



HEFFERNAN INSURANCE BROKERS

A Member of the Heffernan Group

**DATE:** September 22, 2009  
**TO:** Our Valued Client Partners & Friends  
**FROM:** HIB Account Team  
**RE:** **LEGISLATIVE UPDATE 2009-14**  
**HITECH Proposed Interim Final Rule Breach Notification**

---

We are pleased to bring you our **Legislative Update 2009-14: HITECH Proposed Interim Final Rule Breach Notification**. This Legislative Update is a follow up from our earlier Legislative Update 2009-10 **ARRA's HIPAA Amendments Strengthen and Expand HIPAA's Reach**. Please note, the interim final rules do take effect September 23, 2009, but the Department of Health and Human Services as already advised that they will not impose sanctions for failure to comply with these required notifications (see the below). However it is important to review and ensure that you take the necessary actions to comply. In addition, some providers are reviewing and possibly revising their Business Associate agreements in direct response to the Interim Final Rule.

We hope you find this informative, and please, if you have any questions, contact your HIB Account Team for assistance.

### **HITECH Proposed Interim Final Rule Breach Notifications**

The Department of Health and Human Services (HHS) has released its proposed Interim Final Rule requiring Covered Entities and their Business Associates to provide notices of breaches of unsecured protected health information. Although this interim final rule takes effect on September 23, 2009, HHS states that it will not impose sanctions for failure to comply with the required notifications for breaches discovered over the next six months, to allow Covered Entities and their Business Associates time to implement the procedures necessary to achieve compliance with the Interim Rule. Additionally, HHS has established a comment period on the proposed rule through October 23, 2009.

#### **BACKGROUND**

On April 30, 2009 we published a discussion of the Health Information Technology for Economic and Clinical Health Act (HITECH) and its proposed regulations for breaches involving unsecured Protected Health Information (Legislative Update 2009-10). HHS issued the 30 page release augmenting its initial proposed regulations on August 24, 2009.

#### **DISCUSSION**

1. **Who is Subject to the Rules.** Covered Entities (health plans, health care clearing houses, and health care providers) who transmit any health information electronically in connection with a covered transaction and Business Associates who perform functions and activities on behalf of, or certain

**LEGISLATIVE UPDATE 2009-14**  
**HITECH Proposed Interim Final Rule Breach Notifications**

September 22, 2009

Page 2

services for, a Covered Entity that involves the use or disclosure of individually identifiable health information (e.g. third party administrators, pharmacy benefit managers, claim billing companies, actuaries, etc. whose duties require access to protected health information).

2. **Who is Not Subject to the Rules.** Employers / Plan Sponsors who do not receive group health plan protected health information (PHI) electronically, by paper, or orally.
3. **What is “Unsecured Protected Health Information”?** Generally speaking it is PHI that is not secured. According to the new guidance, to be secured HHS requires the information to be unusable, unreadable, or indecipherable such as by encryption under specific standards adopted by the National Institutes of Standards and Technology (NIST), or be completely destroyed to be considered “secure”.

Information, by definition in the new guidance, includes: paper, information in use, information transferred internally, or information that has been redacted or aggregated but not fully de-identified.

4. **What Constitutes a “Breach”.** HHS rules state that a breach will occur if all four of the following requirements are met:
  - a. **Unsecured.** The information involved is not encrypted or fully destroyed;
  - b. **Unauthorized.** Information was used or disclosed in an unauthorized manner in violation of the HIPAA Privacy Rules. You may recall that HIPAA’s Privacy Rules permit Covered Entities and Business Associates to use PHI for purposes of treatment, payment, or health care operations. In other words, if the information is being used for any other purpose, it is “unauthorized”. Additionally, the HIPAA Privacy Rules require that only the minimum necessary information be used.
  - c. **Risk of Harm.** The use or disclosure poses a significant risk of financial, reputational, or other harm to the individual. Covered Entities and Business Associates must determine if there is serious risk here. Not all breaches pose a serious risk.
  - d. **Exceptions.** The HITECH statute provides three exceptions:
    - Unintentional access by a Covered Entity or Business Associate in good faith and within the employee’s course and scope of employment.
    - Inadvertent one time disclosure between Covered Entity or Business Associate workforce members (workforce member means employee, volunteer, trainees, etc. whether paid or unpaid).
    - The recipient wouldn’t reasonably have been able to retain the information.

5. **What are the New Breach Notification Rules:**

- a. **Timelines.** The Covered Entity must provide written notice to all affected individuals no later than 60 days from the date of discovery. The rules define “discovery” as the first day the breach is known by a member of the workforce or should have been known by reasonable diligence. Business Associates must notify the Covered Entity, who then must provide the actual notice.
- b. **Method of Delivery.** The guidance requires written notice by first class mail to the last known address; or, if the individual has agreed to an electronic notice and not revoked such an agreement, the Covered Entity may send it electronically.
- c. **Next of Kin.** We stated in our earlier update (Legislative Update 2009-10) the Covered Entity must send the notice to next of kin or personal representative if the Entity has the address on file.

## LEGISLATIVE UPDATE 2009-14

### HITECH Proposed Interim Final Rule Breach Notifications

September 22, 2009

Page 3

- d. **Obsolete Address Information.** In the event the address information is obsolete on less than 10 individuals, then the Entity may use an alternate method of notice or even provide notice by telephone. If the information is obsolete on more than 10 individuals, then the Entity may put a conspicuous posting on the company website for a period of 90 days or place a conspicuous notice including a toll free contact number in major print or broadcast media in the geographic area the individual most likely resides.
  - e. **Urgent Situations.** In urgent (risk of misuse) situations, the Interim Final Rule states the Entity may provide notice by telephone.
  - f. **500 or More Affected Individuals.** For a breach involving 500 or more individuals in a state, the Entity must notify prominent media without unreasonable delay and within 60 calendar days.
  - g. **Notification of the Secretary of HHS.** For breaches involving 500 or more individuals, the notice to the Secretary must be simultaneous with the notice to individuals. For breaches involving less than 500 individuals, the Entity must maintain a log or other documentation and notify the Secretary no later than 60 days following the calendar year for breaches occurring in the preceding calendar year.
6. **Notice Contents.** The Interim Final Rule requires notices to contain the following elements:
- a. A brief description of the breach including the date of breach and the date of its discovery;
  - b. A description of the types of PHI involved (e.g. name, SSNs, dates of birth, etc.);
  - c. Any steps the individual can take to protect him/herself from potential harm;
  - d. A brief description of what the Entity is doing to investigate, mitigate the harm and protect against further breaches;
  - e. A contact number, email address, website, or postal address for questions or requests for additional information; and,
  - f. Written in plain language.
7. **Business Associate Obligations.** If a Business Associate discovers a breach, the Associate's first obligation is to notify the Covered Entity. The Associate must do so within 60 days of discovery and without unreasonable delay. The notice to the Covered Entity shall include as best as possible the identification of all affected individuals and any other available information that the Covered entity needs to include in its notice to individuals.
8. **Law Enforcement Delay.** If publication of the notice of breach will impede a criminal investigation or cause damage to national security, the Covered Entity may delay notice based on the written or oral statement of a law enforcement official. If it is written, then the delay is as specified in the statement. If it is oral, the delay can be up to 30 days from the date of the oral statement.

### ACTION PLAN

Employers / Plan Sponsors as well as their Business Associates should perform a risk assessment involving all unsecured personal identifiable health information emanating from or produced by the underlying health plan or from other health plan related sources, if any. In the event that you are subject to the Privacy Rules (e.g. Privacy Officers, etc.), we recommend that you complete the following over the next six months:

1. Securitization any unsecured PHI using the NIST rules or similar process;
2. Update your written HIPAA policies and procedures to meet the new HITECH standards;
3. Establish and maintain a breach log;
4. Revise HIPAA training materials; and,
5. Revise Business Associate Agreements to reflect the Interim Final Rule including the procedure to follow in the event of a breach discovered by the Business Associate.

### **STATE LAWS**

California has its own HIPAA privacy laws including the recently enacted (SB 541 and AB 211) which apply mostly to providers and clinical settings). It also has a website at <http://www.ohi.ca.gov/calohi/Default.aspx> (Office of Health Information Integrity (CalOHII)) for the support of HHS's health information exchange initiatives. Federal law will not pre-empt state law unless and to the extent they are contrary to the HIPAA requirements.

Finally, HITECH contains enhanced penalties and provides for states' jurisdiction. Please refer to our Update 2009-10 for details. Once enforcement states, the stakes for failures will be quite high.

**To access archived Legislative Updates please log into [www.heffgroup.com](http://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](mailto: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.*