HEALTH PLAN POLICY		
Policy Title: Breach Notification PHI - Reporting Guideline		**Policy Number:** AC20 **Revision:** D
Department: Administration	**Sub-Department:** Compliance	
Applies to Product Lines: ☐Medicaid ☐Children's Health Insurance Plan ☒Health Insurance Exchange ☒Medicare		☒USFHP ☒Commercial Insured ☐Non Insured Business
Origination/Effective Date: 09/29/2015		
Reviewed Date(s):	**Revision Date(s):** 03/02/2017, 04/10/2019, 04/15/2020, 04/01/2021	

SCOPE:

This policy is to provide guidance for breach notification when unauthorized access, acquisition, use and/or disclosure of member protected health information occurs. Breach notification will be carried out in compliance with regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the effective statutory revisions to HIPAA made pursuant to the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), which was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA).

DEFINITIONS AND ACRONYMS:

- **American Recovery and Reinvestment Act of 2009 (ARRA)**
- **Breach** - means the acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. Except as excluded in the definition below, an acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a breach unless the health plan or Business Associate (BA) demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated.

  Breach Excludes:

  - Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the health plan or BA if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
  - Any inadvertent disclosure by a person who is authorized to access PHI at the health plan or BA to another person authorized to access PHI at the health plan or BA, or organized health care arrangement in which the health plan participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
  - A disclosure of PHI where the health plan or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- **Disclosure -** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.
- **Health Information Technology for Economic and Clinical Health Act (the HITECH Act)**
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- **Office of Civil Rights (OCR) -** the governmental agency which is charged with enforcement of the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information.
- **Protected Health Information (PHI)** - means individually identifiable health information that is transmitted by electronic media; maintained in any medium; or transmitted or maintained in any other form.

POLICY:

A. Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to the health plan, or, by exercising reasonable diligence would have been known to the health plan (this includes breaches by the health plan's business associates). The health plan shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of the health plan. Following the discovery of a potential breach, the health plan shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed by the health plan to have been accessed, acquired, used, or disclosed as a result of the breach. The health plan shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of HHS), media outlets, law enforcement officials, etc.)

B. Breach Investigation: The health plan Privacy Officer or delegate, is to act as the investigator of the breach. The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordination with others in the health plan as appropriate (e.g., health plan administration, HIPAA security incident response team, legal counsel, public relations, risk management, human resources, etc.). CHRISTUS Health public relations shall be the facilitator for all breach notification processes (e.g., Secretary of DHHS, local media, individuals, law enforcement officials, etc.) as directed by the investigative team. All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

C. Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, the health plan will need to perform a risk assessment to determine if there is a low probability that PHI has been compromised. The health plan shall document the risk assessment as part of the investigation by noting the outcome of the risk assessment process. The covered entity has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the investigation team will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

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

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

3. Whether the PHI was actually acquired or viewed;

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

5. The plan to provide individuals with accountings of disclosure based on the necessary information available to the organization

D. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the health plan or the business associate involved. It is the responsibility of the covered entity to demonstrate that all notifications were made as required, including evidence demonstrating any necessity for delay.

E. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the health plan that a notification, notice or posting would impede a criminal investigation or cause damage to national security, the health plan shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

F. Content of the Notice: The notice shall be written in plain language and must contain the following information:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach.

2. A description of the types of unsecured protected health information that were involved in the breach; such as full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of personally identifiable information.

3. Any steps the individual should take to protect themselves from potential harm resulting from the breach.

4. A brief description of what the health plan is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

G. Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:

1. Notice to Individual(s): If, after a risk assessment, it is determined that an impermissible use or disclosure of PHI constitutes a breach and requires notification to individuals, notice shall be provided promptly and in the following form:

    a. Written notification by first-class mail the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the health plan knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out.

    b. Substitute notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

        1) In a case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

        2) In a case where there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the health plan's website, or a conspicuous notice in a major print or broadcast media in the health plan's geographic area where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days so an individual can determine whether their PHI was included in the breach.

    c. If the health plan determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

2. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

3. Known or suspected security or privacy breaches involving CMS information, or information systems, must be reported immediately to the CMS IT Service Desk. Additionally, Sponsor must contact the assigned ISSO and direct supervisor as soon as possible and apprise them of the situation.

4. Notice to Secretary of DHHS: The Secretary shall make available to the public on the DHHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 members is accessed, acquired, used or disclosed.

a. For breaches involving 500 or more individuals, the health plan shall notify the Secretary of DHHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

b. For breaches involving less than 500 individuals, the health plan will maintain a log of the breaches and annually submit the log to the Secretary of DHHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

H. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the health plan shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach.

1. A description of what happened including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.

2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date-of-birth, home address, account number, etc.).

3. A description of the action taken with regard to notification of patients regarding the breach.

4. Resolution steps taken to mitigate the breach and prevent future occurrences.

I. Business Associate Responsibilities: The BA of the health plan that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than five (5) calendar days after discovery of a breach, notify the health plan of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the health plan with any other available information that the health plan is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the health plan will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is the responsibility of the Covered Entity to document this notification).

J. Workforce Training: The health plan shall train all Associates on the policies and procedures with respect to PHI as necessary and appropriate for the Associates to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the health plan.

K. Sanctions: The health plan shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

L. Unauthorized access and/or disclosure: of protected health information will result in disciplinary action up to and including termination, professional discipline and potentially civil penalties and/or criminal prosecution as detailed below. Unintentional unauthorized disclosure or access: to PHI in verbal,

written or electronic means will result in a written warning to the workforce member. Repeated offenses will result in disciplinary action up to and including termination. Intentional unauthorized disclosure or access to PHI in verbal, written or electronic means for commercial or personal gain or for curiosity or malicious harm will result in immediate termination of employment. The OCR has the authority to impose civil penalties up to $1.5 million. OCR may also recommend that violators be subject to criminal prosecution by the Department of Justice and imprisonment may be imposed up to 10 years.

REFERENCES:

- OMB M-07-16, Privacy Data Breach, www.cms.gov
- CMS IT Service Desk: 1-800-786-2580, or email CMS_IT_Service_Desk@cms.gov
- The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414

RELATED DOCUMENTS:

None

REVISION HISTORY:

Revision	Date	Description of Change	Committee
New	12/01/2015	Initial release.	Board of Directors
A	03/02/2017	Compliance Annual Review and Policy Template update	Board of Directors
B	04/10/2019	Updated to current template. Removed Medicaid and CHIP from lines of business. Updated footnotes and References. Updated section G.3. Updated verbiage throughout policy.	Executive Leadership
C	04/15/2020	Yearly review. No change to policy content.	Executive Leadership
D	04/01/2021	Yearly review. No change to policy content.	Executive Leadership