

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

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.