akrivis LAW GROUP PLLC

Client Alert: July 21, 2014

New Enforcement Provisions of HIPAA HITECH Mandate Stronger Compliance

Teresa N. Taylor
Partner
202.730.1271
ttaylor@akrivislaw.com
www.akrivislaw.com

Background

The recent trend to heighten accountability for data privacy breaches is nowhere more apparent than in the new rules and regulations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), effective March 2013. Health care providers must be in compliance with HITECH by September 2014. Several health care providers and their subcontractors or service providers have already been held accountable for breaches of protected health information ("PHI") and incurred steep fines. All health care providers (or termed "Covered Entities" in the regulations) from solo practitioner's offices to nursing homes and hospitals, to hospice organizations and subcontractors and professional services providers need, stronger compliance programs and notification plans, and should conduct routine assessments and audits in order to mitigate risks and prevent violations.

The Challenges

The regulations mandate the protection and confidential handling of protected health information from any reasonably-anticipated threats, uses, or disclosures, and ensure that its workforce also complies with HIPAA. The HIPAA and HITECH Act are extremely dense regulations which federal courts have termed ostensibly complex on every level. This is compounded by technology and internal human resources challenges, and an insurgence of identity theft. Patient data stored in

various media can contain a patient's complete health history, and that data is easily portable and manipulatable. The situation is further complicated by the identification, de-identification and re-identification processes of PHI, and the new enforcement provisions. The new enforcement provisions mandate strict notification procedures and timelines to affected individuals, and also include notification to the Secretary of Health and Human Services, and now hold individual employees as well as third party business associates accountable for each occurring violation.

The rules further mandate that covered entities and business associates implement specific safeguards to protect against disclosure of PHI pursuant to the HIPAA and HITECH rubrics. Specifically, these include:

- Administrative Safeguards (policies, procedures, risk analysis, formalized reporting, and disaster recovery plans);
- Physical Safeguards (restricting access to and ensuring the availability of information systems, and formulating policies for receiving, handling, reusing, and disposing of media containing health information);
- Technical Safeguards (proper authorization, authentication, confidentiality, integrity, auditing, and identification).

Identity thieves unfortunately use automated tools to target small to mid-sized businesses with weak controls. The new enforcement provisions of HITECH are therefore of special importance for these types of companies.

Enforcement

HITECH modifies the HIPPA Enforcement Rule to incorporate an increased and tiered civil monetary penalty structure. The system is designed around the level of knowledge with regards to the violation. Violations with no knowledge are assigned the lowest penalty, while violations with an element of "willful neglect" are assigned the highest penalty. The maximum fines per person, per year, and per violation range from $25,000 to $1,500,000. Because companies and individuals can separately and simultaneously be held accountable criminally and civilly the fines can stack up quickly, particularly where there are multiple violations stemming from a single breach action (such as where an employee steals multiple patient files, or a database is hacked into, or even where an employee negligently shares patient information from several files with a third party in violation of the regulations).

Like HIPPA, HITECH does not allow a private cause of action against a provider. Unlike HIPPA, however, HITECH it does grant the deferral of authority from federal prosecutors to state attorneys general when desired to bring civil law suits on behalf of state citizens for HIPPA violations, and this is in addition to the power of state attorneys general to independently bring suits under state law. HITECH also allows state attorneys general to obtain damages on behalf of state residents or to enjoin further violations of the HIPPA Privacy and Security Rules. Additionally, government audits for compliance are no longer triggered by data breaches, although 25% of all audits are now random.

Recent Cases

Several significant fines and settlements have occurred in recent places.

- February 2011, the Health and Human Services Office of Civil Rights imposed a $4.35 million fine on Cignet Health of Prince George's County, MD, for failing to provide patients with access to requested medical records and failure to cooperate with investigators.

- July 2011, UCLA Health Systems agreed to pay $865,500 to settle complaints of repeated unauthorized access of electronic protected health information.
- March 2012, Blue Cross Blue Shield of Tennessee agreed to pay $1.5 million after 57 unencrypted laptops containing protected health information on more than 1 million individuals were stolen from a leased facility.
- June 2012, the Alaska Department of Health and Social Services agreed to pay $1.7 million after the Office of Civil Rights found that they failed to have proper policies and procedures pursuant to the rules and regulations, failed to perform an adequate risk analysis, failed to implement appropriate device and media controls, and other violations of HIPAA.

Once HITECH's compliance deadline ticks in September 2014, we will no doubt again see an insurgence of state and federal investigations, prosecutions, civil suits, and settlements given that prosecutors and government officials realize that noncompliance cases equate to easy cases to prosecute with hefty fines to collect. Federal prosecutors have been trained over recent years to step up prosecution of regulatory compliance violations for this very reason.

More recently, over the course of this year alone the Department of Health and Human Services has continued to aggressively pursue violations of HIPAA, settling numerous cases for amounts ranging from six figures to nearly $5 million dollars. Health care providers both large and small needed to resolve their liability for patient privacy breaches. The most common cause of violations was a failure to secure electronic databases and information. For example,

- August 2013, Affinity Health Plan spent $1.2 million dollars to settle a breach of over 344,579 individuals' privacy information that was left on a leased photocopier which was thereafter leased to CBS Evening News.
- April 2014, Concerta Health incurred nearly $2 million dollars in fines for a settlement regarding information left on unencrypted laptops which were stolen from employees.

Even when employing safeguards, health care providers faced risks from technological failures and system glitches. In the cases of WellPoint, in July 2013, and NYPH/CU, in May 2014, both organizations suffered severe penalties of $1.7 million and $4.8 million in 2013 from problems with their online databases that released personal information to unauthorized individuals on the internet.

Impact on Small Businesses

No case appears too small for HHS to target and hold entities accountable. Shasta Regional Medical Center settled for $275,000 where two employees who were concerned about the medical treatment a patient was receiving spoke to the media without written authorization; the HHS found that the center did not have proper security measures in place, nor did it properly discipline the employees. Adult Pediatric Dermatology, P.C., of Massachusetts paid $150,000 to settle potential violations of HIPAA where an employee's unencrypted thumb drive was stolen from his car and never found. In a breach involving less than 500 patients where a laptop was stolen, the Hospice of North Idaho paid $50,000. In the face of rapid changes in technology, the risk of liability continues to increase in remarkable ways, as these recent cases illustrate.

Third Party Business Associates

HIPAA did not previously hold accountable third parties and other business associates or subcontractors for regulatory violations. Under the new HIPAA and HITECH rules, business

associates of covered entities are directly regulated; and the existence or absence of a contract with a third party is no longer the deciding factor on whether a third party is actually a business associate or not. The deciding factor remains whether a third party fits within the definition of a business associate as defined in the regulations. HITECH now applies certain HIPPA provisions directly to business associates.

Notably, the Final Rules modified the definition of a business associate. A business associate is defined as a person who on behalf of a covered entity creates, receives, maintains, or transmits protected health information or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity. Business associate includes:

1. A Health Information Organization, E-Prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information;
2. A person that offers a personal health record to one or more individuals on behalf of a covered entity; and
3. A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

Business associates are now subject to and responsible for complying with the provisions and regulations of HIPPA, and are now directly liable for civil and criminal penalties. Specifically, business associates are liable under the HIPPA rules for:

1. Impermissible uses and disclosures of protected health information; Failure to provide breach of notification to the covered entity;
2. Failure to provide access of electronic protected health information to either the individual or covered entity;
3. Failure to disclose protected health information to the Health and Human Services;
4. Failure to provide an accounting of disclosures; and
5. Failure to comply with the requirements of the HIPPA Security Rule.

Other Major Provisions:

HITECH and the Final Rules also severely strengthen the limitations on the use and disclosure, notification, and retention rules of PHI in the following additional areas:

- Marketing, Fundraising, and Sale of Protected Health Information;
- Access of Individuals to Protected Health Information;
- Right to Request a Restriction;
- Student Disclosures;
- Decedents;
- Breach Notification Rule; and
- Notice of Privacy Practices.

akrivis LAW GROUP PLLC

New Enforcement Provisions of HIPAA HITECH Mandate Stronger Compliance

Conclusion

With the expansion of HIPPA regulations comes the risk of increased liability, particularly with the scope of applicability now expanded to include business associates. Many persons, employees, and companies will now find themselves exposed to greater liability. Failure to comply with the new HIPAA and HITECH provisions will likely prove to be damaging as fines are steep and breach notification to affected parties may be very costly. Insurance will not absolve a person or company from liability and accountability. Damage to a company's reputation before the public could be greater still, particularly given the complex notification rules and mandated public disclosure to the Secretary of Health and Human Services. It is far more prudent for companies to invest in a strong compliance program and training, and to engage in routine independent assessments and audits than to run afoul of HIPAA and HITECH and incur high civil and criminal penalties by federal and state prosecution.

Akrivis Law Group, PLLC is experienced with providing independent compliance, audit, and investigatory representation to various companies, and is experienced in defending them during civil and criminal prosecution. We understand the competing demands and challenges companies face amidst regulatory compliance, and know how to mitigate liability and avert costly violations in a highly efficient manner.