

## DHHS POLICIES AND PROCEDURES

---

<b>Section VIII:</b>	<b>Privacy and Security</b>
<b>Title:</b>	<b>HIPAA Breach Notification for Unsecured PHI</b>
<b>Current Effective Date:</b>	<b>4/1/2012</b>
<b>Revision History:</b>	
<b>Original Effective Date:</b>	<b>4/1/2012</b>

---

### Purpose

The purpose of the **HIPAA Breach Notification policy** is to require that all HIPAA-covered DHHS divisions, offices, and sections thereof (“agencies”) complete a Privacy Risk Assessment form to determine whether an incident is a **breach of unsecured protected health information** (“breach”). If DHHS agencies determine that a breach has occurred, that the breach poses a **significant** risk of financial, reputational or other harm to the individual(s) and that no exception exists, they are required to notify the affected individual(s).

*This policy is applicable to all DHHS agencies covered by HIPAA.*

### Background

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted on February 17, 2009. Subtitle D of Division A of the HITECH Act, entitled “Privacy,” among other provisions, requires covered entities under HIPAA and their business associates to provide notification in the event of breaches of unsecured PHI as specified in HIPAA, 45 C.F.R. § 164.404. These notification requirements apply with respect to breaches of unsecured PHI occurring on or after September 23, 2009.

### Policy

DHHS is already committed to ensuring that its agencies protect social security numbers (SSNs) and other identifying information of its clients and workforce members from identity theft. The **HIPAA Breach Notification policy** goes further to require that HIPAA-covered DHHS agencies determine if an unauthorized acquisition, access, use, or disclosure of PHI is a “breach” that poses a significant risk of financial, reputational or other harm to the affected individual(s). In performing a risk assessment, DHHS agencies must do the following:

- (1) Determine whether PHI was involved;

- (2) Determine whether there has been an unauthorized acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule;
- (3) Determine, and document, whether the unauthorized acquisition, access, use or disclosure compromises the security or privacy of the PHI. Compromising the security or privacy of PHI occurs when there is a significant risk of financial, reputational, or other harm to the individual;
- (4) Determine whether there was unsecured PHI involved in the breach (**i.e., not encrypted or destroyed**); and
- (5) Determine whether an exception to the notification requirement applies.

## Definitions

**Access:** the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

**Breach:** the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational, or other harm to the individual.

**NOTE:** A use or disclosure of PHI that does not include the individual's date of birth, zip code or that meets the requirements of a limited data set ( i.e. does not contain the identifiers listed at § 164.514(e)(2)), does not compromise the security or privacy of the PHI.

**Business associate:** a person outside the workforce who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of individually identifiable health information. Examples of business associates include third party administrators or pharmacy benefit managers for health plans, claims processing or billing companies, transcription companies, and persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to PHI.

**Covered entity:** a health plan, health care clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan.

**Discovered:** the first day on which the breach is known to a HIPAA-covered DHHS agency, or would have been known to any person who is a workforce member by exercising reasonable diligence.

**HIPAA Privacy Rule:** The HIPAA Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether **electronic, paper, or oral**. The HIPAA Privacy Rule calls this information PHI.

**Individually identifiable health information:** information that is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- 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; and
  1. Identifies the individual; or
  2. Reasonably could be used to identify the individual.

**Law enforcement official:** an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- Investigate or conduct an official inquiry into a potential violation of law; or
- Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

**Limited data set:** protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (1) Names; (2) postal address information, other than town or city, State, and zip code; (3) telephone numbers; (4) fax numbers; (5) e-mail addresses; (6) social security numbers; (7) medical record; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license plate numbers; (11) vehicle identifiers and serial numbers; (12) device identifiers and serial numbers; (13) Web URLs; (14) Internet Protocol (IP) address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.

**Protected health information:** individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Excludes individually identifiable health information in:

1. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
2. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
3. Employment records held by a covered entity in its role as employer.

**Risk Assessment:** a document that DHHS agencies must complete when submitting a privacy incident or complaint electronically. This document's questions help DHHS agencies determine whether there has been a breach of unsecured PHI.

**Same facility:** same covered entity, business associate, or organized health care arrangement in which the covered entity participates.

**Unsecured protected health information:** PHI that is not secured through the use of a technology or methodology specified by the Secretary that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals.

**Within the scope of authority:** person was acting on behalf of a covered entity or business associate at the time of the inadvertent acquisition, access, or use.

**Workforce member:** employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

## Implementation

The **HIPAA Breach Notification policy** will outline the procedures HIPAA-covered DHHS agencies should follow when they evaluate and report a suspected or known unauthorized acquisition, access, use, or disclosure of protected health information (PHI). These procedures will include information about to whom an impermissible acquisition, access, use, or disclosure of PHI should be immediately reported; who should be involved in determining if a breach of unsecured PHI has occurred; and if the affected individual(s) should be notified.

### I. Reporting HIPAA incidents and complaints

HIPAA-covered DHHS agencies which become aware of a suspected or known unauthorized acquisition, access, use, or disclosure of PHI shall **immediately** notify the DHHS Privacy and Security Office (PSO) by reporting the incident or complaint to the following link:

<https://security.dhhs.state.nc.us/incidents/privacy/index.php>

No later than three (3) business days, the agency's Privacy Official shall complete the "**Privacy Risk Assessment**" form and attach it as a file to the electronic report, in order to answer the following questions:

- Was PHI involved;
- If so, what types of PHI were involved;
- Was there an unauthorized acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule;
- Was the PHI encrypted using at least 128 bit encryption or destroyed by an acceptable method of destruction;
- Did the incident or complaint pose a significant risk of financial, reputational, or other harm to the individual;
- Does an exception to the notification requirement exist; and
- Do the affected individuals need to be notified?

There may be times when answers to the questions above are not yet available. In these instances, the agency's Privacy Official shall report the incident or complaint to the DHHS Privacy and Security Office (PSO) and use the ticket tracking ID number to update the incident or complaint as information becomes available.

***NOTE:** Reporting to the DHHS PSO shall not be delayed for investigative reasons. If definite answers to all of the questions above are not available at the time the incident or complaint is reported, the agency's Privacy Official shall provide the remaining answers no later than **three (3) business days** after the event has been reported to the DHHS PSO.*

## **II. Review by DHHS PSO and DHHS Office of General Counsel**

If, after reviewing the risk assessment and making an initial evaluation, the DHHS PSO determines that there may have been a breach of unsecured PHI, the DHHS PSO shall refer the event to DHHS General Counsel to make the final determination of whether a breach of unsecured PHI has occurred. If DHHS General Counsel, with assistance from the DHHS PSO and agency staff, determines that a breach of unsecured PHI has occurred, the DHHS General Counsel shall recommend notification. To ensure sufficient time for DHHS staff to perform the evaluative process, and to prepare and coordinate notification, if required, the DHHS General Counsel shall make a final decision no later than forty-five (45) days after the department's discovery of the incident.

In order to determine whether the breach of unsecured PHI may require a press release, the DHHS PSO or the DHHS General Counsel shall consult with the Secretary and the DHHS Office of Public Affairs.

### III. Overlapping incidents and complaints

There may be instances when overlapping issues arise and agencies are unsure about whether any given event could violate HIPAA, the NC Identity Theft Protection Act, DHHS policy, other privacy statutes or regulations or a combination thereof. There could also be situations where an event has privacy and security implications.

When evaluating incidents/complaints, the agency should look for key words such as “health information”, “SSN”, or “laptop” and consider how these words might suggest which type of incident or complaint to report.

**If:**

**Consider:**

health information	→	HIPAA
laptop or other DHHS-owned technology resource	→	[security] incident reportable to the DHHS PSO and ITS
SSN or other financial identifiers	→	NC Identity Theft Protection Act

**EXAMPLE:** There can be differences and similarities between a [security] incident reportable to the Department of Information Technology Services (ITS), a security breach under the NC Identity Theft Protection Act and a breach of unsecured PHI under HIPAA. For example, if a DHHS-issued laptop is stolen from a hotel, this event should be reported as a [security] incident to the DHHS PSO, since an information technology resource has been accessed or used without authorization. Whether this event is also a breach of unsecured PHI will depend upon whether the stolen laptop contained PHI (i.e., type of health information together with an identifier).

The “Privacy Risk Assessment” form should be completed to determine whether notification of the affected individuals is required. Whether the DHHS agency will have to notify the affected individuals will depend upon whether the laptop was encrypted or another exception to the notification rule exists. If PHI was present, unauthorized access posed a significant risk of financial, reputational, or other harm to the individual, information was not encrypted or sufficiently destroyed, and no exception exists, the agency will have to notify. If the event involves “personal information” and the laptop was not encrypted, this event could be a security breach, also requiring notification of the affected individuals (*See DHHS Identity Theft and Security Breach Notification Policy, Section VII - Privacy and Security, Privacy Manual, Identity Theft Policies*).

#### IV. Evaluating a HIPAA incident or complaint

The reporting obligation for DHHS agencies is triggered when there is a breach of unsecured PHI. In order to have a breach of unsecured PHI, there must be **PHI + a violation of the HIPAA Privacy Rule + compromise of the privacy and security of the PHI + unsecured PHI + no exceptions**. Therefore, in order to accurately evaluate a HIPAA privacy incident or complaint, please review sections A-E below.

##### A. PHI Involved

First, DHHS agencies should always determine whether PHI was involved. If no PHI was involved, then there can be no breach of unsecured PHI and no obligation to notify.

##### B. Violation of the HIPAA Privacy Rule

DHHS agencies must determine whether there has been an unauthorized acquisition, access, use, or disclosure of PHI in violation of the HIPAA Privacy Rule. If the DHHS agency determines that the HIPAA violation compromised the privacy and the security of the PHI, then the violation would be a “breach.”

##### C. Limited data set + removal of dates of birth and zip codes

DHHS agencies must determine whether a limited data set was involved or whether the dates of birth and zip codes had been removed. Disclosures of PHI that do not include an individual's date of birth or zip code and that meet the requirements of a limited data set are deemed not to compromise the security or privacy of PHI. Therefore, there would be no “breach” and notification would not be required.

**NOTE:** If either zip codes or dates of birth are included in the limited data set, however, then DHHS agencies would have to determine whether the incident compromised the privacy and security of the PHI.

##### D. Compromises the privacy and security of PHI

If a DHHS agency determines that there was a violation of the HIPAA Privacy Rule, it must determine whether the incident compromised the privacy or security of the PHI. In order to reach the harm threshold for a breach, the incident must create a “*significant risk of financial, reputational, or other harm to the individual*” when the incident occurred. The DHHS agency should consider the following factors to determine whether there was a **significant risk of harm**:

- (1) **Nature of the Data Elements Breached.** DHHS agencies should analyze the nature of the data elements compromised. For example, the disclosure of a person's name in one context may be more sensitive than the disclosure of a person's name in another context.
- (2) **Likelihood the information is accessible and usable.** DHHS agencies should assess the likelihood that unsecured PHI will be or has been used by unauthorized individuals.
- (3) **Likelihood the breach may lead to harm.** In the context of the type(s) of data involved in the breach, DHHS agencies should consider the number of possible harms that could arise as a result of the breach, and further assess the likelihood of harm.
- (4) **Ability of the DHHS agency to mitigate the risk of harm.** The risk of harm may depend upon the ability of the DHHS agency to mitigate the effects of the breach. A DHHS agency should consider appropriate breach prevention, monitoring, and mitigation measures that it can take in response to the breach.

#### E. Unsecured PHI – Use of Encryption or Destruction

The term *unsecured PHI* is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by HHS. On April 17, 2009, HHS issued guidance identifying two methods for "securing" PHI: encryption and destruction.

- (1) **Encryption.** To be considered unreadable, PHI must be encrypted using an NIST approved algorithm and procedure. Electronic PHI is encrypted when the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and the key to decrypt the PHI was not obtained. It is important to note that in order to comply with the encryption standards and ensure the encryption keys are not obtained, DHHS agencies must keep encryption keys on a separate device from the data that they encrypt or decrypt.
- (2) **Destruction.** Destruction is also an acceptable method of rendering PHI unreadable. Paper, film, or other hard copy media should be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

[http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)

## F. Exceptions to the Breach Notification Requirement

If DHHS agencies determine that there was a breach of unsecured PHI, they must determine if an exception exists, which could either prevent the necessity for notification of affected individuals or delay notification. The exceptions are as follows:

- (1) **Certain unintentional uses.** Notification is not required for any unintentional use, access, or acquisition of PHI by a DHHS workforce member or an individual acting under the authority of a DHHS agency or business associate, if the acquisition, access or use was made in good faith, within the scope of authority and does not result in further use or disclosure not permitted under the HIPAA Privacy Rule. For example, notification may not be required when a billing employee at a hospital mistakenly receives an email containing PHI, immediately deletes the email and alerts the sender of the mistake.
- (2) **Certain inadvertent disclosures.** Notification is not required for any inadvertent disclosure of PHI by a person who is **authorized** to access PHI at a DHHS agency or business associate if the recipient is **authorized** to access PHI at the same DHHS agency, business associate or organized health care arrangement, and the disclosed PHI is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule. For example, notification may not be required when an employee misdirects an email the wrong employee, but the wrong employee is authorized to see the PHI.
- (3) **Incidents involving no ability to retain the PHI.** Notification is not required when the DHHS agency or business associate has a good faith belief that the recipient was not reasonably able to retain the PHI. According to the federal Department of Health and Human Services (HHS), an example of this situation would be a covered entity that mails a number of explanations of benefits ("EOBs") to the wrong individuals, but the EOBs are returned unopened by the post office as undeliverable.
- (4) **Law Enforcement Notification Delay Allowed.** DHHS agencies are allowed to delay notification of affected individuals when law enforcement determines that there is a criminal investigation or that notification may damage national security. NOTE: In this specific case, notification is still required – just delayed.

If a law enforcement official informs the DHHS agency that the notice to individuals, to HHS or the media would impede a criminal investigation or cause damage to national security, the DHHS agency shall request that the

law enforcement official make an official written request for the delay, specifying the following information:

- his or her full name,
- title,
- organization name,
- reason for the delay; and
- proposed number of days to delay.

All oral requests for a notification delay should be evaluated on a case by case basis. Oral requests for a notification delay should be granted only in the most urgent and serious circumstances. The law enforcement official is still required to provide the information above.

DHHS General Counsel shall make the final determination of whether notification will be delayed. DHHS General Counsel may delay notification for up to thirty (30) days from the date the request was approved. If the law enforcement official can provide sufficient reasons for delaying notification more than thirty (30) days, DHHS General Counsel may consider his or her request.

## V. Notification

If DHHS General Counsel determines that a breach of unsecured PHI has occurred, the DHHS agency shall provide notice of the breach and maintain documentation of such notice.

### A. Notice to Affected Individual

Unless contrary instructions from law enforcement are received (See Section IV (F)(4) above), a written notice of breach shall be provided to each affected individual whose unsecured PHI has been breached, or is reasonably believed to have been breached, as follows:

- (1) **Timing of Notice.** The notice shall be provided promptly and no later than sixty (60) days after the DHHS agency discovers the breach. The breach is considered to be discovered on the first day on which the breach is known, or would have been known to any person who is a workforce member or agent of the DHHS agency (other than the person committing the breach) by exercising reasonable diligence.
- (2) **Manner of Notice.** The notice shall be sent by first-class mail addressed to the affected individual's last known address. Notice may be sent electronically if the individual has agreed to receive electronic notice and the agreement has not been withdrawn. If the DHHS agency **knows** that the

individual is deceased, the DHHS agency shall provide written notice to the next-of-kin or personal representative of such individual if it has the addresses of those individuals. Notice may be provided in one or more mailings as additional information becomes available.

- (3) **Content of Notice.** The notice shall be written in plain language and shall contain the following information: (a) a brief description of the incident, including the date of the breach and the date of the discovery of the breach, if known, (b) a description of the types of unsecured PHI involved in the breach (rather than a description of the specific PHI), (c) any steps the individual should take to protect himself or herself from harm resulting from the breach, (d) a brief description of what the DHHS agency is doing to investigate the breach, to mitigate the harm to the individual and to protect against future occurrences, and (e) contact procedures for the individual to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address.
  
- (4) **Substitute Notice.** If there is insufficient or out-of-date contact information for an individual that precludes written notice to such individual, as soon as reasonably possible after such determination, the DHHS agency shall provide notice reasonably calculated to reach the individual as described below.
  - a. If there is insufficient or out-of-date contact information for **fewer than ten (10)** individuals, notice may be provided by e-mail, telephone or other means.
  
  - b. If there is insufficient or out-of-date contact information for **ten (10) or more** individuals, notice shall (1) be in the form of either a conspicuous posting for ninety (90) days on the DHHS main website home page or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside, and (2) include a toll-free number that remains active for at least ninety (90) days so that the individual can learn whether his or her unsecured PHI was included in the breach.
  
  - c. Substitute notice need not be provided if the affected individual is deceased and the DHHS agency has insufficient or out-of-date contact information for the next of kin or personal representative of the individual.
  
- (5) **Urgent Notice.** If the DHHS agency determines that there is potential for imminent misuse of the unsecured PHI in connection with a breach, the DHHS agency may provide information regarding the breach to individuals

by telephone or other means, as appropriate, **in addition** to providing the required written notice as described above.

B. Notice to HHS

Unless contrary instructions from law enforcement are received (See Section IV (F)(4) above), in addition to notifying the individual as described above, the DHHS PSO also shall notify HHS of the breach of unsecured PHI. Such notification shall be provided as follows:

- (1) If the breach involves **500 or more** individuals, the DHHS PSO shall notify HHS of the breach contemporaneously with providing the notice to the individual and in a manner specified by HHS on its website.
- (2) If the breach involves **less than 500** individuals, the DHHS PSO shall maintain a log or similar documentation of the breach of unsecured PHI and shall report the required information on the HHS website no later than February 25<sup>th</sup> of each year.

C. Notice to Media

Unless contrary instructions from law enforcement are received (See Section IV (F)(4) above), if a breach involves **more than 500 residents of one state or jurisdiction**, in addition to notifying the individual and HHS, the DHHS agency also shall notify prominent media outlets serving the state or jurisdiction. Such notice shall be provided promptly and in no case later than sixty (60) calendar days after discovery of the breach. The notice shall contain the same information included in the notice to the individual.

**EXAMPLE:** If a DHHS agency discovers a breach of 600 individuals, 200 of which reside in North Carolina, 200 of which reside in Virginia, and 200 of which reside in South Carolina, such a breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media. However, individual notification would be required, as would notification to the HHS because the breach involved a total of 500 or more individuals. Conversely, if a DHHS agency discovered a breach of unsecured protected health information involving 600 residents within the state of North Carolina and 600 residents of Virginia, notification must be provided to the individuals, to a prominent media outlet serving the state of North Carolina, to a prominent media outlet serving the Commonwealth of Virginia and to HHS.

#### D. Communications with the Media or Outside Agencies

With the exception of the DHHS PSO, the DHHS Office of the General Counsel, and the DHHS Office of Public Affairs, DHHS employees **are not** authorized to speak on behalf of the department to media personnel or representatives of other outside agencies concerning HIPAA breach of unsecured PHI incidents that have or have not been reported. For more information, please consult the following Web site address:

[http://info.dhhs.state.nc.us/olm/manuals/dhs/pol30/man/Media\\_Policy1.htm](http://info.dhhs.state.nc.us/olm/manuals/dhs/pol30/man/Media_Policy1.htm).

If you need additional help in understanding the document indicated above, please contact the DHHS Office of Public Affairs at (919) 855-4840.

#### E. Retention of Breach Notice Documentation

The DHHS agency shall record and maintain thorough records of all activities related to suspected and known HIPAA breach of unsecured PHI incidents and to the provision of notice to either individuals, HHS, or any communication from law enforcement related to the delayed notification, if applicable, for at least six (6) years from the date the incident was closed or notice was provided, whichever date is the latest.

#### F. Reporting of Incident to DHHS by Business Associate

HITECH created requirements that apply directly to a covered entity's business associates ("BA") in the event of a breach of unsecured PHI. HIPAA-covered DHHS agencies enter into contracts with business associates to perform functions, activities, or services on DHHS agencies' behalves. If in the performance of this function, activity, or service, an incident involving the DHHS agency's PHI occurs, the BA is required to do the following:

- (1) **Notify the DHHS agency.** BA shall notify the DHHS agency immediately, but no later than 24 hours after discovery of an incident involving the DHHS agency's PHI. The DHHS agency will only have 60 days to notify individuals from the date the BA discovered the breach – not the date on which the BA notified the DHHS agency of the breach. Therefore, it is imperative that the BA conducts an investigation immediately and provides the DHHS agency with answers to the following questions:
  - (a) Was PHI involved;
  - (b) If so, what types of PHI were involved;
  - (c) Was there an unauthorized acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule;

- (d) Was the PHI encrypted using at least 128 bit encryption or destroyed by an acceptable method of destruction;
- (e) Did the incident pose a significant risk of financial, reputational, or other harm to the individual;
- (f) Does an exception to the notification requirement exist; and
- (g) Do the affected individuals need to be notified?

The content of the notification to the DHHS agency must also include, to the extent possible, the identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, breached, and any other available information that the DHHS agency is required to include in its notification to the individual.

There may be times when answers to the questions above are not yet available. In these instances, the BA shall report the incident to the DHHS agency and update the DHHS agency immediately as information becomes available. Reporting the incident to the DHHS agency shall not be delayed by BA for investigative reasons.

- (2) **Complete Risk Assessment.** After notifying the DHHS agency about the incident, DHHS agencies should require that the BA complete a risk assessment immediately, but no later than five (5) business days, to determine whether there has been a “breach of unsecured PHI.” If definite answers to all of the questions above are not available at the time the incident is reported, the BA shall provide the remaining answers as they become available. The burden to determine whether there is a risk of harm resulting from the breach is on the DHHS agency - not the BA. Therefore, a BA should not have the discretion to determine whether notification will occur.
- (3) **Contract language.** HIPAA-covered DHHS agencies shall include appropriate language in all contracts with BAs to reflect the BA’s responsibilities to do the following:
  - notify the DHHS agencies of incidents immediately, but no later than 24 hours;
  - provide detailed information (See section V(F)(1));
  - investigate the incident;
  - complete a risk assessment;
  - update the DHHS agency as more information becomes available; and
  - pay all costs of notification or provide the notification, at the discretion of the DHHS agency.
- (4) **Notification.** When an incident is reported by a BA, HIPAA-covered DHHS agencies, in consultation with the DHHS PSO and DHHS General

Counsel, shall review information provided by the BA to determine whether notification is required. If there is disagreement between the DHHS agency and the BA, the DHHS agency's decision shall control since DHHS owns the data and is responsible for providing the notification as the covered entity.

## **VI. Administrative Requirements**

### **A. Training**

DHHS agencies covered by HIPAA shall train all members of their workforce with respect to breach reporting obligations and procedures, annually, so they are able to identify suspected breaches of unsecured PHI and know how to report all suspected breaches to their Privacy Official immediately. Evidence of employees receiving this annual training shall be documented and maintained.

### **B. Intimidating or Retaliatory Acts**

DHHS agencies are prohibited from retaliating against individuals who exercise their rights, or file a complaint under the applicable HHS regulations.

### **C. Sanctions**

Sanctions will be imposed upon members of the DHHS workforce who fail to comply with DHHS breach notification policies and procedures. DHHS expects that all employees will comply with all laws, regulations, standards, policies, procedures, guidelines and expectations regarding the privacy and security of DHHS protected health information. Violations of this policy may subject an employee to disciplinary action up to and including dismissal, as well as any potential civil or criminal sanctions under the law.

### **D. Filing of a Complaint**

Individuals can file a complaint regarding a DHHS agency's compliance with the HIPAA breach reporting rules. This complaint should be investigated and resolved in the same time frame and manner as other privacy complaints (See [\*\*\*DHHS Privacy Incident and Complaint Reporting policy, Section VII - Privacy and Security, Privacy Manual\*\*\*](#)).

## **References**

1. HITECH Act Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009, (effective February 17, 2009)
2. HITECH Act Breach Notification Regulations (effective September 2009)
3. HIPAA Privacy & Security Rules 45 CFR Parts 160, 162, and 164
4. NIST SP 800-111 “*Guide to Storage Encryption Technologies for End User Devices*” and SP 800-88 “*Guidelines for Media Sanitization*”
5. Privacy Risk Assessment form, HIPAA-covered and Non-covered divisions/offices

*For questions or clarification on any of the information contained in this policy, please contact the [DHHS Privacy and Security Office](#). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#).*