Reprinted from
CORPORATE COMPLIANCE INSIGHTS
February 17, 2012 www.CorporateComplianceInsights.com

How To Reduce HIPAA and HITECH Compliance Risks

by **Jo-Ellyn Sakowitz Klein**

About The Author

Jo-Ellyn Sakowitz Klein is senior counsel at Akin Gump Strauss Hauer & Feld LLP, where she leads the firm's interdisciplinary privacy and data protection initiative. Ms. Klein devotes much of her practice to regulatory, transactional and legislative matters affecting the health industry. She also advises clients outside the health sector that are affected by health care or privacy laws and regulation.

With enforcement activity on the rise, including multiple settlements and the launch of a new audit program, many entities are reassessing their approach to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

Entities that fit neatly within the HIPAA mold – such as health plans, health care providers such as hospitals, and other traditional HIPAA covered entities – are evaluating the effectiveness of existing compliance programs, while other entities in the health sector and beyond are considering with new urgency what HIPAA and HITECH mean for them.

HIPAA

HIPAA and its implementing regulations create a complex federal scheme that protects the confidentiality of health information, layered atop more stringent state laws. Enacted in 1996, HIPAA was implemented through primary rulemakings generally taking effect in 2003 (privacy rule) and 2005 (security rule).

At its core, the privacy rule focuses on the extent to which a covered entity can use and disclose protected health information without authorization from the individual, and creates certain individual rights. The security rule focuses on the administrative, physical, and technical safeguards an entity must have in place to ensure the confidentiality, integrity, and availability of electronic protected health information. In the early days of HIPAA, regulators emphasized voluntary compliance and education, and the initial enforcement strategy was largely complaint-driven.

HITECH

The HITECH Act overhauled HIPAA in 2009, dramatically increasing risks for affected entities. HITECH created new privacy restrictions, extended HIPAA's reach to more entities, increased penalties, created new enforcement mechanisms and established a new federal breach notification requirement.

One of the most significant changes to the HIPAA regime under HITECH is the extension of liability to business associates, in addition to covered entities. HIPAA always applied directly to health plans, health care clearinghouses and certain health care providers, and, through mandatory contracting, those servicing covered entities – "business associates" – agreed to maintain the privacy and security of protected health information received in the course of performing their duties.

A business associate's liability was limited to the four corners of its agreement: HIPAA did not apply directly to business associates. New under HITECH, business associates are treated as covered entities. In addition to contractual liability, they will also face direct liability to regulators for penalties if they fail to comply with HIPAA privacy and security requirements.

How to Reduce HIPAA and HITECH Risks

Not surprisingly, tensions are running high among many entities affected by HIPAA and HITECH. This past year brought a rash of enforcement actions and regulators are now rolling out an audit program pursuant to HITECH.

Adding to uncertainty, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has been slow to issue final HITECH regulations. Most notably, the main rulemaking to implement the privacy and security aspects of HITECH, which was proposed in July 2010, has stalled.

The top five steps an entity can take now to reduce HIPAA and HITECH risks are:

• **Know your HIPAA status.** Most covered entities are aware of their HIPAA status, but some companies may be surprised to find that an operating unit or subsidiary may satisfy the definition of a HIPAA health plan or otherwise be engaged in covered functions, warranting further analysis. Similarly, post-HITECH, it is important for entities providing services for (or on behalf of) covered entities to seriously consider whether they satisfy the regulatory definition of "business associate," and to confirm that appropriate steps have been taken to come into compliance if they do.

• **Know your data flows.** The key to HIPAA compliance is to understand how data flows within, into, and out of your organization. A critical task in developing and maintaining a compliance program is to know the answer to one simple, but loaded, question: How does your organization collect, create, receive, use, disclose, maintain, store, transmit and destroy health information that is protected by HIPAA? Take it a step further and break down the "how" into "who," "what," "where," "when," "why," and "how." Who collects data? Where is data stored? Who needs to use it? Do this and you will be positioned to identify most of the HIPAA-related risks that face your organization.

• **Learn from mistakes.** Learn from your organization's mistakes, as well as from the mistakes of others. In the wake of a breach, take time to reflect and update policies and procedures to prevent similar problems in the future. Follow through by providing targeted training for workforce members. Learn from the mistakes of others by reviewing recent OCR resolution agreements and scrolling through breaches reported on the HITECH breach notification site maintained by OCR, and asking whether the fact patterns presented could manifest at your organization. Bolster your policies and procedures and provide appropriate training for workforce members to prevent similar breaches from occurring at your organization.

• **Prepare for auditors.** OCR has launched a pilot HIPAA privacy and security audit program pursuant to HITECH, and covered entities should be prepared to receive a letter indicating that they have been selected to participate. Up to 150 entities will be audited by the end of this year. Each audit will involve a site visit and result in an audit report. Notably, audited entities will be expected to provide requested documentation of their HIPAA compliance efforts within ten business days of being notified of the audit. To prepare, many entities may find it helpful to conduct a self-assessment. HIPAA-mandated documentation should be reviewed to ensure that it is complete, accurate, and readily available. In particular, entities should confirm that all required policies and procedures are in place and align with actual practices, and that appropriate workforce training has been conducted and documented. Steps taken to prepare for a possible audit will enhance compliance and reduce risks, regardless of whether an entity is ultimately selected to participate in the pilot program.

• **Prepare for breaches.** Covered entities and business associates should develop and implement practical breach response plans that detail what will happen when a data incident occurs. Importantly, roles and responsibilities of individuals within the entity should be clearly defined and appropriate training provided. Business associate agreements should be reviewed to ensure the plan comports with contractual obligations.

Common Health Care Compliance Pitfalls

Entities affected by HIPAA and HITECH should be careful to avoid some common compliance pitfalls:

• Do not wait for regulatory certainty to act. While HIPAA compliance would probably be much easier if regulators had adopted final regulations implementing the HITECH Act, entities can take many steps to reduce HIPAA-related risks in their absence. Privacy and data protection law is developing fast and uncertainty abounds. Accept it, and move on.

• Do not leave the shrink-wrap on HIPAA policies. If your organization bought a HIPAA compliance tool kit that is sitting on someone's shelf with the shrink-wrap still intact, you have some work to do. HIPAA policies and procedures must be tailored to your organization and they must be operationalized. HIPAA compliance is more than being able to point to a binder on a shelf.

• **Do not rely on an outdated risk assessment.** You cannot solve a problem you do not know you have. It is vital to work from a risk assessment that accurately reflects your current operations and data flows. How often an entity should conduct a risk assessment will depend on the facts and circumstances of its environment. For some entities once every three years may suffice, but others may find it necessary on an annual basis.

• **Do not be seduced by technology and forget the simple stuff.** Encryption, access controls and strong password protection are all important, but simple physical safeguards – like having locks on drawers and ensuring secure disposal of paper, pill bottles and other items containing protected health information – can make the difference between a ho-hum day at the office and finding your organization on the five o'clock news as reports of a data breach break.

• **Do not contract in haste.** Since HITECH extended HIPAA to apply directly to business associates, business associate agreements have taken on a life of their own, at times competing in length and complexity with the agreement memorializing the underlying service relationship. In this new HIPAA era, issues such as indemnification and audit rights may loom large, and particular care should be taken to distill roles and responsibilities in the event of a data breach. Business associate agreements – and all other HIPAA-related contracts – should be approached thoughtfully, with due consideration given to all risks presented.

In short, covered entities and business associates should take stock of their HIPAA compliance efforts and consider whether opportunities exist to reduce risks. Recent changes in health information privacy and data security law and enforcement reflect broader trends that are playing out in other sectors in the U.S. and across the globe. Those affected by HIPAA and HITECH should take action to stay ahead of the curve.