United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Conducting HIPAA Investigations:

Breach Notification

IHS Annual Conference
March 24-25, 2010

Velveta Golightly-Howell, Regional Manager, OCR Region VIII
Roosevelt Freeman, Regional Manager, OCR Region IV

United States Department of Health & Human Services

Office of the Secretary

Office for Civil Rights (OCR)

Breach Notification

Subpart D – Notification in Case of Breach of Unsecured PHI

45 C.F.R. §§ 164.400-164.414

New Subpart D

- 164.400 – applicability
- 164.402 – definitions
- 164.404 – notification to individuals
- 164.406 – notification to media
- 164.408 – notification to Secretary/OCR
- 164.410 – notification by business associates
- 164.412 – law enforcement delay
- 164.414 – administrative requirements and burden of proof

Brief Summary

- Covered entities must:
  - Notify each affected individual of breach of “unsecured protected health information.”
  - Notice to media if more than 500 people affected.
  - Notice to Secretary of breach through OCR website.
  - Notifications to be provided without unreasonable delay (but no later than 60 days) of discovery of breach.
- Business associate must notify covered entity of breach and identify individuals affected.
- Effective date – September 23, 2009.
- No CMPs/sanctions imposed for 180 days after publication date for violations of Subpart D (March 2010).

What is a “breach”

- An impermissible acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI.
- To compromise the security or privacy means to poses a *significant risk* of financial, reputational, or other harm to the individual.
- Uses or disclosures that do not include identifiers that can be used to identify the individual are not considered to compromise the security or privacy of PHI.

What is a “significant risk” of harm

- Determined by the covered entity through a risk assessment once it learns of a possible breach.
- In determining the level of risk, the covered entity should make a fact-based evaluation of factors such as the recipient of the PHI, the nature of PHI itself, any mitigation that can be taken to lessen potential harm, and the number of identifiers contained within the PHI.

Examples of what is and what may not be "significant risk"

- Covered entity mistakenly discloses PHI to the wrong pharmacy. Since the pharmacy is also obligated to comply with the Security and Privacy Rules, there is low risk of harm to the individual.

- Covered entity loses an unencrypted laptop containing PHI. However, it is recovered the next day and a forensic analysis of the laptop reveals that the information contained has not been accessed. This breach would not pose a significant risk.

Exceptions to the definition of breach

1. Unintentional acquisition, access, or use of PHI by workforce member or person acting under the authority of a CE or BA if done in good faith and in the scope of authority and there is no further impermissible use or disclosure of the PHI.
2. Inadvertent disclosure by a person authorized to access PHI to another person authorized to access PHI at the same CE or BA or OHCA and the information received is not further impermissibly used or disclosed by the recipient.
3. CE or BA have a good faith reason to believe the unauthorized recipient could not reasonably have been able to retain the information.

1. Unintentional acquisition, access, or use - examples

- A billing employee receives and opens an e-mail about a patient that was mistakenly sent to her by a nurse at the same facility. The billing employee alerts the nurse and deletes the e-mail. This would not be considered a breach, as the acquisition of the PHI was unintentional, done in good faith and within the employee's scope of authority.
- A nurse for a covered entity who is authorized to view patient records, decides to access the records of her ex-boyfriend, who is not her patient. The nurse was not acting within her scope of authority because her ex-boyfriend was not her patient, the access was intentional and not done in good faith. The exception would not apply.

2. Good faith belief that information was not retained - examples

- A health plan sends EOBs to the wrong individuals, some of the EOBs are returned by the post office as undeliverable and have not been opened. The covered entity can assume that the PHI of the individuals contained in the unopened, returned EOBs was not breached.
- A nurse mistakenly hands the discharge papers of Patient A to Patient B. However, before Patient B has a chance to look at the papers, the nurse realizes her error and immediately retrieves the paperwork from Patient B. Here, if the nurse can conclude Patient B did not look at Patient A's information, this would not constitute a breach.

Breach Checklist for Covered Entities

1. Has there been an impermissible use or disclosure of PHI?
2. Perform risk assessment - determine and document whether the impermissible use or disclosure compromised the security or privacy of PHI and whether any financial, reputational, or other harm to the individual resulted.
3. Determine if the incident falls under any of the exceptions to the definition of breach

Notification obligation only applies to “Unsecured PHI”

- Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals.
- Acceptable methods of securing PHI are encryption and destruction.
- Loss or compromise of PHI that has been encrypted or properly destroyed does not trigger the duty to notify or report.

Notification to Individuals

- A covered entity must notify each affected individual following the discovery of a breach of unsecured PHI.
- The obligation to notify applies to those breaches that the covered entity knows about or *should have known* about if exercising reasonable diligence.

“Known or should have known” Standard

- Means that covered entities can be liable for failing to provide notice to individuals in situations where they did not know of a breach but would have known if they exercised reasonable diligence.
- Employees of a covered entity are considered agents of the organization and any knowledge an employee has will be attributed to the covered entity (except where the employee is the person committing the breach).
- Because of this standard, covered entities need to have reasonable systems in place to discover breaches including training of staff on prompt reporting of any known breaches.

Timeliness of Notification

- Notice must be provided to the individual without unreasonable delay and in no case later than **60 calendar days** after discovery of the breach.
- 60 days is an outer limit, if the covered entity has completed its risk assessment and confirmed the breach within 20 days, it should send the notifications immediately instead of waiting until day 60.

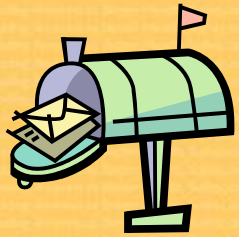
Content of Notification

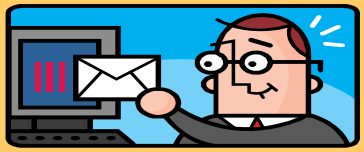
The notification must contain, to the extent possible:

- Description of what happened and dates, if known
- Description of the types of unsecured PHI involved in the breach
- Any steps individuals should take to protect themselves
- Description of what the covered entity is doing to investigate and mitigate harm
- Contact information for individuals to learn more which must include a toll-free telephone number, e-mail address, website, or postal address

Methods of Notification to Individuals

- Written notice to last known address or by e-mail if agreed to by the individual.
- If the individual is deceased, notification may be sent to the next of kin or personal representative of the individual if the CE knows the individual is deceased and has contact information for the next of kin or personal representative.
- Notification may be provided in one or more mailings as information becomes available.
- In urgent situations, notice may be provided by telephone or other means in addition to written notice.





Substitute Individual Notification

- Where here is insufficient or out of date contact information, a substitute form of individual notice reasonably calculated to reach the individual may be provided such as e-mail or telephone
- If the individual is deceased and there is insufficient contact information, no substitute notification is required

Substitute Individual Notification for 10 or more persons

- If the covered entity does not have sufficient contact information for ten or more affected individuals, the following applies:
  1. Conspicuous posting for 90 days on home page of covered entity's website or posting in print or broadcast media where affected individuals may reside; **and**
  2. Include a toll-free number that remains active for at least 90 days where individuals can learn whether they were affected by the breach.
- The posting must include the same information as the written notice to individuals.

45 C.F.R. §164.404(d)(2)

Notification to the Media

- For a breach involving more than 500 residents of a state or jurisdiction, the covered entity must notify prominent media outlets serving that state or jurisdiction in addition to written notice to individuals.
- Must be done without unreasonable delay, no later than 60 days after discovery of breach.
- Content of the notification to media is the same as that which was given to individuals.

Examples of Notification to Media

- If a laptop that contains unsecured PHI of more than 500 residents of a particular city is stolen, the covered entity would need to notify a major television station or daily newspaper serving that city or entire state.
- If the stolen laptop contained the unsecured PHI of 200 residents from State A, 200 residents of State B, and 200 residents of State C, no reporting to the media would be required since there were not 500 or more residents affected from any one state. In this case, however, the covered entity would still be required to report the breach to the Secretary.

Notification to the Secretary

- If a breach involves 500 or more individuals, the covered entity must report the breach to the Secretary at the same time it notifies affected individuals.
- If a breach involves less than 500 individuals, the covered entity will make an annual reporting of all such breaches occurring in a calendar year to the Secretary.
- Reporting by covered entities will be done via OCR's website.
- This data is collected for reporting to Congress and notification to the Regions.

Business Associates

- Business associates must notify covered entities of breaches without unreasonable delay and in no case later than 60 days.
- Breaches are treated as discovered on the first day that the breach is known or by exercising reasonable diligence would have been known to the BA.
- The content of the notification from the BA to the CE must include, to the extent possible, the identification of the affected individuals and as much information that is known to the BA which the CE would be required to include in it notice to the individual.

Action by the CE upon the BA's notification

- If the BA is an independent contractor of the CE (which most BAs are), the notification "clock" for the CE begins when the CE receives notification from the BA regarding the potential breach.
- If the BA is acting as an agent of the CE, notice will be imputed to the CE and the notification "clock" for the CE begins on the day the BA knows or should have known about the underlying breach.

Law Enforcement Delay

- If law enforcement makes a written statement to a covered entity or business associate that notification or posting of a breach would impede a criminal investigation, the covered entity must delay notification until the time specified by law enforcement.
- If the requested delay by law enforcement is oral, the covered entity must document the oral request and delay notification for no longer than 30 days from the date of the request.

Administrative Requirements for Covered Entities

- Many of the administrative requirements at section 164.530 incorporate the breach notification provisions in Subpart D.
- In the event of an impermissible use or disclosure of PHI, the covered entity or business associate has the burden of demonstrating that all notifications were made as required by Subpart D or that the incident did not constitute a breach.

OCR Web Site

- http://www.hhs.gov/ocr/hipaa/
- The full text of the Privacy and Security Rules
- HIPAA Privacy Rule summary
- Covered entity "decision tool" to assist individuals and entities in making these determinations
- Over 200 frequently asked questions
- Fact sheets
- Information about the OCR enforcement program