



September 2009

## LEGISLATIVE UPDATE

*By Jennifer Lunski, Esq.*

### NEW HIPAA SECURITY BREACH NOTIFICATION RULES

In our [June 2009 Legislative Update](#), we discussed the Department of Health and Human Services (HHS) guidance on how covered entities (such as group health plans) and business associates should secure individuals' protected health information as required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HHS issued this guidance due to the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) provisions of the American Recovery and Reinvestment Act (ARRA), which made an important expansion to HIPAA.

Since that time, HHS has published the interim final regulations ("Regulations"), which require notification of breaches of unsecured protected health information ("PHI") by covered entities and their business associates under HIPAA. These new requirements apply to breaches occurring on or after September 23, 2009. However, the preamble to the regulations state that the notification requirements will not be enforced for breaches occurring before February 22, 2010.

The following is an overview of the new Regulations and the action items employers will need to complete in order to be in compliance by the February 22nd deadline. Please contact your Woodruff-Sawyer Benefits representative if you would like assistance in complying with the Regulations.

### OVERVIEW OF REGULATIONS

Covered entities (which include health plans, health care clearinghouses, and health care providers) must notify affected individuals whose PHI has been breached. A breach is defined as the unauthorized access, use, or disclosure of protected health information which results in a significant risk of financial, reputational, or other harm to the individual. A notice is only required for unsecured information.

Information is considered to be secure if the PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals by use of encryption or destruction. If encryption is used, the encryption keys must be kept on a separate device than the encrypted data.

If a breach has occurred, the covered entity must notify affected individuals without unreasonable delay and no later than 60 days after the breach is discovered. The breach is considered discovered on the first day on which the breach is known, or should have been known by exercising reasonable diligence, to any workforce or agent of the covered entity (other than the person committing the breach). The notification shall be in writing and sent by first class mail or electronically if the individuals have agreed to electronic notification. There are special instructions for circumstances in which the entity does not have sufficient contact information or the notification is returned.

The notice to the affected individuals must include:

- A brief description of what happened including the date of the breach and the date of the discovery.
- The type of information that was breached such as social security number or diagnosis.
- Any steps the individuals should take to protect themselves.
- A brief description of what the covered entity is doing to investigate the breach, mitigate harm to the individuals, and protect against future breaches.
- Contact information the affected individuals can use to obtain additional information and have questions answered. Contact options shall include a toll free telephone number, an e-mail address, website address or postal address.



If the breach affects 500 or more individuals, the covered entity must notify HHS without unreasonable delay, but no later than 60 days after the breach is discovered. If the breach affects 500 or more individuals within the same state, the covered entity must also notify prominent media outlets within the state. The same timeframe would apply to the media notification. Instructions for the notification will be posted to the HHS website at a later date. The covered entity must keep a log of all breaches affecting less than 500 individuals and notify HHS on an annual basis within 60 days following the end of the calendar year.

Business associates should also notify covered entities of any breaches that occur within their operations. The same notification timeframe would apply (“without unreasonable delay” but no later than 60 days). The notice must identify each individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, used, or disclosed during the breach.

Please note: Several states have enacted laws regarding notifications following a breach of personal information. The new Regulations indicate that the state law would only be preempted if it conflicts with the federal law. A state law requiring a shorter time period for notifications would not be in conflict.

## ACTION ITEMS

The following steps will need to be taken in order to meet compliance requirements for the new Regulations.

1. **Create Breach Identification Procedures.** Covered entities and business associates need to create HIPAA policies and procedures that identify when a breach has occurred. Breach identification procedures should include the following steps:
  - Review past practices and identify if there has been an impermissible use or disclosure of PHI under the HIPAA Privacy Rule.
  - Determine and record whether the impermissible use or disclosure of PHI compromises the security or privacy of the PHI in a manner that poses a significant risk of reputational, financial or other harm to the individual.

- Determine whether the incident falls under one of the three following statutory exceptions to the breach definition.
    - An unintentional use of PHI by a workforce member acting in good faith and within the scope of his or her authority, and the PHI is not further used or disclosed improperly;
    - An inadvertent disclosure of PHI by an authorized person to another authorized person, and the PHI is not further used or disclosed improperly; or
    - A disclosure of PHI to an unauthorized person where there is a good faith belief that the unauthorized person would not reasonably have been able to retain such information.
2. **Create Breach Notification Procedures.** Covered entities and business associates should determine which breach notification must be sent and who within their organization will be responsible for gathering the necessary information for preparing and sending the notices. The breach notification procedures should be incorporated into HIPAA policies and procedures.
  3. **Maintain Breach Log for HHS Reporting.** Create methods to maintain a log or other documentation of breaches of unsecured PHI under the privacy rule. A designated official should notify HHS 60 days after the end of each calendar year about breaches occurring during the preceding calendar year.
  4. **Revise Business Associate Agreements.** Covered entities and business associates should streamline breach notification efforts. If your third party administrator business associates act as an agent for you as a covered entity, require business associates to notify you of a breach discovery in advance of the 60-day deadline.
  5. **Enhance Employee Training.** Covered entities and business associates will want to provide training so that their employees understand company policies and procedures, and the consequences of failing to timely report privacy and security incidents.

Additional information is available from HHS at: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html>



A copy of the Regulations is available at:

<http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

Please note: The Federal Trade Commission (FTC) has issued similar breach notification regulations that apply to vendors that retain, accept, and process personal health information in the form of personal health records and certain others not covered by HIPAA. An example of a vendor subject to the FTC regulations would be a web-based organization that will receive, store, and maintain an individual's health information for that individual.

A copy of the FTC regulations is available at:

<http://edocket.access.gpo.gov/2009/pdf/E9-20142.pdf>

If you would like assistance in complying with these Regulations, please contact your Woodruff-Sawyer Benefits account representative.

---

*This legislative update is designed only to give general information on this topic, and is not intended to be a comprehensive summary of the subject covered or provide tax or legal advice. Please consult with a qualified tax or legal professional for your specific situation.*

---

*Woodruff-Sawyer is one of the largest independent insurance brokerage firms in the nation, and is an active partner of International Benefits Network and Assurex Global. For over 90 years, Woodruff-Sawyer has been partnering with clients to implement and manage cost-effective and innovative insurance, employee benefits and risk management solutions, both nationally and abroad. Headquartered in San Francisco, Woodruff-Sawyer has offices throughout California and in Portland, Oregon.*

*For more information, call 415.391.2141 or visit [www.wsandco.com](http://www.wsandco.com).*