Title: HIPAA BREACH NOTIFICATION POLICY AND PROCEDURE	**Policy #: 0047 Dept: Compliance**
Effective Date: 1/2014	**Approved By:** Quality & Compliance Committee
Revision Dates: 3/2015	**Revision Date: 3/2015**
Sources: 45 CFR 164.102 through 164.534	

POLICY:
To establish PrimaryHealth's process for employee reporting of any breach or suspected breach of Protected Health Information (PHI). It is the policy of PrimaryHealth to protect the electronic transmission of PHI as well as to fulfill our duty to protect the confidentiality and integrity of member PHI as required by law and professional ethics.

PURPOSE:
The breach notification regulations from the Health Information Technology for Economic and Clinical Health (HITECH) Act require healthcare providers, health plans, and other HIPAA covered entities (including Business Associates) to notify individuals when their health information is breached. The number of individuals affected and the risk that they will be negatively impacted by the breach determines the action to be taken as required by the Health and Human Services Department.
The Breach Notification Template is one mechanism employees can use to report any release of Protected Health Information (PHI) and allows the PrimaryHealth Compliance Officer to determine the category, level of breach and type of corrective action required.

WHAT IS A BREACH?

The definition of the term 'breach':
'Impermissible use or disclosure of PHI is presumed to be a breach, unless it can be demonstrated that there is low probability that PHI has been compromised based upon a four-part risk assessment.'

Examples of a breach include:

- PrimaryHealth employee faxes or sends member PHI in any form or medium, including electronic information, to a healthcare provider in error;
- Member PHI sent by a PrimaryHealth representative to a person or organization outside of PrimaryHealth which was not sent by 'Secure Email' or PHI received at PrimaryHealth which was not sent by the provider or company using 'Secure Email';
- PrimaryHealth employee faxes or sends member PHI to an entity or individual not in the healthcare business (i.e. – Nike, Dominos Pizza, Joe Smith, etc.); or
- Any breach of PHI, including PHI contained in lost or stolen paper documents, laptops or other media. If an event of this type has occurred, immediately notify your manager and PrimaryHealth's Compliance Officer or designee at 541-471-4208 or email complianceofficer@ohms1.com

The term 'breach' does ***not include:***

- Unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or Business Associate if the acquisition, access, or use was made in good faith, within the course and scope of employment or other professional relationship, and does not result in further use or disclosure of the information.
- Any inadvertent disclosure from an individual who is authorized to access protected health information by a covered entity, Business Associate, or organized health care arrangement to another similarly situated covered entity, Business Associate, or organized health care arrangement in which the covered entity participates as long as the recipient does not further use or disclose the information.

  Example*: A member service representative receives and opens an e-mail, sent by a provider containing protected health information about an individual that is not currently a member of PrimaryHealth. The member service representative obtained this information within the scope of his or her authority and the provider sent it as they had reason to believe the individual was a PrimaryHealth member.*

  The member service representative is to notify the provider that the individual is not a PrimaryHealth member and delete the email and any attachments. This ensures that the disclosure of PHI would not negatively impact the individual in any way.

PROCEDURE:

1. Employees, members, providers and vendors may report any breach or suspected breach of PHI. When reports are received from members, providers, or vendors, PrimaryHealth personnel are to complete the Breach Notification Template.

2. When the Breach Notification Form is completed, save and attach the form to an email and send via secure email to **compliance officer@ohms1.com.** The form will be received by the Compliance Department for review and follow-up.

3. Additional action to be taken.

Situation	Action
PrimaryHealth employee sends member PHI in any form or medium, including electronic information, to a provider or company in error.	1. Complete the Breach Notification Form. 2. Contact the recipient of the PHI and direct them to destroy the document. 3. Document the disposition of the PHI on the Breach Notification Form. 4. Print the form and deliver to the Compliance department or email the Breach Notification Form as an attachment to complianceofficer@ohms1.com via secure email
Member PHI sent by a PrimaryHealth representative to a person or organization outside of PrimaryHealth which was not sent by 'Secure Email' or PHI received at PrimaryHealth which was not sent by the provider or company using 'Secure Email'	1. Complete the Breach Notification Form. 2. For PHI received by PrimaryHealth in an unsecure manner, contact the sender and advise them to send all future PHI in a secure manner. 3. Document the disposition of the PHI on the Breach Notification Form. 4. Print the form and deliver to the Compliance department or email the Breach Notification Form as an attachment to complianceofficer@ohms1.com via secure email
PrimaryHealth employee releases member PHI to a provider about the status of other procedures or requests from a different provider which the member might be seeing.	1. Complete the Breach Notification Form. 2. Document the disposition of the PHI on the Breach Notification Form. 3. Print the form and deliver to the Compliance department or email the Breach Notification Form as an attachment to complianceofficer@ohms1.com via secure email
Any breach of PHI, including PHI contained in lost or stolen paper documents, laptops or other media.	1. Immediately notify PrimaryHealth's Compliance Officer ordesignee at 541-471-4208 or Print the form and deliver to the Compliance department or email the Breach Notification Form as an attachment to complianceofficer@ohms1.com via secure email 2. Notify your manager

4. When in doubt if the release of PHI is a breach, complete the Breach Notification Form and contact the Compliance Officer for direction.

DEFINITIONS

Breach	Impermissible use or disclosure of PHI is presumed to be a breach, unless it can be demonstrated that there is low probability that PHI has been compromised based upon a four-part risk assessment.
Business Associate	A Business Associate is an entity that provides services to a Covered Entity and receives or has access to PHI from the Covered Entity. To perform its functions properly, a Business Associate must receive PHI and may use or disclose PHI.
Covered Entity	A Covered Entity is a Health Care Provider, a Health Plan or a Health Care Clearinghouse.
DHS	DHS is the Department of Health and Human Services, which is the federal agency charged with administering HIPAA.
HIPAA	HIPAA is the Health Insurance Portability and Accountability Act of 1996.
HIPAA Privacy Rules	The HIPAA Privacy Rules are the HIPAA regulations issued by DHS at 45 C.F.R. §§164.102 through 164.534.
Protected Health Information or PHI	Protected Health Information or PHI is health information, including demographic information collected from an individual that: 1) is created or received by PrimaryHealth; 2) relates to the past, present or future physical or mental health or condition of the 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; 3) identifies the individual (or reasonably could be used to identify the individual); and 4) is protected under the HIPAA Privacy Rules.

RELATED DOCUMENTS:

\\OHMS3\Employees\Policy and Procedure\HIPPA Breach Notification Form
HIPAA Policy Manual