



Health Care Client Bulletin



Health Care Bulletin No. 09-03

February 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 Quality Management
Consulting Group, Ltd.

*Our affiliated health care
consulting group*

www.qmcg.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.

What is in the Stimulus Bill for Hospitals? Major HIPAA Changes

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 HIPAA that will have a significant effect on hospitals.

New Requirements to Notify Patients and HHS of Breaches

HIPAA has required covered entities to mitigate damages from improper disclosures which, depending on the facts and circumstances might include, but did not necessarily require, notice to the persons whose information was improperly disclosed. The new law will require every covered entity to notify a person when there is a “breach” of that person’s protected health information (“PHI”) and to notify the Department of Health and Human Services (“HHS”) of all breaches.

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.” However, a “breach” does not include:

- any unintentional breach by an employee or individual acting under the authority of a covered entity or business associate if -- (1) the acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual; and (2) the PHI is not further acquired, accessed, used, or disclosed by any person; or
- any inadvertent disclosure from an individual who is otherwise authorized to access PHI

at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility and the PHI received as a result of such disclosure is not further acquired, accessed, used, or disclosed by any person without authorization.

When there is a breach, the covered entity will be required to provide notice within 60 days of discovery of the breach by letter sent via first class mail to the affected person’s last known address. This notice must include: (1) a brief 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, (4) a description of what the covered entity is doing to investigate, mitigate and prevent other breaches, and (5) contact information for the person to use to gain more information. If there is insufficient or out-of-date information that prevents notice directly by mail, the covered entity must publish notice of the breach on its website or in major local media outlets and must include a toll-free telephone number to call for information about the breach. Additionally, 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.

Further, covered entities will be required to disclose all breaches to HHS. Breaches affecting 500 or more patients must be made to HHS immediately. Breaches affecting fewer than 500 people 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 enact-

ment of the Stimulus Bill. The notice of breach in the Stimulus Bill will become effective for breaches discovered on or after thirty (30) days after the publication of the regulations.

Expansion of Security and Privacy Rules to Business Associates

The new law makes the following HIPAA security regulations applicable to business associates of covered entities: (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. Previously, these regulations only applied to covered entities. Application of these requirements to business associates will impose vast and substantial burdens on business associates, which will now need to have many of the policies and procedures in the same manner as covered entities and to utilize many of the same technical functions in the same manner as covered entities. For example, the security rules will now require business associates to:

- 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 (per 45 C.F.R. 164.308(a)(1)(ii));
- implement a security awareness and training program (per 45 C.F.R. 164.308(a)(5));
- implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users (per 45 C.F.R. 164.310(c));
- assign a unique name and/or number for identifying and tracking user identity (per 45 C.F.R. 164.312(a)(2)(i)); and
- implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI (per 45 C.F.R. 164.312(b)).

These are merely examples from the security regulations that will be applicable to business associates. The regulations contain many more requirements. Business associates may have a difficult time meeting these obligations and some business associates will likely not be willing or financially able to do so.

In addition, business associates will be required to notify the covered entity of any breach of confidentiality of PHI. Finally, all of the new privacy and security provisions enacted in the new law will be applicable to business associates.

Importantly, under the changes to HIPAA, a business associate that violates applicable security regulations will be subject to same penalties as a covered entity as provided in 42 U.S.C. 1320d-5 and 42 U.S.C. 1320d-6 (which are increased also in the Stimulus Bill as discussed below).

The new law also requires that the privacy and security rules newly applicable to business associates be incorporated into business associate agreements. Covered entities will need to identify all existing business associate agreements and update them, as well as modify the template business associate agreement or otherwise ensure all future business associate agreements include these privacy and security rule obligations.

These provisions become effective 12 months after the enactment of this law – that is on February 17, 2010.

New Requirement to Comply with Requested Restrictions

Previously under the HIPAA privacy rules, a person could ask for a restriction on the uses or disclosures by the covered entity, but the covered entity did not have to agree to such request. Under the new law, if a person requests a restriction on disclosures the covered entity will be required to comply 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. That is, if a person pays for a service out-of-pocket, he can request that the information about that service not be disclosed to his health plan – and the covered entity must comply. This change will become effective on February 17, 2010.

Electronic Medical Records: New Rules on Accounting and 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 will be required to provide the individual with a copy of such information in an electronic format under the same circumstances as the right of access in the current rules for traditional medical records (45 C.F.R. 164.524). The charge the covered entity may impose for providing such an electronic copy may not be greater than the covered entity's labor costs in responding to the request for the electronic copy. This change will become effective on February 17, 2010.

Also, the new law imposes greater requirements on accounting for disclosures of electronic medical

Health Care Law Group

Michael K. Gire, Chair
614 . 227 . 2318
mgire@bricker.com

Catherine M. Ballard
614 . 227 . 8806
cballard@bricker.com

Martha Post Baxter
614 . 227 . 2314
mbaxter@bricker.com

C. Christopher Bennington
513 . 870 . 6572
cbennington@bricker.com

John F. Birath, Jr
614 . 227 . 2325
jbirath@bricker.com

Richard H. Blake
216 . 523 . 5470
rblake@bricker.com

Mark R. Chilson
513 . 870 . 6570
mchilson@bricker.com

Shannon K. DeBra
513 . 870 . 6685
sdebra@bricker.com

James F. Flynn
614 . 227 . 8855
jflynn@bricker.com

David M. Johnston
614 . 227 . 8817
djohnston@bricker.com

Allen R. Killworth
614 . 227 . 2334
akillworth@bricker.com

Sean M. McGlone
614 . 227 . 8879
smcglone@bricker.com

Randall E. Moore
614 . 227 . 2380
rmoore@bricker.com

Jennifer M. Nelson Carney
614 . 227 . 4870
jnelsoncarney@bricker.com

Kimberly S. Parks
614 . 227 . 8801
kparks@bricker.com

Diane M. Signoracci
614 . 227 . 2333
dsignoracci@bricker.com

Karen D. Smith
614 . 227 . 2313
ksmith@bricker.com

David C. Spialter
614 . 227 . 2342
dspialter@bricker.com

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

Claire Turcotte
513 . 870 . 6573
cturcotte@bricker.com

records than for paper records. While HIPAA establishes the right of patients to have an accounting of disclosures of their PHI, there are several exceptions including disclosures to carry out treatment, payment and health care operations, which do not need to be tracked or included in the accounting. But the new law states that this exception shall not apply to “disclosures through an electronic health record.” That is, covered entities will 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 new law states that this accounting of disclosures of electronic medical records must include disclosure for the period of three years prior to the date on which the accounting is requested. The scope of this change is enormous. Disclosures made for treatment purposes include, for example, disclosures from one covered entity to another, such as a hospital to a physician’s office. Disclosures made for health care operations purposes include, for example, disclosures made in the course of conducting quality assurance. 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. If these disclosures are made from an electronic medical record, covered entities will have to track each one. These rules will become effective on January 1, 2014, for electronic medical records created prior to January 1, 2009. These rules will become effective on January 1, 2011, for electronic medical records created after January 1, 2009.

Greater Enforcement

The Stimulus Bill also provides for much greater enforcement of the HIPAA privacy and security rules. First, as noted above, business associates will be subject to civil and criminal penalties for HIPAA violations in the same manner as covered entities. Second, HHS will be required to conduct investigations of possible violations if it is indicated that the alleged violation was possibly due to willful neglect and will be required to impose civil penalties for violations due to “willful neglect.” Third, the amount of civil penalties will be increased to amounts ranging from \$100 to \$50,000 per violation with maximum penalties for additional violations in any one year ranging from \$25,000 to \$1,500,000. Fourth, the law will require HHS 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). Fifth, the new law authorizes state attorney generals to bring suit in federal district court for alleged violations of HIPAA on behalf of citizens of that state. Sixth, the law also states that HHS shall conduct periodic audits of covered entities and business associates to ensure compliance with HIPAA.

These new enforcement provisions have varying future effective dates; however, note that the increased penalty amounts and authority for state attorney general enforcement became effective for any violation after the date of enactment, February 17, 2009.

More HIPAA Regulations to Come

The Stimulus Bill requires HHS to promulgate new HIPAA regulations on a variety of topics, including rules: (1) implementing the new notification of breach requirements, (2) defining the meaning of “minimum necessary,” (3) describing what information shall be collected in regards to the accounting of disclosures of electronic medical records, (4) implementing the prohibition on the sale of information from electronic medical records and exceptions thereto, (5) implementing the 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 on-going rule-making associated with these new HIPAA laws to ensure compliance with regulations that will be coming out in the near future.

Application to Covered Entities

Note that all of the foregoing changes apply to “covered entities” and, thus, in addition to applying to hospitals, will apply to physicians and physician practices, health plans, health care facilities, and any other entity meeting the definition of covered entity.

This Health Care Client Bulletin was prepared by Allen Killworth. Please contact any member of the Bricker & Eckler LLP Health Care Department for more information. This and previous Client Bulletins may be accessed at www.bricker.com/Publications.