Patient Notification of Breach of Unsecured PHI

System Administrators & Information Custodians
August 2009
HITECH Act HIPAA Amendment

Published 8/24/09; Effective 9/23/09

Covered Entities must notify individual and HHS following discovery of a breach of unsecured PHI.

1. HHS Commentary: “We believe the cost of notifying affected individuals and loss of business that may result from a breach of PHI provide strong incentives for the entity to improve its data security so as to prevent future breaches.”
The cost is expected to be steep:

1. The Ponemon Institute, LLC report of February 2009, “2008 Annual Study: Cost of a Data Breach” estimates that 69 percent of the cost of a data breach is the result of lost business. The study identifies the health care industry as experiencing the highest customer turnover rate directly attributable to data breaches of protected health information.

2. The cost just for handling calls for a breach affecting 500 patients is estimated at more than 8 million dollars.
Two methods to secure PHI:

1. Electronic encryption
   - Currently, our data at rest is not encrypted

2. Paper, film, hardcopy “shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed”
Breach: “unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information”

1. “Unauthorized” means “an impermissible use or disclosure of PHI under the Privacy Rule”
Patient Notification

1. Exceptions:

   • **Unintentional** acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or BA
   
   • **Inadvertent** disclosure of PHI from one person authorized to access PHI at an CE or BA to another person authorized to access PHI at the CE or BA
   
   • Unauthorized disclosure in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information
“Compromises the security or privacy of such information” means “poses a significant risk of financial, reputational, or other harm to the individual”

1. **Risk Assessment** required to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure
   - Must be documented.
Patient Notification

• Consider who impermissibly used or to whom the information was impermissibly disclosed (i.e. to another CE = less risk; PHI returned prior to being accessed – i.e. stolen laptop found, PHI not accessed = less risk)

• Consider the type and amount of PHI involved in the impermissible use or disclosure
  • 1 narrow exception: limited data set that does not contain birth dates or zip codes.
Patient Notification

• If the risk assessment identifies that no significant risk of harm to the individual, then no breach has occurred and no notification is required

  1. Burden of proof on the CE to demonstrate that an impermissible use or disclosure of PHI did not constitute a breach. Must maintain documentation of notification, or alternatively, of the risk assessment.
Patient Notification

Steps in a nutshell:

1. Does the use or disclosure violate the Privacy Rule?
   - If YES, then

2. Does the violation compromise the security or privacy of the PHI?
   - If YES, then

3. Does the incident fall under one of the exception to the breach definition?
   - If NO, then…
Patient Notification

Notification

1. CE must send required notification without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered by the CE.
   • A breach is “discovered” when the CE knows about it, OR, by exercising reasonable diligence, would have known of a breach. **It is important that CEs implement reasonable systems for discovery of breaches.**

2. Privacy Office will send notifications out & maintain risk assessment documentation
Patient Notification

Content of Notification:

1. Description of what happened
2. Types of unsecured PHI involved
3. Any steps individual should take to protect themselves from potential harm
4. What CE is doing to mitigate harm
5. Contact procedures for individuals to ask questions
   • Must provide meaningful access for LEP patients (i.e. different languages)
Patient Notification

Methods of Notification:

1. Notice in written form by first-class mail at the last known address. If individual is deceased, send notice to next-of-kin

2. Must provide substitute notice for mail returned as undeliverable or for patients whose address is unknown
   - More than 10: conspicuous posting on CE’s website homepage or in the newspapers (in geographic areas where patients are likely to reside) for 90 days. If hyperlink, it must be prominent.
   - Must have a toll-free number for calls also
Breach of more than 500 residents of a state:

1. Must notify the media, in addition to sending letters. Supplements but does not substitute for the individual notice.
   • Example: breach involving 600 individuals; 200 in each of three states, no media notification required;

2. Must also immediately notify the Secretary, HHS. HHS will publicly post the names of CEs with breaches of more than 500.

CEs must maintain a log of all breaches of unsecured PHI and submit information annually to the DHHS Secretary
Other HHS comments:

1. CEs and BAs must have reasonable systems in place to detect breaches -- auditing is very important

2. Administrative requirements:
   - Develop and document policies and procedures
   - Train workforce members
   - Have sanctions for failure to comply with these policies and procedures
   - CEs must refrain from intimidating or retaliatory acts
   - All documentation required must be kept for 6 years
Your Responsibilities

If you suspect a privacy or information security breach, notify the Privacy or the Information Security Officer immediately.

Do not conduct your own risk assessment – please call us.

Auditing and monitoring of information systems is paramount.