



HEFFERNAN INSURANCE BROKERS

A Member of the Heffernan Group

DATE: April 30, 2009
TO: Our Valued Client Partners & Friends
FROM: HIB Account Team
RE: LEGISLATIVE UPDATE 2009-10
ARRA's HIPAA Amendments Strengthen and Expand HIPAA's Reach

We are pleased to bring you our **Legislative Update 2009-10: ARRA's HIPAA Amendments Strengthen and Expand HIPAA's Reach**. This update addresses additional changes and updates implemented by the passage of the Americans Recovery and Reinvestment Act of 2009 (ARRA). In particular compliance to the Health Insurance Portability and Accountability Act of 1996 referred to as HIPAA.

We will continue to keep you informed of changes and or clarifications based on the implementation of ARRA, but in the meantime, we hope you find this informative, and please, if you have any questions, contact your HIB Account Team for assistance.

ARRA's HIPAA Amendments Strengthen and Expand HIPAA's Reach

The **American Recovery and Reinvestment Act of 2009** (ARRA) (<http://fdsys.gpo.gov/fdsys/pkg/BILLS-111hr1ENR/pdf/BILLS-111hr1ENR.pdf>) contains yet another major new set of rules: **The Health Information Technology for Economic and Clinical Health Act (HITECH)**. This new law drastically tightens compliance parameters under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), while expanding its reach to entities not previously covered by the original HIPAA Rules. The purpose of this Memorandum is to provide the framework of the legislation. As with HIPAA historically, the substance of the law will appear in new regulations.

PROPOSED REGULATIONS

On April 17, 2009, Health and Human Services (HHS) released **Guidance** (<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>) proposing technologies and methodologies for converting Protected Health Information (PHI) into a format that will protect its use by unauthorized individuals. In other words, HHS is proposing tools for protecting health information and seeking comments from stakeholders regarding the proposed tools. The comment period closes May 21, 2009. On the same date, the Federal Trade Commission issued similar guidance applicable to vendors of personal health records.

DISCUSSION

1. **Effective Dates.** Although the law is generally effective on February 17, 2010, the legislation contains numerous specific effective dates between now and 2014!

LEGISLATIVE UPDATE 2009-10

ARRA's HIPAA Amendments Strengthen and Expand HIPAA's Reach

April 30, 2009

Page 2

2. Breaches Involving Unsecured Protected Health Information:

- a. **Definition of a Breach.** Breach has been defined as: The unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information. It excludes certain inadvertent or unintentional disclosures among authorized (in-house) users.
- b. **In the Event of a Breach.** Other than inadvertent in-house disclosures, the Covered Entity must notify effected individuals within 60 days after the discovery of the breach (unless it would impede a criminal investigation). The Covered Entity must notify HHS and prominent local media if the breach involves more than 500 individuals and must do so immediately. Where 500 or more individuals are involved, the Secretary is also required to post on the **HHS web site** (<http://www.hhs.gov/ocr/privacy/index.html>) the list of Covered Entities involved in the breach. In the case of breaches involving fewer than 500 individuals, the Covered Entity may maintain a log and notify the Secretary of its breaches on an annual basis. This duty to disclose takes effect 30 days after HHS publishes regulations which are due within six months of the law's enactment.
- c. **Applicability.** These new rules apply to Covered Entities as well as Business Associates, as defined by HIPAA Regulations. Also, these rules will now apply to vendors of Personal Health Records (PHRs), as well as other entities to be identified by regulations (most likely advertisers on the PHR website). PHR vendors must notify the Federal Trade Commission (FTC) as well as individuals whose data has been breached. The FTC, in turn, must notify the Secretary of HHS but will retain its own enforcement authority. The FTC issued preliminary guidance on April 17, 2009 and has until August 18, 2009 to issue formal guidance.

3. Enhanced Rules Applicable to Business Associates:

- a. **Security Standards.** Business Associates must establish administrative and physical safeguards that meet the HIPAA Security Rules in effect since 2005. This includes conducting a needs assessment and implementing safeguards to respond to those needs. They must appoint a Security Officer, develop written security policies and procedures and train staff on HIPAA privacy and related rules. Business Associates must also implement technologies that protect Electronic Protected Health Information (e-PHI).
- b. **Breaches.** If a breach occurs and it involves a Business Associate, the Business Associate must notify the Covered entity, as required by the original HIPAA Privacy Regulations. The duty to notify the individuals involved remains with the Covered Entity.
- c. **Jurisdiction, Civil, and Criminal Penalties.** Business Associates will now be under the jurisdiction of HHS. They will be subject to the same civil and criminal penalties as apply to Covered Entities.
- d. **Patient's Rights.** HITECH grants additional rights and protections to covered individuals. Business Associates must comply in the same manner as if they were Covered Entities.
- e. **Applicability of Technologies Guidance.** The law does not require Business Associates to comply with technologies guidance at this time. Business Associates, who do comply, may rely on them as a safe harbor.
- f. **Effective Date.** The expanded rules will apply to Business Associates as of February 17, 2010.
- g. **Business Associate Agreements.** We expect regulations, once published, to assist in modifying Business Associate Agreements.

LEGISLATIVE UPDATE 2009-10

ARRA's HIPAA Amendments Strengthen and Expand HIPAA's Reach

April 30, 2009

Page 3

4. **Patients' Rights.** HITECH brings with it an additional set of patients' rights:
- a. The right to request and receive at a reasonable cost their health information in electronic format if the information is maintained as an Electronic Health Record (EHR).
 - b. The right to apply restrictions on disclosures made to Covered Entities for any item or service, for which the patient has paid the full cost out of pocket.
 - c. The right to receive a full accounting of disclosures made by the Covered Entity or Business Associate involving treatment, payment, or health care operations during the previous three years. Previously, disclosures made for purposes of treatment, payment, or health care operations were excepted from the accounting requirement.
 - d. **Minimum Necessary.** HITECH also requires HHS to issue guidance by August 17, 2011 on the meaning of the term "minimum necessary" expanded to include information to improve patient outcomes and to detect, prevent, and manage chronic diseases.
 - e. **Effective Dates.** If the electronic record constitutes an EHR, the disclosure requirement will apply to all disclosures made on or after January 1, 2014. If a Covered Entity does not currently maintain EHRs, this disclosure requirement will apply the alter of January 2011 or when the Covered Entity acquires EHRs. Patient rights not involving EHRs, we believe, will become effective February 17, 2010.
5. **HIPAA Enforcement.** The following chart demonstrates the significant increase in penalties as well as the ability for state attorneys general to bring actions in federal court for HIPAA violations. The effective date of these penalties vary.

	Current	ARRA
Violations	\$100 per violation to \$25,000 maximum per calendar year	\$100 per violation to \$50,000 maximum per violation
Willful Neglect	N/A	\$25,000 to \$1.5 million per calendar year
Crimes	No monetary penalties	Monetary penalties allowed
Enforcement	HHS (OCR)	HHS (OCR) and states attorneys general in federal court
Recompense to Victims	None	Government Accountability Office to devise a methodology to share monetary penalties with victims

6. **Technologies Guidance.** The Guidance issued on April 17, 2009 defines "unsecured protected health information" to mean PHI that is not secured through the use of technology or methodology described in the Guidance. If PHI is protected by one or more of the methodologies in the Guidance, then it will be treated as "rendered unusable, unreadable, or indecipherable." If it is treated as such, then the breach notification rules in the ARRA legislation will not apply. The Guidance also contains details regarding the written notice:
- a. To be made to the individual or the next of kin (if the individual is deceased);

LEGISLATIVE UPDATE 2009-10

ARRA's HIPAA Amendments Strengthen and Expand HIPAA's Reach

April 30, 2009

Page 4

- b. In the event address information is obsolete on 10 or more individuals, the Covered Entity or Business Associate must make a conspicuous posting on the home page of the Covered Entity's web page or a notice in major print and broadcast media;
- c. If there is imminent potential for misuse of the unsecured PHI, then the Covered Entity or Business Associate is advised to provide notice by telephone

The Guidance characterizes PHI based on its status: PHI at rest (resident in a database); data in motion (data moving through a network); data in use (data that is in the process of being created, retrieved, updated or deleted); and, data disposed (discarded paper records or recycled electronic media). HHS has identified two methodologies for rendering data unusable, unreadable, or indecipherable. These two are: encryption and destruction. Please refer to the **HHS website** (<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>) to view the Guidance in detail.

- 7. **State Laws.** It is clear that the emergence of internet storage of health records creates significant risks of breach of the HIPAA Privacy and Security laws and regulations. Although this is the first federal response to the issue, many states have either addressed or are in the process of addressing the same issues. In the event state laws are more stringent, state law will apply.

To view the ARRA HIPAA amendments (HITECH), go to Page 112 of the **American Recovery and Reinvestment Act of 2009** (<http://fdsys.gpo.gov/fdsys/pkg/BILLS-111hr1ENR/pdf/BILLS-111hr1ENR.pdf>).

To access archived Legislative Updates please log into www.heffgroup.com and clicking on the link for HIB Client Community. If you need information on your Username and Password please contact your HIB Account Team.

Copyright © 2009 Alfred B. Fowler, Attorney at Law.

All Rights Reserved. Reprint with permission only.

This legislative update is published as an information source for our clients and colleagues. It is general in its nature and is no substitute for legal advice or opinion in any particular case.

mike@abferisa.com

IRS Circular 230 disclosure: To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication, unless expressly stated otherwise, was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding tax-related penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any tax-related matter(s) addressed herein.