglect and not corrected: Penalties start at \$50,000/not to exceed \$1,500,000 per year.

The legislation requires a formal investigation and imposition of civil monetary penalties for any violations due to willful neglect. While many of the HITECH final rules are not effective until after February 17, 2010, the provisions on increased penalties go into effect immediately.

Lastly, the legislation also gives state Attorney Generals clear and explicit authority to enforce the HIPAA rules on behalf of their residents; permits civil action against an individual or employee that obtains PHI without authorization; and requires the HHS to conduct periodic audits of both covered entities and business to ensure HIPAA compliance.

#### ***Disclosure Restrictions***

Under the HITECH Act, an individual can request that their health care provider not disclose information to an insurer for “payment or health care operations” if the provider has already been paid in full by the individual.

#### ***Accounting requirements***

The HITECH Act requires a covered entity to provide patients, upon request, an accounting of disclosures of PHI made through the use of an electronic health record if related to treatment, payment or health care operations. If an individual requests an accounting of disclosures, a covered entity must be able to provide disclosure information for the prior three years.

#### ***New Marketing Rules***

The HITECH Act prohibits the sale of an individual’s PHI without a valid authorization from an individual except in limited circumstances relating to public health activities, research, treatment, the sale or merger of a covered entity, payment to a business associate for services, providing an individual with a copy or access to their PHI or any other activity deemed necessary and appropriate by the Secretary of HHS.

#### ***Limited Data Sets – Minimum Necessary***

The HITECH Act imposes a new requirement to the “minimum necessary” standard, specifically, requiring a covered entity to limit uses, disclosures and requests for PHI to a “limited data set”, or if more information is needed, to the minimum necessary amount of PHI to accomplish the intended purpose of the use, disclosure or request.

#### ***Security Breach Notification***

Possibly the most significant of the new rules, the HITECH Act requires that covered entities must notify each patient whose *unsecured* protected health information has been, or is reasonably believed by the

covered entity to have been accessed, acquired, used or disclosed as the result of a breach. While previous HIPAA security requirements applied only to electronic health information, the HITECH rules apply to any form or medium of protected health information. The breach notification requirements apply not only to disclosures to third parties, but to unauthorized internal access to PHI.

The regulations require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach “without unreasonable delay and in no case later than 60 calendar days after discovery”. The 60 day clock starts on the first day that the breach is discovered by any employee or member of the workforce or on the first day that such a person reasonably should have known of the breach.

Business associates are now required to notify the covered entity of a security breach not later than 60 days after discovery of the breach, which the covered entity in turn will notify the affected individuals. If a breach affects *500 or more* individuals, covered entities are required to provide a notice in prominent media outlets in the immediate area as well as notify the Secretary of HHS, which will post the name of the breaching entity on its public Web site.

For breaches involving *fewer than 500* individuals, covered entities are required to maintain a log of such breaches and to notify the Secretary on an annual basis. In any case, a covered entity is required to provide notification to any individual who’s PHI has been determined to have been breached.

Exceptions to notification requirements include the “unintentional or inadvertent use of disclosure by employees or unauthorized individuals with the same facility”.

The Act also requires “vendors of personal health records” and “PHR related entities,” to notify their customers of any breach of unsecured, individually identifiable health information as well as the Federal Trade Commission (FTC). A PHR related entity is defined as an entity that (1) offers products or services through the website of a vendor of personal health records; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals PHRs; or (3) “accesses information in a personal health record or sends information to a personal health record.”

### **HITECH Effective Timeframes**

Most of the provisions of the HITECH legislation take effect February 18, 2010; however, obligation to notify applies to all breaches that are discovered on or after September 15, 2009 and increased penalties for HIPAA violations are effective immediately.

### **HITECH Challenges and Preparation**

A November 2009 HIMSS Analytics Report, commissioned by ID Experts, surveyed approximately 176 senior IT executives, Chief Security Officers, Chief Medical Information Officers, Chief Privacy Officers as well as vendor organizations that have business associate relationships with healthcare organizations. Some of the key findings of that report include:

- One-third (31 percent) of hospitals reported having a data breach at their organization in the last 12 months, despite almost all (91 percent) having conducted a risk assessment and taken actions to address identified risks and gaps.
- Business associates are generally unprepared to meet the new HITECH data breach related obligations. Over 30 percent of business associates surveyed did not know the new HIPAA privacy and security requirements have been extended to cover their organizations.
- 85 percent of hospitals indicated they will take action to protect their patient data that is held by a business associate, while a full 39 percent of business associates admitted they did not know what actions hospitals are taking. In addition, business associates were unaware that 47 percent of hospitals would terminate their contracts for violations.

The risks and challenges associated with the HITECH Act are not going away and in fact, enforcement will continue to be more significant and substantial. Steps to prepare for HITECH compliance include:

1. Identify compliance requirements specific to your organization.
2. Perform a risk assessment that includes an inventory of PHI assets, including a thorough understanding of how PHI is collected, managed and shared as well as how it is stored, accessed and secured.
3. Identify and prioritize high risk areas and revise existing privacy and security policies and procedures to address these risks and meet compliance requirements.
4. Ensure employees and third parties receive privacy and information security training and are constantly aware of their responsibility to protect a patient's personal health information.
5. Review existing relationships between covered entities and business associates and develop a contracting and compliance strategy.
6. Develop an effective breach mitigation, detection and response plan that includes internal staff as well as third parties that collect, manage and share PHI.

## **Summary**

The HITECH legislation increases the challenges of protecting an individual's personal health information, but also presents opportunities to increase efficiencies, lower costs and ultimately raise the level of patient care.

Although some questions remain, the HITECH requirements have generally been defined and enforcement provisions are in place. Health care companies and their business associates need to understand how these requirements apply to their organizations and develop strategies to mitigate the risks and ensure compliance.

## **About the Author**

Eric Nelson is a Practice Leader with Lyndon Group serving clients that have needs with privacy and information security. He is a Certified Information Privacy Professional (CIPP) and specializes in federal, state and international privacy and information security compliance and breach mitigation.

Eric a frequent speaker on the subject of privacy and information security through people, policies and processes, has participated on legislative and regulatory committees and served as an advisor to local and state governments. He has contributed to federal identity theft legislation and developed privacy and information security student curriculum currently used by the University of Illinois.

Eric is a member of The Healthcare Information and Management Systems Society (HIMSS), The Association of Contingency Planners (ACP) and an active member of The Privacy Consortium, a collaborative group of leading international privacy experts. For more information visit: [www.Lyndon-Group.com](http://www.Lyndon-Group.com).

*This article is for informational purposes only and none of its content should be construed as legal advice. Readers are encouraged to seek the advice and guidance of legal counsel for review of applicable laws and how they may apply to your organization.*