

## Employers Offering Health Benefits Can No Longer Ignore HIPAA

### Recent Changes Provide for Affirmative Public Disclosure of Privacy Breaches, Significant New Penalties, New Obligations Under HIPAA and the Expansion of HIPAA's Reach to Business Associates

If you are an employer offering health insurance to your employees (a Health Plan Sponsor), you know that your group health plan (including any medical, dental, vision and health FSA benefits) is considered a "covered entity" under the HIPAA privacy and security rules. For many of you who are Health Plan Sponsors, HIPAA privacy and security compliance was a one-time event involving a plan amendment, a few changes to vendor agreements, a notice to plan participants and some training. You may even have draft privacy policies somewhere on your desk. *[Who even remembers what HIPAA stands for anyway?]* Unfortunately, Health Plan Sponsors can no longer ignore HIPAA. *[By the way, in case you forgot, HIPAA stands for the Health Insurance Portability and Accountability Act of 1996.]*

### Overview of Key Changes

Recent changes to HIPAA - many of which are effective in February 2010 - mean that Health Plan Sponsors should renew their focus on HIPAA privacy and security compliance now. As is explained in greater detail below, there are three main reasons for Health Plan Sponsors to care about HIPAA privacy and security compliance again:

- > Most breaches of HIPAA-protected information (referred to as protected health information or PHI) must now affirmatively be disclosed to the affected individuals, the government and, in some cases, prominent media outlets.
- > The penalties for a breach of HIPAA's privacy and security rules have increased significantly and the federal government is "on record" that enforcement will become a higher priority. In addition, Health Plan Sponsors can now be directly sued by a state attorney general for HIPAA violations.
- > HIPAA imposes new requirements on group health plans and its reach has been expanded to apply directly to many of the entities Health Plan Sponsors contract with (*i.e.*, business associates) to offer health benefits to their employees.

This client alert focuses on these recent HIPAA-related changes and how they affect Health Plan Sponsors (as the representative of the employer's group health plan, which

is a covered entity under HIPAA). A list of recommended steps that a Health Plan Sponsor should take in response to these developments is included at the end of this alert. Drinker Biddle also prepared a client alert in September 2009 entitled “Covered Entities and Business Associates Must Comply with New Federal Notification Requirements for Breaches of Unsecured Protected Health Information” that focuses on the impact of the new breach reporting rules (as they apply to all types of covered entities). Click [here](#) to view a copy of the alert.

---

## More Detail on the Key HIPAA Changes

The law that is responsible for many of these changes is contained in the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and interim final regulations issued by the Department of Health and Human Services (HHS). A refresher of key HIPAA terms is provided in the chart on page 6.

**Notification of Breach of Unsecured PHI:** Under pre-HITECH Act HIPAA rules, a group health plan was required to disclose a breach of the privacy rules to an affected individual if that person exercised his or her right to an accounting of disclosures but group health plans were not subject to a general affirmative duty to report such disclosures. The HITECH Act creates a new, affirmative notice requirement for Health Plan Sponsors and business associates that discover a breach of an individual’s “unsecured” PHI *if* such breach constitutes significant risk of financial, reputational or other harm to an individual. Following a discovery of a potentially harmful breach of unsecured PHI, a covered entity must notify the individuals affected by a breach, HHS and, in certain circumstances, prominent local media outlets. These notifications generally must be made without “unreasonable delay” and no later than 60 days after discovery of the breach (although annual reporting to HHS of aggregate data is permitted for breaches affecting fewer than 500 individuals). Similarly, business associates are required to notify the Health Plan Sponsor of any potentially harmful breaches of unsecured PHI. Note that the reporting obligation is triggered on the date *anyone* within the organization has knowledge of the breach – meaning that Health Plan Sponsors should take affirmative steps to ensure that a plan’s workforce is appropriately trained to report breaches to the plan’s privacy official.

In August 2009, HHS issued interim final regulations providing guidance on how to secure PHI and comply with the notification requirements if there is a breach of unsecured PHI. Generally, PHI is “secured” (and therefore not subject to the breach notification rules) if the PHI is encrypted or destroyed using technology standards approved by HHS. Health Plan Sponsors will want to evaluate whether it is appropriate to secure PHI using the new standards. If PHI is not secured, Health Plan Sponsors should review and update their privacy and security policies and procedures to ensure timely identification and reporting of breaches. Implementation of other safeguards and thorough training of the plan’s workforce may go a long way to avoiding breaches that would trigger the notice obligations. Health Plan Sponsors also will need to coordinate with their business associates to ensure timely notification of breaches.

**Increased Penalties and Enhanced Enforcement:** The framework of civil monetary penalties and enforcement is expanded under the HITECH Act. Under the new structure:

(1) higher federal civil monetary penalties apply, with minimum penalties varying based on the person’s level of culpability (see the chart on page 6);

(2) previously available affirmative defenses are modified, and generally only available if a violation is corrected (*i.e.*, if a Health Plan Sponsor exercises reasonable diligence to comply and discovers a violation but takes no steps to correct such violation, the Health Plan Sponsor will likely be penalized);

(3) HHS must formally investigate any complaint that suggests a violation due to willful neglect and must impose civil monetary penalties for violations that result from willful neglect; and

(4) state attorneys general are authorized to bring civil actions on behalf of state residents in federal district court for HIPAA privacy and security rules violations to obtain injunctive relief or financial damages (\$100 per violation up to \$25,000 for all similar violations within a calendar year).

**Direct Application to Business Associates:** Not only does the HITECH Act impose new obligations on group health plans, it also for the first time directly regulates HIPAA business associates that have access to health plan participant information in the course of performing services for the group health plan. A Health Plan Sponsor typically has relationships with many business associates including third-party administrators, accounting firms, law firms, insurance brokers and consulting firms. Although business associates have traditionally been bound by a contractual obligation to adhere to the specific privacy and security terms in a written business associate agreement, the HITECH Act requires that some of the HIPAA privacy rule requirements and many of the HIPAA security rule standards, for administrative, physical and technical safeguards and policies and procedures and documentation requirements, apply directly to business associates in the same way as those standards have previously been applied to covered entities. Business associates are now subject to the same penalties and enforcement mechanisms applicable to group health plan.

**Other Changes to Note:** As is mentioned above, Health Plan Sponsors should be aware that the HIPAA privacy and security rules have also been expanded as follows:

- > **Changes to the Minimum Necessary Rule.** Health Plan Sponsors must already comply with the minimum necessary rule when disclosing PHI to others. Under the HITECH Act, HHS is required to issue guidance regarding what constitutes the “minimum necessary” amount of PHI which may be used or disclosed to accomplish the purpose of such use or disclosure. Until that guidance is issued, a Health Plan Sponsor must limit its use and disclosure of PHI to information in a “limited data set,” to the extent practicable. A limited data set excludes direct-identifiers, but allows disclosure of more information than pure “de-identified information.” For example, a limited data set may include certain potentially identifying information such as birth date, admission and discharge date, and certain elements of an individual’s address.
- > **Expanded Accounting of Disclosure Requirement.** Prior to HITECH, a Health Plan Sponsor didn’t have to worry about making an accounting of disclosures for purposes of treatment, payment or health care operations. HITECH limits this exception and once this provision is effective (2011 at the earliest), Health Plan Sponsors will be required to include disclosures of PHI contained in electronic health records when disclosed for purposes of treatment, payment or health care operations. The accounting must include information about disclosures made during the three-year period ending on the date of the accounting request. HHS is required to issue regulations implementing this requirement.

- > *Individuals Have Increased Access to PHI and Can Restrict Disclosures.* Under the HITECH Act, individuals may request electronic access to PHI maintained in electronic health records and may request the electronic transmission of such electronic health record to a designated third party. Additionally, an individual may direct a provider not to share the individual's PHI with the individual's group health plan if the individual pays for the item or service in full, out-of-pocket (prior to the HITECH Act, providers were not required to implement such restriction requests); this requirement does not apply to disclosures for treatment purposes.
- > *There Are Also New Restrictions on the Sale of PHI and an Expanded Definition of Marketing.* While these rules are applicable to all covered entities, the traditional group health plan may not be affected significantly by this rule change. Several provisions in the HITECH Act appear designed to allow traditional group health plan activities (*e.g.*, disease management and wellness programs) to continue unaffected by the marketing restrictions, but more guidance from HHS on the application of these restrictions to group health plans would be helpful.

---

## Interaction of GINA and HIPAA Privacy

The Genetic Information Nondiscrimination Act of 2008 (GINA) restricts the use and disclosure of genetic information and required HHS to modify the HIPAA privacy rules to implement corresponding changes. GINA includes a number of other changes affecting group health plans, especially wellness programs. Click [here](#) to view the Drinker Biddle client alert on GINA and wellness programs.

GINA makes explicit that PHI includes an individual's genetic information (this was previously HHS's interpretation but the new law is helpful confirmation). In addition, GINA generally prohibits group health plans from using or disclosing genetic information for "underwriting purposes." Genetic information means, with respect to a particular individual, the individual's (or his/her family members') genetic tests, the manifestation of a disease or disorder in the individual's family members or any request for (or receipt of) genetic services by the individual or any family member of the individual. Genetic information *does not* include information about a disease or disorder manifest in the individual himself/herself. Underwriting purposes is broadly defined and includes anything related to eligibility determinations (including enrollment), adjustment of cost-sharing mechanisms and application of any pre-existing condition exclusion as well as any other activity related to the creation, renewal or replacement of coverage. Prior to GINA, the HIPAA privacy rule broadly permitted a variety of uses and disclosures for payment and health care operations that would fall within the scope of underwriting purposes and Health Plan Sponsors should update their policies and procedures to reflect the new restrictions. HHS has issued proposed regulations to implement GINA's requirements (published October 7, 2009). If the proposed rules are finalized, these regulations would require group health plans to include a statement about the prohibition on the use of genetic information for underwriting purposes in the plan's notice of privacy practices.

---

## Effective Dates

The effective dates of these provisions vary. The higher civil penalties are effective now. The breach notification rules became effective September 23, 2009. Most of the

remaining HITECH provisions are effective February 17, 2010, although some provisions will take effect at various times over the next several years as additional guidance is issued (such as the expanded accounting of disclosure requirement). GINA's restrictions are generally effective for plan years beginning on or after May 21, 2009.

---

## Health Plan Sponsor Action Required

Health Plan Sponsors should review their prior HIPAA privacy and security compliance efforts, determine where there may be compliance gaps, and implement updated policies and procedures. Action steps include:

- Reviewing existing business associate agreements and implementing new agreements (which will be necessary in almost *all* cases).
- Reviewing the standards for "securing" PHI and implementing as appropriate. Alternatively, establishing procedures to identify breaches and provide the required notifications. *Remember, many breaches of PHI must now be communicated to the affected participants, the government and, in some cases, prominent local media outlets. Also, the penalties related to the breach have increased dramatically. To the extent possible, it now makes even more sense for Health Plan Sponsors to take steps in advance to prevent such breaches from occurring.*
- Reviewing existing administrative, technical and physical safeguards and implementing additional safeguards as necessary. *These safeguards continue to be required by the HIPAA privacy and security rules and the higher penalties can be applied to violations of these safeguards.*
- Reviewing the plan's minimum necessary standards and revising to accommodate the limited data set requirement, as appropriate.
- Reviewing and updating the plan's administrative practices and all privacy and security policies and procedures to address the expanded rules, especially the breach notification requirements and the prohibition on the use of genetic information for underwriting purposes.
- Updating the plan's privacy notice to incorporate GINA's restrictions and appropriate HITECH changes.
- Training the plan's workforce members. *Note: Training is not only a good business practice, it is specifically required by the law. For example, training must include information on the policies and procedures that implement the breach notification rules. It makes sense to remind the employees who do work for the health plan about the old HIPAA privacy and security rules, as well as explain the changes to HIPAA and the steps the Health Plan Sponsor is taking to further protect PHI to avoid violations and their consequences. Individuals should be informed about the significantly higher civil penalties. Health Plan Sponsors and business associates must: (1) impose sanctions for any failure to comply with these policies and procedures; (2) permit individuals to file complaints regarding these policies and procedures (or a failure to comply with them); and (3) refrain from intimidating or retaliatory acts against complainants and those exercising their HIPAA rights.*
- Monitoring future developments to be able to implement new regulatory guidance when issued.

## New HIPAA Civil Penalties

Culpability Standard	Minimum Penalty (per violation)	Maximum Penalty (per violation)	Total Aggregate Maximum Penalty
<b>No Knowledge</b> (if a person does not know, and by exercising reasonable diligence would not have known, of the violation)	\$100	\$50,000	\$1.5 million (for all violations of an identical requirement or prohibition during a calendar year)
<b>Reasonable Cause</b> (if a violation is due to reasonable cause and not willful neglect)	\$1,000	\$50,000	
<b>Willful Neglect – Corrected</b> (if a violation is due to willful neglect, but was corrected)	\$10,000	\$50,000	
<b>Willful Neglect – Not Corrected</b> (where a violation is due to willful neglect, but was not corrected)	\$50,000	None	

## HIPAA Privacy & Security Refresher

Key Terms	
Business Associate	A health plan service provider that (i) performs on behalf of the plan any of several covered functions (such as claim processing, utilization review, benefit management or repricing) or (ii) provides to the plan any of the several specified services (such as actuarial, accounting, consulting, management, administrative, or financial services). <b><i>This may include your broker, TPA, accounting firm, consulting firm and/or law firm.</i></b>
Covered Entity	One of the three types of entities (certain health care providers, health care clearinghouses and health plans) that are subject to HIPAA. <b><i>This client alert is written to apply to Health Plan Sponsors, in the role as the sponsor of a covered entity.</i></b>
Group Health Plan	Health insurers, HMOs, various governmental medical programs and <i>employer-sponsored group health benefit plans</i> (such as medical, dental, vision, prescription drug, health flexible spending account and long-term care plans and some employee assistance programs).
Protected Health Information (PHI)	Individually identifiable health information that is transmitted or maintained in any form or medium and that relates to the past, present or future physical or mental health or condition of a participant, the provision of health care to a participant, or the past, present, or future payment for the provision of medical care to a participant. Information is individually identifiable if it either actually identifies an individual or contains enough specific information to do so.

**A Word About Fully Insured Plans...** Fully insured group health plans are considered “covered entities” even though the insurer or HMO itself is also a covered entity. Compliance generally may be easier for an employer that only offers an insured health plan to its employees, but the same rules generally apply. This is because HIPAA does provide some limited exceptions for a group health plan that provides benefits *solely* through an insurance or HMO contract *if* the plan does not create or receive any PHI except “summary” information and enrollment/disenrollment information. *Note, however, that a health care flexible spending account is considered a self-funded group health plan and, therefore, most employers will find it necessary to take some minimum steps to comply with HIPAA’s requirements for this FSA benefit.*

## Employee Benefits & Executive Compensation Practice Group

If you have any questions about this client alert, please contact any member of our Employee Benefits & Executive Compensation Practice Group listed below.

**Kathleen O'Connor Adams**  
(312) 569-1306  
Kathleen.Adams@dbr.com

**Kelly S. Kuglitsch**  
(414) 221-6059  
Kelly.Kuglitsch@dbr.com

**Jean D. Renshaw**  
(610) 993-2259  
Jean.Renshaw@dbr.com

**Gary D. Ammon**  
(215) 988-2981  
Gary.Ammon@dbr.com

**David Levin**  
(202) 230-5181  
David.Levin@dbr.com

**Michael D. Rosenbaum**  
(312) 569-1308  
Michael.Rosenbaum@dbr.com

**Mark M. Brown**  
(215) 988-2768  
Mark.Brown@dbr.com

**Howard J. Levine**  
(312) 569-1304  
Howard.Levine@dbr.com

**Dawn E. Sellstrom**  
(312) 569-1324  
Dawn.Sellstrom@dbr.com

**Barbara A. Cronin**  
(312) 569-1297  
Barbara.Cronin@dbr.com

**Benjamin S. Lupin**  
(215) 988-2905  
Benjamin.Lupin@dbr.com

**Lori L. Shannon**  
(312) 569-1311  
Lori.Shannon@dbr.com

**Mona Ghude**  
(215) 988-1165  
Mona.Ghude@dbr.com

**Joyce L. Meyer**  
(312) 569-1305  
Joyce.Meyer@dbr.com

**Mark J. Simons**  
(610) 993-2247  
Mark.Simons@dbr.com

**Amy Lynn Graves**  
(312) 569-1318  
Amy.Graves@dbr.com

**Sarah Bassler Millar**  
(312) 569-1295  
Sarah.Millar@dbr.com

**Joshua J. Waldbeser**  
(312) 569-1317  
Joshua.Waldbeser@dbr.com

**Megan Glunz Horton**  
(312) 569-1322  
Megan.Horton@dbr.com

**Joan M. Neri**  
(973) 549-7393  
Joan.Neri@dbr.com

**Holly C. Kopack Willobee**  
(312) 569-1312  
Holly.Willobee@dbr.com

**Sharon L. Klingelsmith**  
(215) 988-2661  
Sharon.Klingelsmith@dbr.com

**Monica A. Novak**  
(312) 569-1298  
Monica.Novak@dbr.com

**David L. Wolfe**  
(312) 569-1313  
David.Wolfe@dbr.com

**Christine M. Kong**  
(212) 248-3152  
Christine.Kong@dbr.com

**Cristin M. Obsitnik**  
(312) 569-1303  
Cristin.Obsitnik@dbr.com

### Other Publications



[www.drinkerbiddle.com/publications](http://www.drinkerbiddle.com/publications)

### Sign Up



[www.drinkerbiddle.com/publications/signup](http://www.drinkerbiddle.com/publications/signup)

### Disclaimer Required by IRS Rules of Practice:

Any discussion of tax matters contained herein is not intended or written to be used, and cannot be used, for the purpose of avoiding any penalties that may be imposed under Federal tax laws.

# Drinker Biddle

## Employee Benefits & Executive Compensation Practice Group

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY  
NEW YORK | PENNSYLVANIA | WASHINGTON DC | WISCONSIN

© 2009 Drinker Biddle & Reath LLP.  
All rights reserved.  
A Delaware limited liability partnership  
Jonathan I. Epstein and Edward A. Gramigna, Jr.,  
Partners in Charge of the Princeton and Florham Park,  
N.J., offices, respectively.

This Drinker Biddle & Reath LLP communication is intended to inform our clients and friends of developments in the law and to provide information of general interest. It is not intended to constitute advice regarding any client's legal problems and should not be relied upon as such.