



Bricker & Eckler Bulletin



Keeping clients and friends informed of breaking legal developments

March 2009

Bricker & Eckler LLP

100 South Third Street
Columbus, Ohio 43215-4291

Phone 614 . 227 . 2300
Fax 614 . 227 . 2390
info@bricker.com
www.bricker.com

COLUMBUS | CLEVELAND
CINCINNATI-DAYTON

The Stimulus Bill Amends HIPAA

The American Recovery and Reinvestment Act of 2009, commonly referred to as the “Stimulus Bill,” was signed into law by President Obama on February 17, 2009. Tucked in the lengthy Stimulus Bill are major changes to the HIPAA privacy and security requirements that will have a significant effect on “covered entities” – including health plans, health insurers, and long-term care insurers – and on their business associates.

It’s important to note that in addition to health insurers, HMO’s and long term care insurers, employer sponsored health benefits plans are also “covered entities” and are subject to the new requirements. This is particularly important when an employer sponsored health benefits plan is self-insured. Employers who sponsor and self-insure a health benefits plan to provide coverage to their employees must be sure that their self-insured plan and the plan’s business associates (such as the plan’s third party administrator) are in compliance with the new requirements by the effective dates. This bulletin highlights some of the major changes to HIPAA.

New Requirements to Notify Consumers and HHS of Breaches

Since its original enactment, HIPAA has required covered entities to mitigate damages from improper disclosures of protected health information (PHI). Covered entities had no obligation to notify persons whose information was improperly disclosed. The Stimulus Bill requires every covered entity to notify a person when there has been a “breach” of that person’s PHI and to notify the Department of Health and Human Services (“HHS”) of all breaches.

“Breach” Defined. The term “breach” is new in the Stimulus Bill and is defined as: “the unauthorized acquisition, access, use, or disclosure of [PHI] which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” Excluded from this definition are:

- (1) any unintentional breach by an employee or individual acting under the authority of a covered entity or business associate if the acquisition was made in good faith and the PHI is not further used or disclosed; and
- (2) any inadvertent disclosure by a covered entity or business associate to another individual at the same entity if the PHI is not further used or disclosed.

Notice Required to Individuals. Within 60 days of discovery of a breach, a covered entity must provide notice via first class mail to the affected person’s last known address. Among other things, the notice must include:

- (1) a description of what happened and the date of the breach,
- (2) a description of the information involved in the breach,
- (3) the steps the person should take to protect himself or herself, and
- (4) a description of the covered entity’s investigation and mitigation efforts.

At Bricker & Eckler, we are focused on the industries in which our clients do business.

- Banking & Financial Services
- Construction
- Education
- Green Strategies
- Health Care
- Insurance
- Investment Banking & Structured Finance
- Manufacturing & Logistics
- Nonprofit Organizations
- Public Sector
- Real Estate
- Technology & Intellectual Property

Notice to Local Media. In any case in which 500 or more persons are affected by a breach, the covered entity must provide notice to major local media outlets.

Notice Required to HHS. Covered entities are required to disclose all breaches to HHS. Notice of breaches affecting 500 or more persons must be made to HHS immediately. Breaches affecting fewer than 500 persons may be tracked by the covered entity and reported annually to HHS.

The new law requires HHS to promulgate regulations to implement the notice of breach requirements within six months of the enactment of the Stimulus Bill. **The notice requirements will become effective for breaches discovered on or after thirty (30) days after the publication of the regulations.** Based on these requirements, the earliest that the new notification of breach provisions could take effect is September 2009.

Expansion of Security and Privacy Rules to Business Associates

The Stimulus Bill makes Business Associates (BAs) directly subject to HIPAA's security regulations. Until now, these regulations only applied to covered entities. The specific rules extended to BAs are: (1) the administrative safeguards contained in 45 C.F.R. 164.308, (2) the physical safeguards contained in 45 C.F.R. 164.310, (3) the technical safeguards contained in 45 C.F.R. 164.312, and (4) the policies, procedures and documentation requirements contained in 45 C.F.R. 164.316.

Compliance with these requirements is a substantial new burden on business associates. BAs must adopt many of the policies and procedures now in place for covered entities, and BAs must implement many of the same technical protections in the same manner as covered entities. Among other things, the new law requires BAs to:

- implement physical safeguards for all workstations that access electronic PHI, restricting access to authorized users;
- implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI;
- assign a unique name and/or number for identifying and tracking user identity;
- implement a security awareness and training program; and
- conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the business associates.

BAs whose primary business involves providing services to health plans (for example, third party administrators) may already be substantially in compliance with these new requirements, and full compliance may be manageable. But some BAs may find the requirements daunting and be unwilling or financially unable to comply with them.

Notice of Breaches by Business Associates. Business associates will be required to notify the covered entity of any breach of confidentiality of PHI acquired from that covered entity.

Business Associates Subject to Penalties for Violations. The same enhanced civil penalties that apply to covered entities that violate the security regulations now apply to BAs. (See below.) Criminal penalties also apply to BAs.

Agreements with BAs must be Amended. The privacy and security rules newly applicable to business associates must be incorporated into BA agreements. Covered entities will need to identify all existing business associate agreements and update them, and ensure that all new business associate agreements include these privacy and security rule obligations.

The provisions related to BAs become effective on February 17, 2010.

New Requirement to Comply with Requests for Restrictions on Use of PHI

Previously under the HIPAA privacy rules, a person could ask for a restriction on the uses or disclosures of PHI by a covered entity, but the covered entity did not have to agree to such request. Under the Stimulus

Bill, the covered entity is required to comply with such a request if: (1) the person requests a restriction on the disclosure to a health plan for payment or health care operations purposes and (2) the PHI pertains solely to services for which the person was self-pay. In other words, if a person pays for a health care service out-of-pocket, he or she can request that the information about that service not be disclosed to the health plan – and the covered entity must comply. **This change will become effective on February 17, 2010.**

Electronic Medical Records: New Rules on Access and Accounting

Access. The Stimulus Bill adds new access requirements for covered entities using electronic medical records. If a covered entity uses or maintains an electronic medical record, the covered entity must provide the individual with a copy of the record in an electronic format if the individual requests it in that format. The current rules regarding an individual's right to request traditional medical records and the time frame for responding to these requests apply to requests for electronic records. **This change will become effective on February 17, 2010.**

Accounting. The Stimulus Bill also imposes greater requirements on accounting for disclosures of electronic medical records than for paper records. While HIPAA establishes the right of patients to have an accounting of disclosures of their PHI, under the current regulations covered entities are not required to track and account for disclosures made for certain purposes, such as treatment, payment, and health care operations. But the Stimulus Bill states that this exception shall not apply to “disclosures through an electronic health record.” Thus, it appears that covered entities will also have to track disclosures of electronic medical records made for treatment, payment, and health care operations and provide an accounting to patients of such disclosures upon request.

The scope of this change to the accounting requirements is enormous. Disclosures made for payment purposes include, for example, disclosures made to review health care services with respect to medical necessity or coverage under a health plan, disclosures made for medical management, disclosures made to coordinate benefits, disclosures made for external review purposes, and any other disclosure related to the processing and payment of a claim. Disclosures made for health care operations purposes include, for example, disclosures made in the course of conducting quality assurance, disclosures made to auditors and actuaries, disclosures made as part of the underwriting process, disclosures made as part of fraud detection and prevention, disclosures made for subrogation and recovery purposes, disclosures made as part of due diligence related to a merger or other transaction, and any other disclosure made as part of the business operations of the health plan. If these disclosures are made from an electronic medical record, covered entities will have to track each one and itemize these when an accounting is requested. **These changes will become effective on January 1, 2014, for electronic medical records created prior to January 1, 2009. These changes will become effective on January 1, 2011, for electronic medical records created after January 1, 2009.**

Greater Enforcement

The Stimulus Bill also grants additional enforcement power related to violations of the HIPAA privacy and security rules. In addition to subjecting business associates to civil and criminal penalties for HIPAA violations, the law *requires* HHS to conduct periodic audits of covered entities and business associates to ensure compliance with HIPAA, and requires HHS to investigate complaints and impose penalties for willful neglect.

Civil penalties for violation of the privacy or security rules are increased to a range of \$100 to \$50,000 per violation, with maximum penalties for additional violations in any one year ranging from \$25,000 to \$1.5 million. Importantly, HHS is required to distribute portions of the collected civil money penalties to persons whose information was improperly disclosed or used -- creating a financial incentive for individuals to report suspected HIPAA violations.

Finally, state attorneys general are given new civil enforcement authority related to violations of HIPAA on behalf of citizens of that state. Limited federal resources, the large number of covered entities, and the wide range of potential violations made enforcement of all but the most egregious violations a daunting task for the Office of Civil Rights of HHS. The addition of 50 state attorneys general with enforcement power is

likely to result in far more thorough investigations of complaints and other enforcement activity, and a far higher risk of inconsistent application and interpretation of the requirements from state to state.

These new enforcement provisions have varying future effective dates. The increased penalty amounts and authority for enforcement by state attorneys general became effective for any violation occurring after February 17, 2009.

More HIPAA Regulations to Come

The Stimulus Bill requires HHS to promulgate new HIPAA regulations on a variety of topics, including: (1) implementing the requirements related to notification of breaches, (2) defining the meaning of “minimum necessary,” (3) describing what information shall be collected when tracking disclosures of electronic medical records for accounting purposes; (4) implementing the prohibition on the sale of information from electronic medical records, (5) implementing mandatory HHS investigations and penalties for violations due to willful neglect, and (6) establishing a methodology for distributing a percentage of collected penalties to persons harmed by violations. Covered entities will need to monitor the rule-making associated with these new HIPAA laws to ensure compliance with future regulations.

What Health Plans and Business Associates Should Do

What health plans and business associates must do to comply with some of the new requirements will not be entirely clear until HHS promulgates regulations (for example, the notification of breach requirements and the new accounting requirements). Compliance with these new requirements will be difficult, if not impossible, until the regulations are drafted. Most of the new requirements which require HHS to promulgate regulations have delayed effective dates to provide time for the promulgation of regulations. However, if the process of promulgating the initial HIPAA privacy and security regulations is an indication of how long the rule making process will take, it is unlikely the final regulations will be in place before the effective date of most of the new requirements. Health plans and business associates should closely monitor the rulemaking process in the interim.

Some of the new requirements do not require the promulgation of regulations by HHS (for example, the requirement to honor a request for a restriction on use and disclosure of PHI, the requirement to provide an electronic copy of electronic records in response to a request for access, and most notably, the expansion of the security regulations to BAs). The effective date of these changes varies, but the earliest effective date is February 17, 2009. Health plans and BAs should begin thinking about what changes will be required in their policies and procedures and what BA agreements will need to be amended, and they should begin training their workforce on these new requirements now.

Bricker & Eckler LLP will be updating its HIPAA website to notify you when draft regulations are issued and of other significant developments. We will also be developing useful tools to assist covered entities and business associates in complying with the new requirements, including sample policies and procedures, BA amendments and other tools. Information about such tools will also be posted on the Bricker & Eckler HIPAA website as they become available. The website is located at www.bricker.com/hipaa.

For more information, please contact Elisabeth A. Squeglia, esqueglia@bricker.com, or Faith M. Williams, fwilliams@bricker.com.

Insurance and Employee Benefits Law Group

Insurance

Faith M. Williams
614 . 227 . 2374
fwilliams@bricker.com

Elisabeth A. Squeglia
614 . 227 . 2396
esqueglia@bricker.com

Robert H. Katz
614 . 227 . 2397
rkatz@bricker.com

Miranda C. Motter
614 . 227 . 4810
mmotter@bricker.com

Employee Benefits

Christine M. Poth
614 . 227 . 2395
cpoth@bricker.com

Peggy Bomberger
614 . 227 . 4858
pbomberger@bricker.com

This document has been prepared as a general reference document for informational purposes. The information contained herein is not intended to be and should not be construed as legal advice. Each circumstance should be considered and evaluated separately, and possibly with involvement of legal counsel.

Please contact Bricker & Eckler for permission to reprint this bulletin in part, or in its entirety.