Office of the Commissioner
Breach Notification Policy

Policy #: DHHS-02-18               Issue Date: 05/01/18
Revised without revisions: 10/19/18

I. SUBJECT

Consumer Information: Breach Notification Policy

II. POLICY STATEMENT

It is the policy of the Maine Department of Health and Human Services ("the Department") to comply with all applicable federal and state laws regarding data privacy, security, and breach notification. Because the Department collects personal and sensitive information from consumers of Department services, we take the protection of an individual's identity and information very seriously.

This policy applies to the entire Department, its workforce, contractors and agents who work with, access, use, disclose or maintain the Protected Health Information or other private consumer information (together, "PI") in the Department’s files or on its electronic systems, and explains how the Department will respond to a possible or actual breach of the privacy and/or security of PI maintained by the Department or its vendors in any format.

III. RATIONALE

This policy is developed to comply with federal and state requirements involving the breach of unsecured protected health information and/or personal information.

IV. PROCEDURE STATEMENT

A. Possible or Actual Breach of Privacy and Security of PHI

1. Reporting: Workforce members must immediately report any actual or potential risk to the privacy, security or confidentiality of PI, in any format, to their office Privacy/Security Liaison, and/or the Department’s Director of Healthcare Privacy consistent with the steps set forth in the Standard Operation Procedure for Responding to a Privacy/Security Incident (SOP) set forth in Attachment A. The Privacy/Security Reporting Template should be filled out and sent securely to the Director of Healthcare Privacy. Attachment A(1).
2. **Evaluate and Assess Risk:** Only the Commissioner’s designated privacy or security workforce members shall perform the required risk assessment in accordance with the guidance set forth in **Attachment B** and consistent with applicable state or federal law.

**B. Provide Timely Notice of Breach**

1. **Time Frame/Discovery of Breach:** The Department will comply with the applicable federal and/or state requirement(s) for timely notification of consumers if it determines that a breach has occurred.

2. **Law Enforcement Delay:** The Department will honor an appropriate law enforcement request to delay breach notification for 30 days, or longer if the request is in writing, if notification would compromise an investigation or other law enforcement activity. Once that restriction is lifted, the Department will notify the affected individuals within seven (7) days as required by State law.

3. **Business Associates:** The Department will contractually require business associates accessing, using, maintaining or disclosing PHI, in any format, on our behalf to notify us as soon as possible, but no later than 24 hours, after learning of a possible or actual breach. Business associates will be required to cooperate with the Department and provide as much information as possible for inclusion in the breach notification letter.

**C. Operational Responsibility:** The process of notifying affected individuals of a breach of their unsecured PI, will **only** be performed by a member of the Privacy/Security Team, Privacy/Security Steering Committee, or its approved designee(s) as set forth in Attachment A. The Department will follow the required process for providing notification to consumers, regulators, media, and others, as required by law.

**D. Workforce Training**

All members of the Department workforce shall receive training on this Breach Notification policy as part of the Department’s documented Health Information Privacy and Security training.

**E. Other the Department Privacy, Security and Compliance Policies**

This policy is applied within the context of the Department’s commitment to information privacy and security generally, as required by law. Within that framework, workforce members must continue to comply with all the Department privacy and security policies, or risk sanction up to and including termination of employment.
V. DEFINITIONS

**HIPAA - Protected Health Information** is information about a patient, including clinical or demographic information that may identify a patient, which relates to the patient's past, present or future physical or mental health or condition, related health care services or payment for health care services.

**HIPAA- Unsecured Protected Health Information** is PHI that has not made "unusable, unreadable, or indecipherable" to unauthorized users through a method such as government specified encryption or other destruction method. PHI that is considered "secured" would not require the Department to provide notification to individuals, the media or others in the event of a breach.

**Maine: Notice of Risk to Personal Data Act - Personal Information means** an individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

A. Social security number; B. Driver's license number or state identification card number; C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; D. Account passwords or personal identification numbers or other access codes; or E. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information is compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

VI. DISTRIBUTION

All Staff via e-mail and posting on the DHHS Intranet.

VII. ATTACHMENTS

A Standard Operating Procedure for Responding to a Privacy/Security Incident
A(1) Incident Reporting Template
B Breach Risk Assessment Guide
B(1) Breach Notification Requirements Checklist
B(2) Notification Requirements to Secretary of DHHS
B(3) Notification to Media
B(4) Maine Law, Consumer Reporting Agencies

____________________  ______________________
October 19, 2018       Bethany Hamm
                        Acting Commissioner
Standard Operating Procedure for Responding to a Privacy/Security Incident

**For the purposes of this SOP, "incident" is defined as an actual or potential exposure of consumer information.**

**Example:**
1. If ePHI/PI was posted to a public site, take it down ASAP.
2. If PHI/PI was accidentally emailed to the wrong person, a) email a request to delete along with an affirmation of destruction or b) mail the affirmation to the recipient in a self-addressed stamped envelope ASAP.

**Privacy/Security Team:**
- Director of Healthcare Privacy (HPD)
- General Counsel (GC)
- Director of Business Technology (DBT)
- Commissioner’s Office Administrative Support Staff (COS)

**Incident* Reported to DHHS Staff**

1. Complete written incident reporting template (Attachment A(1)) with currently known details. Email securely to Privacy/Security Team. COS to open new matter.
2. Call/email HPD.
3. Mitigate incident immediately, where possible. **

**Privacy/Security Team:**
1. Discuss initial details, HPD to document, identify root cause to the extent possible.
2. Apply law to the facts to determine whether breach has occurred under federal or state law.
3. If OIT- or OIT-vendor related, DBT = liaison.

If it appears that a breach HAS occurred and notification is required

1. Engage Appropriate Steering Committee Members.
2. Prepare notification to consumer, media, govt., etc.
3. Engage ID protection vendor where determined appropriate.

If it appears that NO breach has occurred

Mitigate, Educate, Monitor, Document

If it is unclear whether a breach has occurred

1. Continue investigation.
2. Engage Appropriate Steering Committee Members.
3. Breach?
   - Upon determination:
     - Yes
     - Engage members to comply with statutory requirements and documentation.
     - Following up with mitigation, monitoring, education.

If it looks like a breach has occurred
Privacy/Security Incident Reporting Template

Initial Contact – How did we learn of the incident?

Briefly Explain the Incident:

Risk Assessment Questions:

1. What was the specific information involved? What type of identifiers were exposed?

2. Was the data in paper, electronic, or another format? If electronic, was the data encrypted?

3. Who made the disclosure? How was the disclosure made?

4. To whom was the disclosure made?

5. Was the identifiable data viewed? Did the opportunity exist for the information to be viewed or acquired by someone without Department permission or authority?

6. Has the incident been mitigated – i.e., what has been done to fix the issue, if anything?

Please send this information to
Director of Healthcare Privacy (Encrypted, with High Importance)
Breach Risk Assessment Guide

All privacy and security issues or potential breaches are unique. The Department is required by law to document and maintain a record of each step of each HIPAA/HITECH risk assessment process.

At minimum, a good faith risk assessment must include the following 4-step inquiry:

1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification.

For HIPAA purposes, PHI consists of:
   a. Name;
   b. Street address, city, county, precinct, zip code;
   c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
   d. Phone numbers;
   e. Fax numbers;
   f. Email addresses;
   g. Social Security numbers;
   h. Medical record numbers;
   i. Health plan beneficiary numbers;
   j. Account numbers;
   k. Certificate/license numbers;
   l. Vehicle identifiers and serial numbers, including license plate numbers;
   m. Device identifiers and serial numbers;
   n. Web Universal Resource Locators (URLs);
   o. Internet Protocol (IP) address numbers;
   p. Biometric identifiers, including finger and voice prints;
   q. Full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data). New – Genetic information, such as family history and test results.

Analysis: What type and amount of PHI was involved?
   • Is this a loss and return of a laptop with only highly encrypted information?
   • Were readable charts found outside of the Department?
   • Is this a single, misdirected fax that was shredded by the recipient who works for the same office?
   • Document the specific HIPAA identifiers involved.
Breach Risk Assessment Guide

2. The unauthorized person who used the PHI or to whom the disclosure of PHI was made.

Analysis: To determine whether such risk or harm applies, investigate the circumstances surrounding the incident, including:
- Who impermissibly used the information?
- Who had access to the information? Was there authorization to do so?
- Who shared or disclosed the information?
- To whom the information was impermissibly disclosed (e.g., was it disclosed to a recipient also governed by the Privacy Rule?)
- Was there a loss or theft?

3. Whether the PHI was actually viewed or acquired or, alternatively, if only the opportunity existed for the information to be viewed or acquired.

Analysis: Consider asking questions pertinent to the situation, such as:
- Was a lost portable device with PHI encrypted according to government standards, or was it unencrypted with an opportunity for information to be viewed?
- Were letters containing patient, member or client information sent to the wrong individuals and opened?
- Were patient files viewable to unauthorized individuals?

4. The extent to which the risk to the PHI has been mitigated.

Analysis: Consider asking questions pertinent to the situation, such as:
- What steps were taken to lessen the risk to the information disclosed?
- Did the recipient return the data and sign a confidentiality agreement affirming that no PHI was viewed or would be retained?
- Did the recipient have a Business Associate Agreement with the Department?
- Was the PHI impermissibly accessed, used or disclosed limited to that provided in a limited data set, pursuant to an executed Data Use Agreement, (which is PHI limited to demographics and dates) but without the inclusion of individual(s)' birthdate(s) and/or zip code(s)?
- Was the information de-identified, taking it outside of HIPAA protection?

Federal Exceptions/Safe Harbors are as follows:

1. The use, disclosure or access involving PHI was made unintentionally by a member of the workforce or an agent of the Department, was within the scope of that person's authority, and was not further used or disclosed.

Example: No breach notification is required where a provider unintentionally faxes unsecured PHI intended for review by another hospital colleague, but instead reaches the hospital billing office. The employee immediately both notifies the sender of the error and shreds the fax;
Breach Risk Assessment Guide

2. The *inadvertent* disclosure was made by the Department workforce member or Business Associate to another workforce member of the same entity and the PHI was not further used or disclosed.

   **Example:** Laboratory Assistant leaves file with PHI intended for registration on Medical Assistant’s desk in error. The receiving MA alerts the Laboratory Assistant immediately, redirects the file, and there is no further use;

3. A disclosure where the Department or its Business Associate believes in *good faith* that an unauthorized person to whom disclosure was made could not reasonably retain the PHI.

   **Example:** Staff gives member A’s document to member B, but then immediately realizes the error and recovers the document before member B studies the document or leaves the office.

If any of these safe harbors apply, notification is *not* required under federal law. If they do not apply, breach notification is required.
Breach Notification – Requirements Checklist

1. Notification must be made by first class mail to the last known address of the affected individual, or next of kin if deceased, or to parent/guardian for a minor or incapacitated patient.

2. Notification may be made by email where permitted by the patient.

3. Notification must be in plain language. Notice must also be in compliance with Title VI of the Civil Rights Act to ensure meaningful access to the notice by those with Limited English Proficiency, and to ensure appropriate notice/communication to those individuals with disabilities, in compliance with the Americans with Disabilities Act.

4. Content must include:
   a. A brief description of the event;
   b. Date of breach, and date of discovery of breach, to the extent these dates are known;
   c. Types of unsecured PHI disclosed, including full name, social security number, date of birth, home address, account number, diagnosis, disability code, etc.;
   d. Steps patients should take to protect themselves from potential harm from identity theft or fraud, such as contacting credit card companies, credit reporting agencies, etc.;
   e. A brief description of the actions taken by the Department to investigate the breach, mitigate/lessen the harm to individuals, and/or protect against further breaches;
   f. The Department's contact information for individuals to ask questions or learn more, including a toll-free number, email address, website, or postal address.

5. The General Counsel shall be consulted in all breach notification situations, and in all cases, prior to any type of notification or public reporting. In the event of breach of security of an electronic system as defined by Maine's Notice of Risk to Personal Data Act, the General Counsel will make any required notification to the Attorney General.

6. Where 500 or more individuals are affected, in addition to letter notification, contemporaneous notice must be provided to:
   a. Major media outlets serving the area; and
   b. The Secretary of Federal DHHS via its DHHS website.

7. Where less than 500 individuals are affected, the Department must maintain a log of the breach(es) and submit it annually to DHHS within 60 days of the end of the calendar year via the DHHS website.

8. Where a crime report is made, law enforcement may delay notification for 30 days, or longer if requested in writing, to prevent interference with an investigation or criminal process.
Breach Notification – Requirements Checklist

9. Substitute notice, required where the Department is missing valid contact information for ten or more affected individuals, will require (a) conspicuous posting on the Department website for a minimum of 90 days and conspicuous notice in major statewide print or broadcast media in the appropriate geographic area where those impacted by the breach are likely to reside, both of which shall include a toll free telephone number, and (b) email notice to individuals, where email addresses are available. Substitute notice for less than ten individuals may take the form of written notice, telephone contact or other means.

10. **URGENT NOTICE**: Where a risk assessment and investigation deems the situation urgent because of the risk of misuse of PHI, we may wish to provide notice to individuals by telephone or other means, in addition to the first class mailing and any other notification methods required by law.

11. The Director of Healthcare Privacy will keep record of all our efforts in our investigation and breach notification follow up activities
Breach of Unsecured PHI
Notification to Secretary of DHHS

See the following link:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/briinstruction.html

Information required will include:

1. A brief description of the event;
2. Date of breach, date of discovery of breach to extent these dates are known;
3. Types of unsecured PHI disclosed, including full name, social security number, date of birth, home address, account number, diagnosis, disability code, etc., as well as the location of the PHI (laptop, email, portable device);
4. Steps clients should take to protect themselves from potential harm from identity theft or fraud, such as contacting credit card companies, credit reporting agencies, etc. ;
5. Safeguards in place prior to the breach;
6. A brief description of the actions taken by the Department to investigate breach, mitigate/lessen the harm to individuals, protect against further breaches;
7. The Department’s contact information for individuals to ask questions or learn more, including a toll-free number, email address, website, or postal address.
Breach Notification to Media Where 500 or More Individuals' Unsecured PHI is Affected

The following elements must be included in the communication:

1. A brief description of the event;
2. Date of breach, date of discovery of breach to extent these dates are known;
3. Types of unsecured PHI disclosed, including full name, social security number, date of birth, home address, account number, diagnosis, disability code, etc.;
4. Steps clients should take to protect themselves from potential harm from identity theft or fraud, such as contacting credit card companies, credit reporting agencies, etc.;
5. A brief description of the actions taken by the Department, to investigate breach, mitigate/lessen the harm to individuals, protect against further breaches;
6. The Department's contact information for individuals to ask questions or learn more, including a toll-free number, email address, website, or postal address.
Maine Law Requirement
Breach Notification to Consumer Reporting Agencies
Where Over 1,000 Individuals’ Unsecured PHI is Involved

1. Estimated number of individuals whose data is involved in breach;
2. Actual or anticipated date of notification to individuals; and
3. General content of notice, excluding identities and personal information.