Document ID: CHIP-0020	Title: CVS Health Corporate Breach Notification Policy and Procedure	
Parent Documents: N/A		
Effective Date: See Document Information Page	**Last Review Date:** See Review and Revision History Section	**Business Process Owner (BPO):** Exec Dir, Senior Counsel, LAW Privacy Legal
Exhibit(s): N/A		
Document Type: Policy and Procedure		

PURPOSE

The purpose of this Policy and Procedure is to set forth the steps that CVS Health® will follow with respect to a Breach of Protected Health Information (PHI), including electronic Protected Health Information (ePHI), and Personally Identifiable Information (PII) as required by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and state laws.

SCOPE

This Policy and Procedure applies to all CVS Health Workforce Members, entities, sites, departments, programs, Covered Entities and Business Associate functions who access, use, create, receive, maintain or transmit PHI/ePHI and/or PII.

This Policy does not apply to membership insured by non-US based coverage through Aetna® International Inc. (and its subsidiaries).

POLICY

1. The Privacy Office, in consultation with the Legal Department as appropriate, will determine whether any access, use, or disclosure of PHI/ePHI and/or PII that is not permitted by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) or applicable state privacy laws (an "incident") is a Breach requiring notification under the Breach notification provisions of the HIPAA Privacy Rule and/or applicable state law.

2. In determining whether the incident is a Breach under the HIPAA Privacy Rule, the Privacy Office will first determine whether the incident involved unsecured PHI/ePHI and/or PII.

3. If the incident involved unsecured PHI/ePHI and/or PII, the Privacy Office will perform a Risk Assessment of the unauthorized use or disclosure of PHI/ePHI and/or PII to determine if it constitutes a Breach or determine whether any of the exceptions to the definition of a "breach" under 45 CFR § 164.402 apply and/or applicable state law.

4. If none of the exceptions apply, the Privacy Office will coordinate with other business areas, including but not limited to security experts, forensic experts, Legal, Compliance, Human Resources, and Communications, as needed, who will determine whether there is a low probability that the PHI/ePHI and/or PII has been compromised based on a Risk Assessment of at least the following factors:

i. The nature and extent of the PHI/ePHI and/or PII involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI/ePHI and/or PII or to whom the disclosure was made;

iii. Whether the PHI/ePHI and/or PII was actually acquired or viewed; and

iv. The extent to which the Risk to the PHI/ePHI and/or PII has been mitigated.

5. If the Privacy Office cannot demonstrate based on the Risk Assessment that there is a low probability that the PHI/ePHI has been compromised, it will presume that the incident is a Breach.

6. The Privacy Office will do a review of applicable state law to determine whether the incident is a Breach under applicable state law.

7. If the Privacy Office determines that the incident constitutes a Breach under either the HIPAA Privacy Rule and/or applicable state law, then:

   a. for PHI/ePHI and/or PII held by CVS Health in a Covered Entity capacity, it will, subject to any delay required by law enforcement in accordance with the Privacy Rule, make the required notification to affected individual(s), the U.S. Department of Health and Human Services (HHS) and, if applicable, media and state government official/agencies of the Breach without unreasonable delay in the manner required by the Privacy Rule and/or applicable state law, but in no event later than 60 days after the Breach is discovered or sooner if required by applicable state law. The impacted business area(s) will work in consultation with the Privacy Office to notify impacted individuals and entities as needed.

   b. for PHI/ePHI and/or PII held by CVS Health in a Business Associate capacity, CVS Health will notify the Covered Entity of the impermissible use or disclosure in the time and manner required by the Business Associate Agreement (BAA) and in no case later than 60 calendar days after discovery. CVS Health will take the steps required by the BAA if different from the above steps.

8. The Privacy Office will document its investigation, Risk Assessment, and required notifications, and make such documentation available to HHS promptly upon request. CVS Health will retain the documentation for the period required by 45 CFR § 164.530(j).

9. All applicable Workforce Members will be trained on this Policy and Procedure as is necessary and appropriate for them to carry out their job functions, and within a reasonable period after the effective date of any material changes in this Policy and Procedure if the changes affect the Workforce Member's job function.

10. When serving as a Covered Entity, CVS Health shall treat a Breach as discovered as of the first day on which such Breach is known to CVS Health, or, by exercising reasonable diligence, would have been known to CVS Health. CVS Health, as a Covered Entity, 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 of CVS Health.

PROCEDURES

1. Reporting

All Workforce Members and all Business Associates are required to report immediately upon discovery to the Privacy Office any incident involving the acquisition, access, use, or disclosure of PHI/ePHI and/or PII in a manner not permitted by the Privacy Rule or applicable state law (see Mitigation of Improper Disclosure (CHIP-0024) for more information). Business Associates are required to inform CVS Health of a Breach in accordance with the Business Associate Use and Disclosure of PHI (CHIP-0027) Policy. The Privacy Office may be contacted at:

a. PBM, Accordant, Coram, CVS Specialty®, and Med-D: privacy.officer@cvshealth.com

b. CVS Retail: HIPAAIncidents@cvshealth.com

c. Long Term Care (LTC) Pharmacies and Omnicare®: LTCprivacy.officer@cvshealth.com

d. MinuteClinic®: HIPAAIncidents@cvshealth.com

e. Aetna lines of business: PrivacyInvestigationsandReporting@AETNA.com or other point of contact, as listed on the *Privacy website.*

2. Investigation

The Privacy Office will investigate all reported incidents to determine whether the acquisition, access, use, or disclosure of PHI/ePHI and/or PII was in violation of the Privacy Rule or applicable state law, and, if so, whether it constitutes a Breach.

3. Secured vs. Unsecured PHI/ePHI and/or PII

If the Privacy Office determines that the acquisition, access, use, or disclosure in question was in violation of the Privacy Rule or applicable state law, the Privacy Office, along with Information Security Architecture (ISA) if applicable, will determine whether the incident involved secured or unsecured PHI/ePHI and/or PII. If the incident involved secured PHI/ePHI and/or PII and does not constitute a Breach under applicable state law, it will document these findings, log any disclosures for accounting purposes to the extent required (see General HIPAA Privacy Policy (CHIP-057918) and Accounting of Disclosures (CHIP-051171) Policies for more information) and close the Risk Assessment.

4. Exceptions

a. If the Privacy Office determines that the incident involves unsecured PHI/ePHI and/or PII, it will determine whether the incident falls within one of the following exceptions under the HIPAA Privacy Rule:

i. Any unintentional acquisition, access, or use of PHI/ePHI by a Workforce Member or person acting under the authority of a Covered Entity or a Business Associate, if the 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 by the HIPAA Privacy

Rule. A person is acting "under the authority" of a Covered Entity or a Business Associate when the person is acting on behalf of that entity and is acting "within the scope of the authority" if the person was acting on behalf of the Covered Entity or Business Associate at the time of the impermissible access, use, or disclosure.

ii. Any inadvertent disclosure by a person:

A. who is authorized to access PHI/ePHI (1) at CVS Health to another person authorized to access PHI/ePHI at CVS Health; or (2) at a Business Associate of CVS Health to another person authorized to access PHI/ePHI at that Business Associate of CVS Health; or (3) at an organized health care arrangement in which CVS Health participates to another person authorized to access PHI/ePHI at that organized health care arrangement; and

B. the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

iii. A disclosure of PHI/ePHI where CVS Health has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI/ePHI.

5. Risk Assessment

a. If the Privacy Office determines that the incident does not qualify for an exception, it will determine whether there is a low probability that the impermissible acquisition, use, or disclosure of the unsecured PHI/ePHI compromised the PHI/ePHI involved. To do so, the Privacy Office or Business Associate(s) of the impacted business area(s), as applicable, will perform a Risk Assessment based on at least the following four factors:

i. The nature of the PHI/ePHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI/ePHI or to whom the disclosure was made;

iii. Whether the PHI/ePHI was actually acquired or viewed;

iv. The extent to which the Risk to the PHI/ePHI has been mitigated.

If the Privacy Office determines that that an unauthorized use or disclosure does not constitute a Breach, the Privacy Office will maintain documentation of the Risk Assessment or application of any exceptions to the definition of Breach.

6. State Law Review

The Privacy Office will review applicable state laws to determine whether the incident is a Breach under those laws, irrespective of whether it constitutes a Breach under the HIPAA Privacy Rule. Applicable state laws and regulations may provide for shorter notification periods than the limits set forth below. CVS Health will comply with the more stringent state law or regulation notification periods when applicable.

7. Notification Timeframe

If the Privacy Office cannot determine based on its Risk Assessment that there is a low probability that the PHI/ePHI and/or PII has been compromised and/or if it determines that the incident constitutes a Breach under applicable state law, subject to any delay required by law enforcement as provided in Section 15 below, it will notify affected individuals by first-class mail, without unreasonable delay, but in no event later than 60 days after the Breach is discovered or within such shorter time period specified under applicable state law. The 60 day period will be measured as of the first day on which the Breach is known, or by exercising reasonable diligence should have been known, to a CVS Health Workforce Member (other than the person committing the Breach) or to a Business Associate of CVS Health that is an Agent of CVS Health (as determined under Federal common law of agency).

8. Contents of Notification.

The contents of the notification will be written in plain language and will include, to the extent possible:

a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

b. A description of the types of unsecured PHI/ePHI and/or PII 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);

c. Any steps individuals should take to protect themselves from potential harm resulting from the Breach;

d. A brief description of what CVS Health is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches;

e. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address; and

f. Any additional information required by applicable state law.

9. Form of Notification.

Subject to any additional requirements under applicable state law:

a. The notification will be provided in compliance with governing state and federal laws and regulations and, where necessary, PBM client contractual obligations.

b. If CVS Health knows the impacted individual is deceased and has the address of the next of kin or Personal Representative of the individual, it will provide written notification by first-class mail to either the next of kin or Personal Representative of the individual. The notification may be provided in one or more mailings as information is available.

10. Substitute Notice.

Subject to any additional requirements under applicable state law:

a. If CVS Health has insufficient or out-of-date contact information that precludes written notification to the individual, it will provide a substitute form of notice reasonably calculated to reach the individual.

b. Substitute notice will not be provided to next of kin or Personal Representatives (if available) of the individual 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.

c. If there is insufficient or out-of-date contact information for fewer than ten (10) individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means. A toll-free phone number is not required.

d. If there is insufficient or out-of-date contact information for ten (10) or more individuals, then the substitute notice will:

   i. be provided in the form of either a conspicuous posting for a period of 90 days on the home page of the CVS Health website, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside; and

   ii. include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI/ePHI and/or PII may be included in the Breach.

11. Urgent Situations

The Privacy Office will make a determination whether an incident requires urgency because of the possible imminent misuse of unsecured PHI/ePHI and/or PII and, if so, it will provide notification by telephone or other appropriate means available in addition to the notification described above.

12. Media

If the Breach involves the unsecured PHI/ePHI of more than 500 residents of a state or jurisdiction, or as required by applicable state law, CVS Health will notify prominent media outlets serving the state or jurisdiction of the Breach within the same time frames and providing the same information as would be provided directly to the individual or as otherwise required by applicable state law.

13. HHS

a. For Breaches of unsecured PHI/ePHI made by CVS Health or a Business Associates of CVS Health, involving 500 or more individuals, regardless of their state or states of residence, CVS Health will provide notification of the Breach without unreasonable delay, and in no event later than 60 days following the discovery of the Breach, to HHS with the notice provided to the affected individuals and in the manner specified on the HHS website.

b. For Breaches of unsecured PHI/ePHI made by CVS Health or a Business Associate of CVS Health involving fewer than 500 individuals, the Privacy Office will maintain a log or other

documentation of the Breaches and, not later than 60 days after the end of each calendar year, provide notification to HHS for Breaches occurring during the preceding calendar year, in the manner specified on the HHS website.

14. Breaches of PHI /ePHI Held by CVS Health in a Business Associate Capacity

a. In the case of PHI/ePHI held by CVS Health in a Business Associate capacity, CVS Health will notify the Covered Entity following the discovery of a Breach of unsecured PHI/ePHI held on behalf of that Covered Entity.

b. CVS Health will provide the notification in the time frame specified in the BAA and will comply with the requirements of the BAA regarding any further notifications and steps following the Breach.

c. The notification will include, to the extent possible, the identification of each individual whose unsecured PHI/ePHI has been or is reasonably believed by CVS Health to have been, involved in the Breach.

d. CVS Health will provide the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available.

15. Delays for Law Enforcement

Subject to any additional requirements under applicable state law:

a. If a law enforcement official states to CVS Health that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, CVS Health will:

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

   ii. 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 is submitted during that time.

16. Notification to State Regulators and National Credit Reporting Agencies

If required, CVS Health will notify state regulators and national credit reporting agencies of a Breach in accordance with applicable state regulations.

17. Additional Notification Requirements in the Case of Part D Breaches Involving the PHI/ ePHI of Enrollees of a SilverScript Insurance Company (SSIC) Prescription Drug Plan

a. Except as provided in b. below, CVS Health will provide concurrent notification to SSIC's Regional Office Account Manager when it notifies HHS. This notification to the Regional Account Manager will include the same information that was submitted to HHS.

b. CVS Health will report to the Regional Account Manager within two (2) business days of learning of (i.e., it will not wait until the mandatory reporting date to HHS), or such other time frame specified in CMS Part D Guidance, any Breaches:

   i. for which there is a potential for significant beneficiary harm (i.e., a high likelihood that the information was used inappropriately); or

   ii. situations that may have heightened public or media scrutiny (i.e., a higher number of beneficiaries affected or particularly egregious Breaches).

c. In cases where CVS Health has notified HHS of the Breach within the time frame specified in Section 16.b., it may send a copy of that Breach report to SSIC's CMS Account Manager. Otherwise, CVS Health will send as much detail as possible to the CMS Account Manager via email, including a description of the Breach and the number of beneficiaries impacted.

d. CVS Health will take such additional steps as required by the CMS Account Manager. These steps may include:

   i. additional reporting (e.g., to provide corrective action steps taken in response to the incident);

   ii. beneficiary or provider notification, to the extent not already determined to be required per above process;

   iii. appropriate communications (e.g., press release, letters, etc.), to the extent not already determined to be required per above process; and

   iv. the provision of credit protection services, to the extent not already determined to be required per above process.

REFERENCES

- 45 C.F.R. §164.400-§164.414
- 45 CFR 164.530(j)

DEFINITIONS

1. **Aetna®**: Aetna Inc. and each of its subsidiaries that provide traditional and consumer-directed health insurance products and related services.
2. **Agent:** Any Employee or Contractor.
3. **Assessment:** The review of a Vendor's administrative, technical and physical security measures to assess compliance with CVS Health's information security policies, standards and procedures. An Assessment may be conducted via internal resources or by an external company.
4. **Breach:** Any acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule and which compromises the security or privacy of the PHI or that would require notifications under applicable state law.
5. **CMS**: Centers for Medicare and Medicaid Services.
6. **Information Security Architecture (ISA):** An organization within CVS Health charged with formulating information security policy, protecting Information Assets, and monitoring the security of CVS Health's technology infrastructure.
7. **Part D Breach:** A breach involving the PHI of a Medicare beneficiary.

8. **Personally Identifiable Information (PII):** Any piece of information which can be used to identify alone or when combined with other personal or identifying information which is linked to a specific individual. This includes name, address, biometric records, date of birth, social security number, mother's maiden name, telephone number.
9. **Risk:** A measure of the extent to which a resource is threatened by a potential circumstance or event, and typically a function of:
    - The adverse impacts that would arise if the circumstance or event occurs; and
    - The likelihood of occurrence. Information system or technology resource related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and technology resource, and reflect the potential adverse impacts to CVS Health's operations (including mission, functions, image, or reputation), assets, Agents, and/or other third parties.
10. **SilverScript Insurance Company (SSIC):** A CVS Health subsidiary that has contracted with Centers for Medicare and Medicaid Services (CMS) as a Medicare Part D Plan Sponsor.

Please refer to General HIPAA Privacy Policy CHIP-057918 for definitions of these defined words:

Accordant; Business Associate; Business Associate Agreement; Coram; Covered Entity; CVS Health®; CVS Pharmacy®; CVS Retail; CVS Specialty®; ePHI; Health Care Operations; Health Insurance Portability and Accountability Act (HIPAA); HIPAA Privacy Rule; Long Term Care (LTC) Pharmacy; Med-D; MinuteClinic®; Omnicare®; PBM; Personal Representative; Privacy Office; Protected Health Information (PHI); Workforce Member

REVIEW AND REVISION HISTORY

Date	Revision No.	Reason for Change	Sections Affected
02/08/10	1.00	New policy & procedure.	All
07/28/10	2.00	Updated procedure, added definition.	Procedures
12/16/11	3.00	Annual Review	All
03/14/13	4.00	Updated template; updated related document links.	All
03/07/14	5.00	Annual review. Updated template and updated link to related document CHIP-0003.	All
09/07/14	6.00	Coram integration. Added References section.	References
06/29/15	7.00	Updated template; revised Policy and Procedures sections; updated References and Definitions sections.	All
07/01/16	8.00	Annual review. Changed "Customer" to "individual" for clarification; updated email and Definitions list.	All
07/21/16	9.00	Header, Footer, or Review and Revision History changes only	Header, Footer, or Review and Revision History
02/21/17	10.00	Remove and replace outdated content; update template, entity names, and Definitions list.	All
02/21/18	11.00	Annual review; remove and replace outdated content; update template and Definitions.	All
02/20/19	12.00	Annual review; update template and Definitions	All
02/10/20	13.00	Annual review; remove and replace outdated content; update template and Definitions.	All
12/10/20	14.00	Remove and replace outdated content; update Purpose, Scope, Policy, Procedures, and Definitions.	All