

## **PHI Breach Determination and Notification Process**

*Addendum to Huron's HIPAA Compliance Program  
December 2009*

**Under recently enacted regulations related to HITECH provisions of HIPAA, organizations may be required to notify individuals, the DHHS, and in some cases, the media, if the Covered Entity or a Business Associate discovers a breach of unsecured PHI. This Addendum to Huron's HIPAA Compliance Program describes Huron's process for reviewing potential breaches of unsecured PHI, determining whether the breach is reportable, and the providing notification and reporting of the breach when appropriate.**

### **Unsecured PHI**

Notification is required if there is a breach and PHI is "unsecured." Conversely, notification is not required if there is a breach and PHI is "secured." PHI is secured if it meets the following standards:

- Electronic data at rest, which includes data that resides in databases, file systems, flash drives, memory, and any other structured storage method: Encryption consistent with National Institute of Standards and Technology ("NIST") Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
  
- Electronic data in motion, which includes, for example, data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange: Encryption in compliance, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated. In addition, encryption keys should be kept on a separate device from the data that they encrypt or decrypt.
  
- Data disposed, which includes discarded paper records or recycled electronic media: The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
  1. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
  2. Electronic media have been cleared, purged, or destroyed consistent with "NIST Special Publication 800-88, Guidelines for Media Sanitization,6" such that the PHI cannot be retrieved.

### **Huron Personnel Reporting Requirements**

Generally, a breach has occurred if PHI is accessed, used or disclosed in a way that is not allowed under the HIPAA Privacy Rules; and such access, use or disclosure compromises the security or privacy of the PHI. Huron personnel who discover, believe, or suspect that PHI has been accessed, used or disclosed in a way that violates the HIPAA Privacy Rules, should immediately report such information to the Huron HIPAA Compliance Officer or Huron Legal Department, in accordance with the Huron HIPAA Compliance Program.

Huron personnel who are determined to have failed to adhere to the policies and procedures regarding reporting of breach of unsecured PHI will be subject to the disciplinary policies of Huron.

## **Breach Determination and Notification Process Steps**

The Huron Legal Department will determine whether a breach of unsecured PHI has occurred and whether the incident falls within the reporting requirements. In summary, the process steps to make this determination involve addressing these questions:

Step 1: Has PHI been disclosed that violates HIPAA?

Step 2: If yes, does the disclosure present “significant risk of harm” to the individual(s)?

Step 3: If yes, does the disclosure fall under an exception to the reporting requirement?

Step 4: If no, Huron and/or the Covered Entity will complete the notification and reporting requirements.

### **Step 1:**

Upon receiving a report of a potential breach, the Legal Department will review the report to determine whether there has been an access, use or disclosure of PHI by Huron personnel that violates the HIPAA Privacy Rules.

### **Step 2:**

If there has been a violation, the Legal Department will then determine whether the breach poses a significant risk of harm to individual as a result of the impermissible use or disclosure of PHI.

Several factors are considered in performing this risk assessment:

- Who impermissibly used the information, or to whom was the information impermissibly disclosed?
- Did Huron take immediate steps to mitigate an impermissible use or disclosure?
- Was the impermissibly disclosed PHI returned prior to access for an improper purpose?
- What was the type and amount of PHI involved in the impermissible use or disclosure?

### **Step 3:**

If it is determined that the breach does pose a significant risk of harm to individuals, the Legal Department will consider whether there is an applicable exception to reporting, including:

- Any unintentional acquisition, access, or use of PHI by Huron personnel, if done in good faith and within the scope of authority, and which does not result in further use or disclosure in a manner not permitted under the Privacy Rule
- Any inadvertent disclosure by a person authorized to access the PHI to another person authorized to access the PHI, and the PHI is not further used or disclosed in a manner not permitted under the Privacy Rule
- Any disclosure where Huron has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

### **Step 4:**

If it is determined that: 1) a breach of unsecured PHI has occurred, 2) such breach poses a significant risk of harm to the individual as a result of the breach; and 3) no exception to the reporting requirement applies, Huron will work with the Covered Entity to notify each individual whose unsecured PHI was breached. The Covered Entity or Huron will notify individuals without unreasonable delay, and in no case later than 60 calendar days following discovery of the breach by Huron. The notice of breach to individuals will include the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI involved in the breach;
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of the actions taken to investigate the breach, mitigate harm to individuals, and protect against any further breaches; and

- Contact procedures for individuals to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, web site, or postal address.

The Covered Entity or Huron will provide the notice in written form by first-class mail to the last known address of each individual, or may provide written notice by electronic mail, if the individual agrees to receive electronic notice, and such agreement has not been withdrawn. If the affected individual is a minor or otherwise lacks legal capacity, the notification may be sent to the individual's Personal Representative. If the individual is deceased, the notice may be sent to the deceased individual's next of kin or Personal Representative if the address of the decedent's next of kin or Personal Representative is known.

If there is insufficient contact information for some or all affected individuals, individuals will be sent a substitute notice. If sufficient contact information is unavailable for fewer than ten (10) affected individuals, substitute notice may be provided through an alternative form of written notice, such as electronic mail, telephone or other means. If no current contact information is available for the individuals, notice may be posted on the website in a manner that is reasonably calculated to reach the individuals.

If there is insufficient or out of date information for ten (10) or more individuals, substitute notice will be provided through a conspicuous posting on the home page of the Covered Entity's or Huron's website or conspicuous notice in major print or broadcast media, for a period of 90 days. In addition, a toll-free phone number will be established for 90 days so individuals can obtain more information about the breach.

If it has been determined that the breach of unsecured PHI involved more than 500 residents of a particular state or jurisdiction smaller than a state, such as a county or city, the Covered Entity or Huron will notify a prominent media outlet of the breach. The Covered Entity or Huron will determine whether media notification is required and if so, will cause such notification to be made. Notification to media may be made by issuing a press release.

Huron will notify DHHS of all breaches of unsecured PHI made by Huron personnel, either on an annual basis or immediately, depending on how many individuals were affected by a breach. If a breach of unsecured PHI involved more than 500 Individuals, Huron will notify DHHS concurrently with the notification sent to an individual (without unreasonable delay but in no case later than 60 calendar days following discovery of a breach).

Under the direction of the HIPAA Compliance Officer, Huron will create and maintain a log of all breaches involving less than 500 individuals committed by Huron personnel. Within 60 days after the end of each calendar year, Huron will submit the log to DHHS. Huron will also maintain the log and all other documentation regarding breach of unsecured PHI for six years. Huron is not required to submit information to DHHS for breaches that occurred before September 23, 2009.

## GLOSSARY OF TERMS

Business Associate	A Business Associate is an entity provides services to a Covered Entity and receives or has access to PHI from the Covered Entity. To perform its functions properly, a Business Associate must receive PHI and may use or disclose PHI.
Designated Record Set	A Designated Record Set is a group of records maintained by or for the Covered Entity that <b>includes the enrollment, payment, claims, adjudication, and case or medical management record system and any other information maintained by or for the Plan that is used, in whole or in part, to make decisions about participants concerning their participation in, or benefits under, the Plan.</b>
DHHS	DHHS is the Department of Health and Human Services, which is the federal agency charged with administering HIPAA.
Health Oversight Agency	A federal or state governmental agency charged with overseeing or monitoring health or health care.
HIPAA	HIPAA is the Health Insurance Portability and Accountability Act of 1996.
HIPAA Privacy Rules	The HIPAA Privacy Rules are the HIPAA regulations issued by DHHS at 42 C.F.R. §§ 164.101 through 164.531.
Law Enforcement Official	A federal or state governmental employee authorized to enforce federal and/or state laws.
Limited Data Set	A Limited Data Set is a set of PHI that excludes direct identifiers or the individuals to whom the PHI relates. Direct identifiers include the individual's name, street address, telephone and facsimile numbers, email addresses, social security numbers, medical records numbers, health plan beneficiary numbers, any account numbers, certificate or license numbers, vehicle identifiers (including license plate numbers), and internal protocol numbers.
Protected Health Information or PHI	Protected Health Information or PHI is health information, including demographic information collected from an individual that: 1) is created or received by Huron; 2) relates to the past, present or future physical or mental health or condition of the individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; 3) identifies the individual (or reasonably could be used to identify the individual); and 4) is protected under the HIPAA Privacy Rules.