Department of Public Health and Human Services (DPHHS)

Health Insurance Portability and Accountability Act ("HIPAA") Privacy Policy

Laurie Lamson,
Operations Services Branch Manager

Date:

Legal Citations: Health Insurance Portability and Accountability Act ("HIPAA"), HiTech Act of the American Recovery and Reinvestment Act ("ARRA") of 2009 (Social Security Act Sections 1171-1180, 42 USC 1320d- 1320d (9)), 45 CFR 164.302 et seq.

Policy Title:	Risk Assessment		
Policy Number:	016	Version:	1.0
Approved By:			
Effective Date:	January 1, 2010		

Purpose:

This policy addresses the use of the Risk Assessment Tool found at attachment A to this policy.

Policy:

1. General – DPHHS will conduct a risk assessment when protected health information (PHI) is accidently, inadvertently, or through employee error disclosed. DPHHS employees are responsible for adhering to other HIPAA polices related to disclosure of information before, during and after the risk assessment described in this policy.
2. The Risk Assessment Tool will be utilized as follows:
    a. There are 15 questions to be answered with either a "yes" or "no" on this Risk Assessment Tool.
    b. The answers to the questions posed on the Risk Assessment Tool will determine if there is a risk of harm to the individuals whose PHI was released.
    c. The questions deal with unsecured PHI, minimum necessary, significant risk, types and amounts of PHI involved, specific breach definition exclusions, and burden of proof.
3. DPHHS is charged with finding and proving a disclosure was not a breach using the Risk Assessment Tool. The findings and conclusions of the supervisor, bureau chief and others involved in the assessment will be sent to the HIPAA Privacy Officer, who will document the findings for the HIPAA record.
4. If the Risk Assessment Tool does determine the disclosure is a breach of PHI, the steps provided in Policy #17 – Duty to Notify will be followed.

address, account number, diagnosis, disability code or other types of information were involved).

3. Any steps the individual should take to protect themselves from potential harm resulting from the breach. Those steps would include contacting credit reporting companies and enrolling in yearly free credit reports.
4. A brief description of what DPHHS is doing to investigate the breach, to mitigate harm to the individuals, and to protect against further breaches.
5. Contact procedure for individual to ask questions or learn additional information, which includes a toll-free telephone number, an email address, website, or postal address.

DPHHS will notify the media per 45CFR164.406 of a breach of PHI that involves more than 500 individuals. This notification to the media is in addition to written notification to the individuals, it does not substitute for individual notification unless there is no known address, telephone number, or email address for the individual affected. DPHHS will utilize the Public Information Officer, DPHHS, 406-444-0936 to release this media information. The Public Information Officer will describe event and include the following information as communicated to the victims:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
3. Any steps the individual should take to protect themselves from potential harm resulting from the breach. Those steps would include contacting credit reporting companies and enrolling in yearly free credit reports.
4. A brief description of what DPHHS is doing to investigate the breach, to mitigate harm to the individuals, and to protect against further breaches.
5. Contact procedure for individual to ask questions or learn additional information, which includes a toll-free telephone number, an email address, website, or postal address.

DPHHS will notify the Secretary of Health and Human Services per 45CFR164.408 of a breach that involves more than 500 individuals. The letter will be incident specific and will provide information regarding what occurred. This notification is in addition to the yearly notification per federal regulations. The letter will also include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
3. Any steps the individual should take to protect themselves from potential harm resulting from the breach. Those steps would include contacting credit reporting companies and enrolling in yearly free credit reports.

4. A brief description of what DPHHS is doing to investigate the breach, to mitigate harm to the individuals, and to protect against further breaches.
5. Contact procedure for individual to ask questions or learn additional information, which includes a toll-free telephone number, an email address, website, or postal address.

DPHHS will utilize a Breach Notification Log to record breaches of PHI. This log/database will be used to report to the Secretary of Health and Human Services on a yearly basis. Samples of each of these letters, notifications, and logs are available on the "Forms" portion of the HHS website.

On a yearly basis, DPHHS will send a report due each February per federal regulation, to the Secretary regarding breaches of unsecured protected health information. This report is in addition to any notification letter(s) sent to the Secretary when there is a breach of unsecured PHI affecting over 500 individuals.

Contracts with business associates of DPHHS will specify the responsibility to notify the covered entity, DPHHS, immediately upon discovery of a breach of unsecured protected health information. Contract language may include language regarding who will take responsibility for breach notifications. In the absence of such language, DPHHS will be responsible for notifications.

When notification would jeopardize law enforcement activity, and they have properly notified DPHHS and the business associate requesting a delay, an additional 30 days will be allowed prior to notification being sent out. This temporary law enforcement activity delay will be recorded in the HIPAA database with detailed documentation regarding the law enforcement individual(s) who requested the delay – date of request, reason for delay and by authority of which law enforcement entity.

Department of Public Health and Human Services (DPHHS)

Health Insurance Portability and Accountability Act ("HIPAA") Privacy Policy

Laurie Lamson,
Operations Services Branch Manager

Date:
Revised Date:

Legal Citations: Health Insurance Portability and Accountability Act ("HIPAA"), HiTech Act of the American Recovery and Reinvestment Act ("ARRA") of 2009 (Social Security Act Sections 1171-1180, 42 USC 1320d- 1320d (9)), 45 CFR 164.302 et seq.

Policy Title:	Duty to Notify		
Policy Number:	017	Version:	1.0
Approved By:			
Effective Date:	January 1, 2010		

Purpose:

This policy addresses the Duty to Notify when unsecured protected health information (PHI) has been released or a breach of PHI has occurred. DPHHS is required to notify the affected individuals, the media and the Secretary of Health and Human Services without unreasonable delay and in no case later than 60 calendar days from the date of discovery of a breach.

Policy:

1. General – DPHHS is required to notify clients when a breach of PHI has occurred if that breach poses a significant threat to their privacy and security.
2. Based on the risk assessment results (HIPAA Policy 016), notification may be required to the individual involved, local or state wide media, and the Secretary of Health and Human services.
3. A report to the Secretary of Health and Human Services is required each year regarding breaches that occurred during the previous year.

Procedure:

DPHHS will utilize a written form letter delivered by first class mail at the last known address for notification to an individual of a breach. The letter will be incident specific and will provide information regarding what occurred. In the case of a returned letter or insufficient last known address, a substitute notice may be utilized such as a posted public notice, a web posting, a telephone call, or other means. The letter, notice or posting shall be done in a manner that is reasonably calculated to reach the individuals and include the following information:

1. The date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home

Attachment "A" HIPAA Policy 016 - Risk Assessment Tool *

Q#	Question	Yes - Next Steps	No - Next Steps
	Unsecured PHI		
1	Was the impermissible use/disclosure unsecured PHI (e.g.. not rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of Health and Human Services)? Currently DPHHS does not use encryption technology so any email containing PHI sent outside the State network would be a disclosure or use of unsecured PHI. The correct answer to this question would be "Yes".	Continue to next question	Notifications not required. **Document decision.**
	Minimum Necessary		
2	Was more than the minimum necessary for the purpose accessed, used or disclosed? Minimum necessary is the least amount of information (PHI) needed to fulfill the request. A party requesting the "entire medical record," must specifically justify the request as the minimum, or reasonable amount necessary to meet the needs of the request (e.g., transfer of care, medical history of longstanding condition, etc.) before DPHHS will disclose the PHI.	Continue to next question	May determine low risk and not provide notifications. **Document decision.**
	Was there a significant risk of harm to the individual as a result of the impermissible use or disclosure?		
3	Was it received and/or used by another entity governed by the HIPAA Privacy & Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 & FISA of 2002? Did you send it to a co-worker? Did you send it to a business associate? Is there a business associate agreement with that entity? Did you use unencrypted email?	May determine low risk and not provide notifications. **Document decision.**	Continue to next question
4	Were immediate steps taken to mitigate an impermissible use/disclosure (ex. Obtain the recipients' assurances the information will not be further used/disclosed or will be destroyed)?	May determine low risk and not provide notifications. **Document decision.**	Continue to next question
5	Was the PHI returned prior to being accessed for an improper purpose (e.g., A laptop is lost/stolen, then recovered & forensic analysis shows the PHI was not accessed, altered, transferred or otherwise compromised)?	May determine low risk and not provide notifications. **Document decision.** Note: don't delay notification based on a hope it will be recovered.	Continue to next question
	What type and amount of PHI was involved in the impermissible use or disclosure?		
6	Does it pose a significant risk of financial, reputational, or other harm?	Higher risk - should report	May determine low risk and not provide notifications. **Document decision.**

What type and amount of PHI was involved in the impermissible use or disclosure?			
7	Did the improper use/disclosure only include the name and the fact services were received?	May determine low risk and not provide notifications. **Document decision.**	Continue to next question
8	Did the improper use/disclosure include the name and type of services received, services were from a specialized facility (such as a substance abuse facility), or the information increases the risk of ID Theft (such as SS#, account#, mother's maiden name)?	High risk - should provide notifications	Continue to next question
9	Did the improper use/disclosure not include the 16 limited data set identifiers in 164.514(e)(2) nor the zip codes or dates of birth? Note: take into consideration the risk of re-identification (the higher the risk, the more likely notifications should be made).	High risk - should provide notifications	May determine low risk and not provide notifications. **Document decision.**
10	Is the risk of re-identification so small that the improper use/disclosure poses no significant harm to any individuals (ex. Limited data set included zip codes that based on population features such as the population centers around Missoula, Great Falls, Bozeman and Billings, doesn't create a significant risk an individual can be identified. In smaller population centers around Montana a zip code could run the risk of re-identification).	May determine low risk and not provide notifications. **Document decision.**	Continue to next question
Specific Breach Definition Exclusions			
11	Was it an unintentional access/use/disclosure by a DPHHS employee acting under the Department's authority, made in good faith, within his/her scope of authority (employee was acting on the Department's behalf at the time), and didn't result in further use/disclosure (ex. billing employee receives an e-mail containing PHI about a patient mistakenly sent by a nurse (co-worker). The billing employee alerts the nurse of the misdirected e-mail & deletes it)?	May determine low risk and not provide notifications. **Document decision.**	Continue to next question
12	Was access unrelated to the DPHHS employee's duties (ex. did a receptionist look through a patient's records to learn of their treatment)?	High risk - should provide notifications	Continue to next question
13	Was it an inadvertent disclosure by a person authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same organization, ***and*** the information was not further used or disclosed (ex. An employee who has the authority to use/disclose PHI in that organization discloses PHI to another individual in that same organization and the PHI is not further used/disclosed)?	May determine low risk and not provide notifications. **Document decision.**	Continue to next question

Specific Breach Definition Exclusions			
14	Was a disclosure of PHI made, but there is a good faith belief that the unauthorized recipient would not have reasonably been able to retain it (Ex. EOBs were mistakenly sent to wrong individuals and were returned by the post office, unopened, as undeliverable)?	May determine low risk and not provide notifications. **Document decision.**	Continue to next question. Note: if the EOBs were not returned as undeliverable, these should be treated as breaches.
15	Was a disclosure of PHI made, but there is a good faith belief that the unauthorized recipient would not have reasonably been able to retain it (ex. A nurse mistakenly hands a patient discharge papers belonging to a different patient, but quickly realized the mistake and recovers the PHI from the patient, and the nurse reasonably concludes the patient could not have read or otherwise retained the information)?	May determine low risk and not provide notifications. **Document decision.**	**Document findings.**
Burden of Proof: Required to document whether the impermissible use or disclosure compromises the security or privacy of the PHI (significant risk of financial, reputational, or other harm to the individual).			

*Montana Department of Public Health and Human Services adapted from HIPAA Collaborative of Wisconsin – HIPAA COW.