

FEDERAL SPENDING BILL INCLUDES MAJOR NEW HIPAA REQUIREMENTS

By: Paul E. Knag

MARCH 2009

The Health Care Department at Murtha Cullina is pleased to provide clients and friends with information about topics of interest in the health care area.

If you have questions about the issues addressed in this newsletter, or any other matters involving health care law issues, please feel free to contact the following attorneys:

Heather O. Berchem
Marcel J. Bernier
Jacqueline DeAndrus Bucar
Robert V. Giunta, Jr.
H. Kennedy Hudner
Paul E. Knag
Mark F. Korber
Kenneth L. Levine
Michael E. McDonough
Martha Everett Meng
Elizabeth Neuwirth
Stephen E. Ronai
Alfred E. Smith, Jr.
Louis B. Todisco



The \$787 billion federal spending bill which became law on February 17, officially known as the “American Recovery and Reinvestment Act of 2009,” contains major changes to HIPAA’s Privacy and Security provisions. The portion of the

Act which addresses HIPAA is known as the Health Information Technology for Economic and Clinical Health Act (HITECH).

The effect on covered entities will be substantial. All Business Associate contracts must be amended to include additional provisions. There are changes relating to minimum necessary, marketing, fundraising, restriction request and disclosure accounting rules. Moreover, there will be new rules describing desired technical safeguards, which, if not adopted, will require notifications of various types. The effect on other entities will also be substantial. Business Associates will now be directly covered by HIPAA, the definition of Business Associate is expanded, and certain other entities which are neither covered entities nor Business Associates will be covered by requirements of the new law. Moreover, penalties are being increased, and states’ attorneys general have been given a direct civil right of action under HIPAA. The era of HHS using its discretion to limit HIPAA penalties is over.

Following is a summary of each of these changes.

Effective Date. Where not otherwise provided, the provisions of HITECH are effective February 17, 2010.

Extension of Privacy and Security Provisions and Penalties to Business Associates; Requirement of Revised Business Associate Agreements. Sections 13401 and 13404 of HITECH extend to Business Associates the requirements of many of the security and privacy provisions of HIPAA. Under prior law, Business Associates were obligated to follow HIPAA provisions under the Business Associate Agreements they executed. Now administrative safeguards, security policies and documentation requirements apply directly to Business Associates. This gives HHS (and other enforcement authorities) the right to proceed directly against these entities. In addition, HITECH provides specifically that the additional requirements of this title that relate to privacy and security and that are made applicable with respect to covered entities and Business Associates “shall be incorporated into the Business Associate agreement between the Business Associate and the covered entity.”

Annual Guidance on the Most Appropriate and Effective Technical Safeguards. The HIPAA Security Rule as currently in effect is a flexible set of standards that does not mandate any specific technology. Under Section 13401(c) of HITECH, annual guidance is to be issued by HHS as to what it deems the most appropriate and effective technical safeguards.

In Boston: 617.457.4000
In Hartford: 860.240.6000
In Madison: 203.245.9991
In New Haven: 203.772.7700
In Stamford: 203.653.5400
In Woburn: 781.933.5505

www.murthalaw.com

Murtha Cullina LLP | Attorneys at Law | www.murthalaw.com

Breach Notifications to Individual, Covered Entity and HHS.

Section 13402 of HITECH contains detailed requirements of specific notifications that are to be provided to individuals where there has been a breach of their so-called “unsecured” protected health information (“PHI”). “Unsecured PHI” means PHI that is not secured using the technical safeguards set out in the annual guidance which is to be issued. If no such guidance is issued, “unsecured PHI” means PHI that is not secured by a technology standard that renders PHI unusable, unreadable or indecipherable to unauthorized individuals and is developed or endorsed by a standard developing organization that is accredited by the American National Standards Institute (see Section 13402(h)).

There are exceptions to the breach notification requirements where the access was unintentional and in good faith by an employee of the covered entity or to another individual authorized to access PHI at the facility. Notification must be in writing, and sent as soon as possible, but within 60 days after discovery of the breach, and sent via first class mail to the individual’s last known address, unless the individual has requested communication by electronic mail. Where current contact information is not available, then notice should be placed on the website of the covered entity (required if there are at least 10 or more individuals with non-current contact information) or notice in print or broadcast media. Such notice must include a toll free number. Notice must also be given to HHS. Such notice to HHS shall be annual, except it shall be immediate if more than 500 persons are involved in a particular breach. Otherwise, a log of violations is to be submitted annually. In the case of breach by a Business Associate, notice must also be given to the covered entity.

Under subsection j of Section 13402, interim regulations are to be published within six months of enactment and the provisions of 13402 apply to breaches discovered within 30 days thereafter. Many states, including Connecticut, already require notification to individuals when there has been unauthorized access to or acquisition of an individual’s personal information. However, Connecticut’s “Security Breach” notification law is narrower than the provisions in HITECH. The Connecticut notification requirement is triggered only when there has been unauthorized access to electronic information of an individual which includes the individual’s first name or first initial and last name in combination with one or more of the following: 1) Social Security number; 2) driver’s license number or state identification number; or 3) account number, credit or debit card number with any required security code, access code or password that would permit access to an individual’s financial account. The Connecticut law also provides for an exception to notification

when, after appropriate investigation and consultation with relevant state, federal or local law enforcement agencies, the entity determines that the breach will not likely result in harm to the individuals whose personal information has been accessed. Providers should be aware, however, that these security breach notification requirements under Connecticut law extend to the unauthorized access to any individual’s personal information, including employees.

Right to Prevent Disclosure of Out of Pocket Services to Health Plan. Section 13405(a) provides that if an individual requests that services rendered to him/her, and paid for out of pocket, not be disclosed to the individual’s health plan, that request must be honored by the covered entity.

Right to Accounting of Disclosures. This right is expanded to include accounting of disclosures for purposes of treatment, payment or operations during the previous three years if the disclosures were through an electronic medical record. Section 13405(c). However, for entities which acquired an electronic health record by January 1, 2009, this provision will be effective January 1, 2014, otherwise January 1, 2011 or the date of acquisition of the electronic health record, whichever is later. The Secretary is also permitted to extend these effective dates.

Expansion of Minimum Necessary Requirement. Under Section 13405(b), a covered entity is treated as “in compliance” with the minimum necessary standard only if the covered entity limits PHI disclosure, to the extent practicable, to the “limited data set,” as currently defined (i.e., no name, postal address other than city, state and zip code, telephone or fax number, e-mail address, social security number, medical record number and certain other identifiers). This requirement sunsets when new guidance on “minimum necessary” is issued by the Secretary within eighteen months.

Sale of Records. HITECH prohibits sale of PHI without patient consent. This does not prevent payment where the sale is for public health purposes, for treatment purposes, in connection with a sale, transfer, merger, or consolidation of covered entities, and for research purposes (so long as the price reflects only the costs of preparation and transmittal of the data). Regulations are to be promulgated within 18 months of enactment, and the requirements become effective 6 months thereafter (see Section 13405 (d)).

Patient Access to Electronic Format. If a covered entity uses or maintains an electronic health record, then the individual has the right to an electronic copy, with fees not to exceed the labor costs of responding (see Section 13405 (d)).

Marketing Communications Restricted. Under Section 13406(a), communications which are deemed part of health care operations and excluded from the definition of marketing as contained in 164.501(1)(i), (ii) or (iii) are now limited to those communications for which the covered entity has not been paid directly or indirectly, unless the communication involves a drug or biologic currently being prescribed. Otherwise, an authorization from the individual is needed.

Fund-raising. All fund-raising communications must provide for the opportunity to opt out of receiving further communications (see Section 13406(b)). This is consistent with current law.

Requirements for Vendors of Personal Health Records and Other Non-HIPAA Entities. Section 13407 provides that following any breach of security of unsecured personal health records, a vendor of such records must report same to any US citizen or resident whose records have been breached, and also report same to the Federal Trade Commission (“FTC”). This requirement also applies to entities that offer products or services through the website of a vendor of personal health records. It also applies to certain entities that are not covered entities that access information in a personal health record. Any service provider to such vendor must notify the vendor. The FTC must promulgate interim final regulations within 180 days of the enactment date, and the regulations apply to breaches discovered on or after 30 days after promulgation of such regulations.

Violations of the notification requirements are treated as unfair and deceptive acts or practices in violation of the Federal Trade Commission Act. This would apparently mean that a private right of action would exist in Connecticut under the Connecticut Unfair Trade Practices Act.

Expanded Definition of Business Associate. Section 13408 expands the definition of Business Associate to include those who provide PHI as a data transmission service. This would include a Health Information Exchange Organization, a Regional Health Information Organization, an Ehealth prescribing gateway or vendor providing such services.

Higher Civil Monetary Penalties. If a violator did not know, and by exercising reasonable diligence would not have known, of the violation, there is a minimum penalty of \$100 per violation but not more than \$25,000 per year for violation of the same requirement. Violations due to reasonable cause, and not willful neglect, have a minimum CMP of \$1000 per violation but not more than \$50,000 per year for violation of the same requirement. If there is willful neglect, but the

violation is corrected within 30 days after the violator knew or should have known of the violation, the CMP is a minimum of \$10,000, but not more than \$250,000 per year for violation of the same requirement, and a maximum of \$50,000 per violation and \$1,500,000 for violations of the same requirement in a calendar year. If the willful neglect violation is not corrected within 30 days, the minimum penalty is \$50,000 per violation with no maximum. HHS is to consider the nature and extent of the violation and the harm caused in assessing penalties. Within 3 years, HHS must promulgate a regulation to provide part of the CMP money to harmed individuals. In addition, if HHS determines that a violation is due to willful neglect, a penalty must be imposed (see Section 13410). These provisions are effective immediately to violations occurring after the effective date, except that provisions relating to willful neglect are effective February 17, 2011, with regulations to be published not later than 18 months after the date of enactment, February 17, 2009.

State Attorney General Actions. A new civil action right is created for the benefit of state attorneys general. State attorneys general will be allowed to sue to enforce violations of HIPAA privacy and security rules if the violations have not been corrected in 30 days and affect that state’s residents. Damages of \$100 per violation but not more than \$25,000 for violations of the same requirement, plus attorneys’ fees and costs, may be obtained.

Connecticut Member, Lex Mundi A Global Association of Independent Law Firms

MURTHA
CULLINA

This newsletter is one of a series of publications by Murtha Cullina LLP and should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult your own lawyer concerning your own situation and any specific legal questions you may have.

BOSTON

99 High Street
Boston, MA 02110
Tel: 617.457.4000
Fax: 617.482.3868

STAMFORD

177 Broad Street
Stamford, CT 06901
Tel: 203.653.5400
Fax: 203.653.5444

HARTFORD

CityPlace I
185 Asylum Street
Hartford, CT 06103
Tel: 860.240.6000
Fax: 860.240.6150

WOBURN

600 Unicorn Park Drive
Woburn, MA 01801
Tel: 781.933.5505
Fax: 781.933.1530

MADISON

71 Wall Street
Madison, CT 06443
Tel: 203.245.9991
Fax: 203.245.9997

NEW HAVEN

Whitney Grove Square
Two Whitney Avenue
New Haven, CT 06510
Tel: 203.772.7700
Fax: 203.772.7723