



CONNER  
STRONG &  
BUCKELEW

legislativeUPDATE

August 23, 2013

## General Compliance Date for the HIPAA Final Rule Grows Near

September 23rd 2013 marks the general compliance enforcement date for the Final Rule of the Omnibus Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The Final Rule published early this year clarifies and implements changes enacted by the Health Information Technology for Economic and Clinical Health (HITECH) Act and finalizes HIPAA’s privacy, security and enforcement rules. The Final Rule also makes changes to the definition of business associate, breach notification requirements and restricts the use of genetic information for underwriting purposes. While the majority of the Final Rule addresses providers of healthcare, some of the provisions of the law may require employer-sponsored health plans to make conforming changes to existing HIPAA policies and documents. Employers should examine current HIPAA compliance practices and determine if changes are needed to comply with the final rules. This Legislative Update addresses how the Final Rule may impact employer-sponsored group health plans subject to the HIPAA privacy, security and HITECH rules.

### **HIPAA General Background**

HIPAA is a massive law and the privacy, security and HITECH rules fall under HIPAA’s administrative simplification legislation. Specifically, the privacy and security rules determine how certain health information is used, maintained, disclosed and transmitted. HIPAA is not a blanket privacy law covering all privacy situations; the HIPAA privacy and security rules apply exclusively to “covered entities,” a term defined under the law that includes health plans, healthcare clearinghouses (organizations that process health information) and healthcare providers. A health plan under the HIPAA rules is any plan that provides or pays the cost of medical care, which includes major medical plans, prescription drug, vision, dental, health flexible spending accounts, health reimbursement accounts, certain employee assistance programs and long-term care plans that offer medical benefits.

HIPAA HITECH rules place many HIPAA compliance responsibility directly on business associates. A business associate is any entity that performs a service for the covered entity and has access to “protected health information” (PHI). The privacy and security rules place restrictions on how covered entities and business associates can use and disclose PHI in any form. Any individually identifiable health information used, held or transmitted by a covered entity is PHI. Group health plans and business associates with access to PHI must protect and safeguard this information as prescribed under the HIPAA rules.

### **How Do the HIPAA Privacy and Security Rules Apply to Employers?**

Employers sponsoring group health plans are responsible for their plan's HIPAA compliance. An employer's administrative practices and funding arrangement (self-insured or fully-insured) heavily influences the level of a plan sponsor's HIPAA compliance obligations. Employers with fully-insured health plans and no access to PHI have limited HIPAA compliance obligations and in these cases, many HIPAA responsibilities rest with the insurer. It's important to note that just having a fully-insured health plan does not remove a health plan sponsor (employer) from HIPAA compliance obligations and employers must truly take a "hands-off" PHI approach to limit HIPAA compliance obligations. Employers who self-insure any portion of their health plan, even if the employer uses a third party administrator, are required to comply with the relevant HIPAA obligations. Employers are encouraged to thoroughly understand their access, use, maintenance, and disclosure of PHI to correctly understand and comply with HIPAA rules. If the employer has any access to any PHI in connection with their group health plan administration, the employer must take measures to comply with the applicable HIPAA privacy and security rules. Primary HIPAA obligations that plan sponsors with access to PHI through health plan administration must adhere to include:

1. Assigning a privacy/security official to enforce and oversee HIPAA obligations.
2. Designating specific employees to have access to PHI and restricting access of PHI only to those individuals.
3. Training affected employees on permitted usage of PHI and requiring employees to use PHI as permitted under the HIPAA rules.
4. If electronic PHI is used, maintained, or disclosed, implementing the proper safeguards to protect the integrity of the information.
5. Issuing Privacy Notices, as required, to plan participants at the appropriate intervals.
6. Notifying plan participants of breaches when required.
7. Determining all business associates and having HIPAA-compliant Business Associate Agreements (BAAs) for all business associates.
8. Establishing policies and procedures for designated employees who use PHI for plan administration purposes and for individuals who exercise their rights under the HIPAA rules.
9. Amending other plan documents as needed.

### **Changes in the Final Rule Likely to Impact Employer-Sponsored Health Plans**

In addition to the above requirements, plan sponsors with access to PHI through health plan administration must incorporate the Final Rule in HIPAA compliance initiatives. The final HIPAA guidance includes many important changes that will likely impact employer-sponsored health plans and their HIPAA administrative practices. Key areas of the rules that will likely impact employer sponsored health plans include:

**Changes to the Privacy Notice:** Group health plans with access to PHI should determine if they are required to update their plan's Privacy Notice. In addition to the existing Privacy Notice content requirements, the latest guidance requires that Privacy Notices are updated to reflect:

- **Updates to the "Uses and Disclosures" statements as needed** – Every Privacy Notice is required to tell participants through the Notice how the plan will use and disclose PHI. According to the Final Rule, Notices must inform individuals that the use of most psychotherapy notes and the use of selling and marketing PHI (that is not done for healthcare operations) will require the individual's authorization.
- **Breach Notification** – Individuals must be informed of their right to received a notice

when there has been a breach of his or her unsecured PHI.

- **No genetic information used for underwriting** – The Generic Information Nondiscrimination Act (GINA) prohibits the use of genetic information in many situations. If a health plan uses or discloses PHI for underwriting purposes, the Privacy Notice must contain a statement that the plan will not use genetic information for underwriting purposes.
- **Right to opt out of fundraising** – The Privacy Notice must contain a statement that the individual has a right to opt out of fundraising communications if applicable.
- **Paying out of pocket (typically for providers of healthcare)** – HITECH rules require providers to agree to not disclose any PHI for any services paid in full by the individual.

Privacy Notices must be updated in accordance with the Final Rule no later than September 23, 2013. Notices previously updated for the 2010 HITECH rules may need limited updates to comply with the final rules. If the Privacy Notice is maintained on a website, the plan must post the revised Notice no later than this date and provide the updated Notice in the next annual mailing to plan participants. If the Notice is not maintained on a website, the company must issue the revised Notice within 60 days of any change, i.e., within 60 days after September 23, 2013.

**An expansion of the definition of Business Associates:** The Final Rule has expanded the definition of business associate to include:

- **subcontracts** - any subcontractor of the business associate that has access to PHI. Each subcontractor, contracting with another subcontractor must enter into a BAA if the subcontractor has access to PHI. The requirement continues on a “downward stream” and must encompass every subcontracting relationship where PHI is used, maintained, transferred and disclosed. The business associate must enter into the agreement directly with the subcontractor and subcontractors have to enter into BAAs with other subcontractors. The covered entity is not required to have a direct BAA with the subcontractor of a business associate.
- **document and data storage entities** – entities that maintain PHI for a covered entity in electronic or physical form, regardless of whether or not the entity assesses the PHI, will be a business associate of the covered entity.
- **organizations that provide data transmission services** – any entity that provides the covered entity with PHI data transmission services and has regular access to the PHI. There is a small exception which excludes entities that act as “conduits for the transportation of PHI” and that only access PHI on an irregular and infrequent basis.
- **personal health record vendors** – vendors that manage or provide personal health records to the covered entity. Vendors that provide the records directly to the individual are not considered business associates of the covered entity.
- **financial institutions** – this refers to institutions that provide services to the covered entity which go beyond payment processing activities. For example, if a financial institution has access to accounts receivable information that includes PHI, this financial institution may be considered a business associate of the covered entity.

**Requirement to Amend BAAs:** A covered entity whose partnership with another entity involves the use or transmission of PHI is required to have a BAA with the business associate. The Final Rule may require some updates to existing BAAs and covered entities should work with their business associate to make sure contracts are compliant. The Department of Human and Health Services (HHS) issued a [sample BAA](#) for covered entities to use when updating BAA policies.

BAAs compliant with the Final Rule should require the business associate to adhere to HIPAA security rules, include language that notes the business associate will enter into a BAA with subcontractors as needed, hold subcontractors to the same standards as the business associate with respect to how PHI is used, created, maintained and transmitted and require the business associate to report breaches to the covered entity.

If a BAA was effective after January 25, 2013, the BAA must comply with the HIPAA Final Rules by September 23, 2013. HIPAA compliant BAAs in effect prior to January 25, 2013, that have not been modified or renewed (except by an automatic renewal) between March 26 and September 23, 2013, are eligible for a special transition rule. This transition rule provides that the BAA must be amended by the earlier of –

- the date of the renewal or modification
- or by September 22, 2014

BAAs that do not meet the conditions under the special transition rule have to be updated by September 23, 2013.

**Updated Breach Rules:** Under the old rules, a breach had to pose a “significant” financial or reputational risk, or other harm to the individual whose PHI was breached to trigger a breach notification to the individual. Under the Final Rule, the “harm threshold” is removed and covered entities and business associates must consider any unauthorized acquisition or disclosure of PHI a breach and issue a notice to the affected individual except in cases where the covered entity (or business associate) can demonstrate, through a risk analysis that there was a low probability that the PHI was compromised. The risk analysis the covered entity is expected to perform must consider the nature and extent of the PHI, the person who made the unauthorized access of PHI or the unauthorized disclosure, whether or not the PHI was actually acquired or viewed, and determine the extent of which the breach risk was mitigated.

**No Use of Genetic Information for Underwriting Purposes:** The Genetic Information Nondiscrimination Act (GINA) places restrictions on how employers can use genetic information. Genetic information includes an individual's and family member's genetic test, genetic counseling, and the appearance of a genetic disease in an individual or family member. The Final Rule prohibits plans from using genetic information for underwriting purposes. Plan activities such as eligibility determinations, enrollment in benefits, premium determinations, employee contribution amounts, and applying any pre-existing condition exclusion (which will be prohibited in 2014) are considered underwriting activities and plans are prohibited from considering genetic information in performing any of these activities.

### **Revised Enforcement Rules Place More Employers at Risk for HIPAA Violations and Penalties**

The Final Rule made changes to HIPAA Enforcement Rules and these changes, coupled with the more relaxed breach notification standards, are likely to increase the level of HIPAA violations and audits by the Office of Civil Rights (HHS' HIPAA enforcement division), as well as result in more penalties assessed to covered entities and business associates. Previously, HHS was required to try to resolve investigations of complaints and compliance reviews by informal means. One major change to the Enforcement Rule is that informal resolution is now discretionary. This gives HHS the right to move directly to penalty proceedings for covered entities with HIPAA violations.

The second major change to the Enforcement Rule is that HHS is now permitted to impose a penalty on a covered entity for a violation of its business associate when the business associate is a covered entity's agent. This is an important change for employers who self insure and use a third-party administrator (business associate) to administer benefits. Often in these types of arrangements the employer delegates many HIPAA compliance obligations to the third-party administrator, which may, through specifications in the BAA, make the business associate an agent of the covered entity. Under this arrangement, a covered entity may face penalties and fees for the actions of a business associate acting as the covered entity's agent. In general, a business associate would be an agent if the covered entity had the authority to direct the performance of the service provided by the business associate after the relationship was established.

Covered entities complying with the more relaxed breach notification requirements may have to report breaches to HHS more often than before. This increased reporting obligation may mean an increased risk of enforcement audits from HHS.


### **What Should Employers Do Next?**

Employers sponsoring group health plans should carefully review their plan administrative practices to determine how the HIPAA privacy, security and HITECH rules apply to their group health plan. Employers sponsoring group health plans with any access to PHI should:

- Examine all business partner relationships to determine if additional business associates exist based on the expanded definition of business associate under the Final Rule.
- Review the plan's Privacy Notice and update the Notice as needed. If changes are required to the existing Privacy Notice, plan sponsors should put measures in place to ensure new Notices are distributed timely.
- Ensure all BAAs are amended as needed and reflective of the Final Rule as of the compliance effective date.
- Update policies and procedures to align with the additional requirements imposed by the Final Rule if applicable.
- Train employees with access to PHI on the new breach analysis and requirements.
- Review current HIPAA practices and documents to ensure there are no additional HIPAA compliance gaps.

Should you have questions regarding the Final HIPAA Rule or any other area of compliance, please contact your Conner Strong & Buckelew account representative. For a complete list of Legislative Updates issued by Conner Strong & Buckelew, please visit our online [Resource Center](#).

 [connerstrong.com](http://connerstrong.com)

 877-861-3220

 [news@connerstrong.com](mailto:news@connerstrong.com)

 [Change My Preferences](#)

**CONNER  
STRONG &  
BUCKELEW**

INSURANCE | RISK MANAGEMENT | EMPLOYEE BENEFITS

 in

[Click here to change your email preferences or unsubscribe from all communication.](#)