Managing Breaches:
Understanding Applicable State and Federal Law

Aimee Wall
UNC School of Government

What should the health department do if health information "escapes" or is misused? Health departments know that they must act fast to respond this type of information breach but they are not always sure how they should respond. For the most part, the department's response should draw upon common sense and good management skills, but there are some legal guideposts that must be followed as well. Both federal and state laws address the issue of health information breaches.

The first step in the legal analysis is to evaluate the facts of the situation and determine whether legal obligations have been triggered. The trigger in this context is a breach – the health department must determine whether a breach occurred. If so, the next step is to identify the department's legal duties. One of the primary duties in both sets of laws relates to notice – notice to individuals, the public, and/or the government. In addition, federal law requires the health department to mitigate potential harm caused by the breach and include the breach in any accounting of disclosures. Below is a review of what constitutes a breach and a discussion of the legal duties triggered in the event a breach is discovered.

WHAT IS A "BREACH"?

Federal

Under federal law,[1] the term "breach" means the acquisition, access, use, or disclosure of protected health information[2] (PHI) in a manner not permitted by the HIPAA Privacy Regulation ("Privacy Regulation") which compromises the security or privacy of the PHI. Security or privacy of PHI is compromised if the breach poses a significant risk of financial, reputational, or other harm to the individual (often referred to as the "risk-of-harm threshold").

There are a few exceptions to the federal definition.

- Unintentional access or use: When a workforce member or person acting under the health department's authority (including through a BA), *unintentionally* acquires, accesses, or uses PHI in violation of the Privacy Regulation, a breach will not exist if (1) the person acted in good faith, (2) the action was within the person's scope of authority, and (3) the action does not result in further use or disclosure in violation of the Privacy Regulation.

---

[1] Breach provisions were added to the HIPAA Administrative Simplification based on a statutory directive included in a section of the 2009 stimulus bill often referred to as the HITECH Act. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5). The new regulations are primarily found in 45 C.F.R. Part 164, Subpart D (45 C.F.R. § 164.400 through 164.414).

[2] The term "protected health information" is defined broadly to mean individually identifiable health information, whether oral or recorded in any form or medium. It includes information that relates to the past, present, or future physical or mental health or condition of an 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. 45 C.F.R. § 160.103.

- Inadvertent disclosure: When a person acting under the health department's authority inadvertently discloses PHI to another person at the health department (or a BA) who is *not* authorized to receive that particular PHI but *is* authorized to receive other PHI, a breach will not exist if the action does not result in further use or disclosure in violation of the Privacy Regulation.
- Disclosure without retention: When PHI is disclosed in violation of the Privacy Regulation, a breach will not exist if the health department "has a good faith belief…that the person to whom the disclosure was made would not reasonably have been able to retain such information."[3]

State

Under state law, the term "security breach" is defined in the context of the Identity Theft Protection Act in the consumer protection arena.[4] The term refers to an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing *personal information* if:

- illegal use of the personal information has occurred,
- illegal use of the personal information is reasonably likely to occur, or
- the incident creates a material risk of harm to a consumer.

A security breach also exists if encrypted records or data are involved *and* the key is also available.

This state law protects "personal information," which is different from PHI. In order for information to be "personal information" under this law, it must include all of the following: the person's first initial or name, the person's last name, and at least one piece of "identifying information" such as a social security number, financial account number, email address, or fingerprints.[5] Publicly available records and directories are not considered personal information.

The only exception to the definition of security breach specifically recognized in the law applies when employees or agents (i.e., BAs) of the health department acquire and use the information (1) in good faith and (2) for a legitimate purpose.

WE HAVE HAD A BREACH – WHAT SHOULD WE DO ABOUT IT?

If a health department determines that a breach involving PHI has occurred, federal law imposes two immediate duties: the duty to mitigate harm and the duty to provide notice of the breach to various parties. In the event of a breach involving *disclosure* (as opposed to *use*) of PHI, the department must also ensure that the breach is reflected in its accounting of disclosures.

If a health department determines that a breach of personal information has occurred under state law, the department's primary legal responsibility relates to notice.

---

[3] 45 C.F.R § 164.402(2)(iii).

[4] Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A. The relevant section of this Article (G.S. 75-65) is made applicable to health departments via G.S. 132-1.10(c1).

[5] The full list of "identifying information" is: (1) social security or employer taxpayer identification numbers, (2) drivers license, state identification card, or passport numbers, (3) checking account numbers, (4) savings account numbers, (5) credit card numbers, (6) debit card numbers, (7) personal identification code (PIN) assigned to a cardholder of a financial transaction card, (8) electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names, (9) digital signatures, (10) any other numbers or information that can be used to access a person's financial resources, (11) biometric data, (12) fingerprints (13) passwords, and (14) parent's legal surname prior to marriage. G.S. 14-113.20(b). Items (8), (13) and (14) are *not* considered identifying information unless it would permit access to a person's financial account or resources.

Mitigation

If PHI is used or disclosed in a manner that violates the health department's policies and procedures or the Privacy Regulation, the health department has a duty to "mitigate to the extent practicable, any harmful effect that is known" to the health department.[6] What does that mean? The answer will depend on the circumstances. Mitigation basically means that the health department must try to lessen or minimize the severity harm to the person whose information was used or disclosed.[7] The department will need to evaluate the circumstances of the use or disclosure and determine which steps are most appropriate.

Notification

Federal

If a health department discovers a breach of *unsecured*[8]PHI, federal law requires the following notifications:

- *Individual*: The health department must notify each individual whose PHI has been (or is reasonably believed by the department to have been) accessed, acquired, used, or disclosed. The notification must take place "without unreasonable delay" (no more than 60 calendar days). See below for details regarding the content of the notice.
- *Media*: If the breach involves more than 500 residents of the state or a jurisdiction, the health department must notify prominent media outlets serving that State or jurisdiction. The notification must take place "without unreasonable delay" (no more than 60 calendar days).
- *U.S. DHHS*: The health department must notify the U.S. Department of Health and Human Services of *all* breaches of unsecured PHI.[9] For larger scale breaches (>500), the notification must occur at the same time the individual is notified. For smaller scale breaches (<500), the department must provide an annual log or accounting of breaches to DHHS not later than 60 days after the end of the calendar year.

If a business associate of the health department discovers a breach, it must notify the health department "without unreasonable delay" (no more than 60 calendar days). Once the health department receives such notice from a business associate, it must then make its required notifications.

Law enforcement officials may request a delay in notification in some circumstances.

---

[6] 45 C.F.R. § 164.530(f).

[7] mitigate. Dictionary.com. *Merriam-Webster's Dictionary of Law*. Merriam-Webster, Inc. http://dictionary.reference.com/browse/mitigate (accessed: April 16, 2010).

[8] The notification requirements apply only when the PHI used or disclosed was "unsecured." PHI is considered "unsecured" if it is not secured using a technology or methodology specified by guidance issued by the U.S. Department of Health and Human Services (DHHS). The guidance was issued in draft form on April 17, 2009 and was amended to address concerns raised by public comments. In short, the guidance describes technologies and methodologies that render PHI "unusable, unreadable, or indecipherable to unauthorized individuals – with a primary focus on (1) encryption and (2) destruction of storage media. The current version of the guidance is available online at http://www.hhs.gov/ocr/privacy/ or can be found at 74 Fed. Reg. 42742-43.

[9] Information and links for reporting breaches to DHHS are available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

State

If the health department discovers a security breach, state law requires the following notifications:

- *Individual*: The health department must notify the affected person without unreasonable delay. While the law does not define "unreasonable delay," it does recognize that the department will need to gather contact information, determine the scope of the breach and "restore the reasonable integrity, security, and confidentiality of the data system."
- *State:* If the health department is required to notify more than 1,000 people at one time, it must also notify the Consumer Protection Division of the Attorney General's Office without unreasonable delay.
- *Consumer reporting agencies:* If the health department is required to notify more than 1,000 people at one time, it must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

A law enforcement agency may request a delay in the notification in some circumstances.

Accounting

The Privacy Regulation provides that individuals have a right to receive an accounting of disclosures of PHI upon request.[10] Therefore, any breach that occurs must be reflected in the accounting. The health department should already have a system in place for documenting those disclosures that need to be included in an accounting so this should not actually present a change in the department's policies and procedures.

SHOULD THE DEPARTMENT ACTIVELY LOOK FOR BREACHES?

Under federal law, if a breach occurs and the health department fails to follow up as required by law, the department will be held responsible if it knew or *should have known* about the breach. In other words, a breach will be treated as discovered as of the first day it is known to the entity, or, *by exercising reasonable diligence would have been known to the entity.*[11]

The Privacy Regulation requires all covered entities, including health departments, to have administrative, technical and physical safeguards in place to prevent and help them identify breaches. Departments are also expected to train staff and volunteers about the entity's policies and procedures with respect to PHI and should have systems in place to identify workforce members who are not complying with those policies and procedures. If the department has all of these systems in place and they are all working well, the department should be able to identify and respond to breaches in a timely manner.

[10] 45 C.F.R. § 164.528.

[11] 45 C.F.R. § 164.404(a)(2) ("…a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity….").

NOTICE REQUIREMENTS: COMPARING FEDERAL AND STATE LAW

RECIPIENT OF NOTICE		
	FEDERAL	**STATE**
Individuals	Must notify each individual whose PHI has been (or is reasonably believed by the department to have been) accessed, acquired, used, or disclosed. The notification must take place "without unreasonable delay" (no more than 60 calendar days). See below for details regarding the content of the notice.	Must notify the affected person. The notification must take place "without unreasonable delay."
Government	Must notify U.S. DHHS of *all* breaches of unsecured PHI. If >500 breaches, notification must occur at the same time the individual is notified. If <500 breaches, the department must provide an annual log or accounting of breaches to DHHS not later than 60 days after the end of the calendar year.	Must notify the Consumer Protection Division of the Attorney General's Office without unreasonable delay.
Media	If >500 residents of the state or a jurisdiction, the department must notify prominent media outlets serving that State or jurisdiction. The notification must take place "without unreasonable delay" (no more than 60 calendar days).	None
Consumer reporting agencies	None	If > 1,000 individual notifications, must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.
CONTENT OF NOTICE		
	FEDERAL	**STATE**
Description of incident	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 incident in general terms

Description of information	A description of the types of unsecured PHI that were involved in the breach (but not the actual PHI)	The type of personal information that was subject to the breach
Advice to minimize harm	Any steps individuals should take to protect themselves from potential harm resulting from the breach	Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports
Description of action taken	A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches	The general acts of the business to protect the personal information from further unauthorized access
Contact information	Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Website, or postal address.	A telephone number that the person may call for further information and assistance, if one exists The toll-free numbers and addresses for the major consumer reporting agencies. The toll-free numbers, addresses, and Website addresses for the Federal Trade Commission and the NC Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.
METHOD OF NOTICE		
	FEDERAL	**STATE**
Written	Written notification by first-class mail to the individual at the last known address. Email notice permitted if the individual agrees to electronic notice.	Written notice. Electronic notice permitted if (1) valid email address, (2) individual agrees to electronic notice and (3) notice consistent with federal law regarding electronic records and signature.
Urgent situations	If possible imminent misuse, may notify by telephone or other means *in addition to* written notice.	

Substitute notice	If insufficient or out-of-date contact information, a substitute form of notice may be provided (i.e., telephone contact, media posting)	Substitute notice permitted if: - The cost of providing notice is >$250,000, - >500,000 people affected, - Department does not have sufficient contact information, or - Department is unable to identify particular affected persons. Substitute notice includes *all* three of the following: email for those with email addresses, website posting, and notice to major statewide media.