Policy and Procedure		
SUBJECT: Reporting and Investigation of Potential Privacy and Security Breaches	DEPARTMENT: Regulatory Compliance, Risk Management and Government Affairs	
ORIGINAL EFFECTIVE DATE: **02/11**	DATE(S) REVIEWED/REVISED: **05/12, 10/14, 05/16, 12/17, 12/18, 10/19, 04/20**	
APPROVED BY: **Chief Compliance and Risk Officer**	NUMBER: **RA 42**	PAGE: **1 of 8**

SCOPE:
Providence Health Plan, Providence Health Assurance, Providence Plan Partners, and Ayin Health Solutions as applicable (referred to individually as "Company" and collectively as "Companies").

APPLIES TO:

Fully Insured						
Individual	Small Group	Large Group	Self-Insured	Medicare	Medicaid	Ayin
☐Oregon On Exchange	☐Oregon On Exchange (SHOP)	☐Oregon	☐ASO	☐Medicare	☐Medicaid	☐YCCO
☐Oregon Off Exchange	☐Oregon Off Exchange (SHOP)	☐Washington	☐TPA			☐WHA
☐Washington On Exchange						
☐Washington Off Exchange						
☒ APPLIES TO ALL ABOVE LINES OF BUSINESS						

POLICY:
Any Company workforce member who becomes aware of a suspected privacy breach, security breach, or inadvertent disclosure shall complete the online Privacy and Security Concern Form at the Regulatory Compliance, Risk Management and Government Affairs home page as soon as possible and within the same business day that the concern was received at the latest. The purpose of this policy is to describe steps that must be taken in the event of a Suspected or Actual Breach of Unsecured Protected Health Information (PHI) as required under the Health Insurance and Portability Accountability Act of 1996 (HIPAA) and by the Health Information Technology for Economic and Clinical Health Act (HITECH) or state privacy rules that protect all individually identifiable health information or PHI held or transmitted by Company and its business associates.

DEFINITIONS:

Breach or Actual Breach:

An unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI) which compromises the security or privacy of such information. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Breach does not include:

- Any good faith unintentional acquisition, access or use of PHI by a workforce member or business associate acting within the scope of employment where the PHI is not further used or disclosed. For example, if a workforce member inadvertently opens the wrong member's Facets record and therefore immediately closes out that member record without further using or disclosing the PHI.
- An inadvertent disclosure of PHI by one person authorized to access PHI to another person authorized to access PHI at the same covered entity, business associate or organized health care arrangement if the PHI is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule. For example, a workforce member is included in a Company email containing member PHI in error and deletes the email and does not further use or disclose the information.
- A disclosure of PHI where Company has a good faith belief that the unauthorized recipient would not reasonably have been able to retain the PHI. For example, a covered entity may send an explanation of benefits to the wrong individual. This inadvertent disclosure would typically trigger the breach notification requirements. However, if the explanation of benefits is returned to the covered entity unopened, the exception applies and there is no breach.

Examples of potential privacy breaches may include:

- Correspondence, letters, Explanation of Benefits (EOB) containing PHI received by someone other than the intended recipient;
- Information containing PHI faxed to someone other than the intended recipient;
- Email containing PHI is sent to an unauthorized person;
- Workforce member looking at the records of a relative, friend, coworker, etc., without a business need to know that information;
- Lost or stolen papers containing PHI.

Examples of potential security breaches:

- Failure to send PHI with "#SECURE#" encryption when using email;
- Lost or stolen unencrypted laptops, computers, servers, tapes, CD ROMs, flash drives, phones, PDAs and any other mobile data-storage medium containing PHI;
- Theft or misuse of Company information or assets;
- Misuse, intrusion or attacks against Companies electronic networks and computers.

Knowledge Management System (KMS):
Is a tool used by the Call Center Representatives and houses what are called "scenarios". Each scenario provides guidelines on what information is needed from the caller and what information is allowed to be disclosed.

Non-Event:
Disclosure was permitted by HIPAA and other applicable privacy laws or investigation immediately revealed that no disclosure occurred. These cases are still worked and tracked.

Protected Health Information (PHI):
Any information, including demographic information, that is created or received by a covered entity and relates to:

a) The past, present or future physical or mental health or condition of an individual;
b) The provision of health care to an individual;
c) The past, present or future payment for the provision of health care to an individual;

And that identifies the individual for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information concerning persons living or deceased (less than 50 years) and may be written, oral or electronic.

Substantiated:
Unable to disprove that Company caused a disclosure of protected health information (PHI).

Suspected Breach:
An incident where there is a reasonable likelihood that PHI was inappropriately acquired, accessed, used or disclosed.

Unsubstantiated:
Proven that Company did not cause a disclosure of protected health information (PHI).

Unsecured PHI:
PHI that is not encrypted or destroyed in a manner that makes the PHI unreadable to unauthorized individuals.

Workforce Member:
Employees (caregivers), volunteers, trainees, medical staff and other persons under the direct control of Company whether or not they are paid by the Company. This may also include independent contractors, depending upon the arrangement.

PROCEDURE:
Any workforce member who learns of, or whose actions result in or contribute to a suspected breach is required to immediately report the suspected breach using one of the following methods:

- Via the Privacy and Security Concern Form
- To your immediate supervisor
- To your department's Manager/Director
- To the Chief Compliance, Privacy and Risk Officer/Privacy Officer at x46562
- To the 24/7 Integrity Line at 888-294-8455. This option can be used if an event occurs after normal business hours and/or you would prefer to report anonymously.

Each of these reporting options shall result in a Privacy and Security Concern Form being submitted, either by the workforce member, the supervisor, manager or director or by Privacy Program workforce members. Workforce member shall not delay this reporting for any reason (e.g. do not conduct a full assessment or evaluation of incident prior to reporting).

Business Associates must report breaches according to the Business Associates' contract and Business Associate Agreement requirements. Business Associate will report a suspected breach immediately via the phone number (877-512-7119) listed in the Business Associate Agreement signed by the vendor. Once Company has been notified, the Company business contact will report using the Privacy and Security Concern form. Once reported, all suspected breaches will be managed pursuant to the process outlined in this policy. The Regulatory Compliance, Risk Management and Government Affairs Privacy Program will be the responsible department in conducting the investigation.

Upon receipt of a report of a suspected breach, workforce members shall complete a Privacy and Security Concern Form. This form is located online at the Regulatory Compliance, Risk Management and Government Affairs department homepage. Once submitted the form will automatically be sent to the following points of contact:

- Chief Compliance, Risk Officer and Privacy Officer
- Privacy Program Manager
- Senior Privacy Coordinator

If the suspected breach is a potential security breach, Privacy Program workforce members will forward the completed form to the Chief Information Officer (CIO) or designee.

CONDUCTING AN INVESTIGATION:
Upon receipt of the Privacy and Security Concern Form, Privacy Program workforce members will begin an investigation into the suspected breach.

If Privacy Program workforce members determine that the potential breach is an actual breach, the investigation will be documented in the incident management software tool that is used to log and work all privacy casework across the organization in a centralized database. The tool is called EthicsPoint., All case documentation will include a detailed summary (substantiated or unsubstantiated) of what happened, PHI that was disclosed, root cause analysis, a risk assessment that evaluates the probability of compromise, all corresponding/supporting documents that are identified as part of the case. A completed Accounting of Disclosure and if appropriate and/or possible, mitigation and corrective action taken. All efforts will be made to resolve an investigation within sixty (60) days of receipt of the Privacy and Security Concern Form.

If Privacy Program workforce members determine that a suspected breach is not an actual breach, it will be classified as a Non-Event. Non-Events include those suspected breaches are excepted in the definition of breach, or that are in fact permitted by HIPAA and other applicable privacy laws and that fall within the Health Plan's normal operating guidelines, such that no further action is required. Non-Events will investigated and documented in a spreadsheet that contains basic details and describes why the potential breach was classified as a Non-Event.

Investigation can include, but is not limited to, the following:
- Coordination with the Business Associates, departments and workforce members involved in the case;
- Interviews of workforce members and/or affected members as appropriate;
- Audit of workforce member(s) communications as appropriate;
- Review of recorded calls if available;
- Retrieval of PHI disclosed in error and/or a verbal statement from unintended recipient that the PHI has been destroyed and will not be retained, used, or further disclosed;
- Informal and formal Risk Assessments to determine the level of risk a potential breach poses.

<u>Probability of Compromise Analysis (Risk Assessment)</u>
All reported potential breaches will be evaluated by performing a Risk Assessment that establishes the level of probability of compromise of the PHI involved. The assessment must be thorough, completed in good faith and reach conclusions that are reasonable. To meet these requirements, the risk assessment must consider at least:
- The nature and extent of the PHI involved (i.e., types of identifiers, likelihood of re-identification, and the amount of data and its sensitivity);
- The unauthorized person to whom the data was disclosed;

- Whether the PHI was actually acquired or viewed;
- The extent to which the risk has been mitigated.

Examples of high risk cases include, but are not limited to, exposures of PHI that:

- Put an individual in danger
- Have a likelihood of causing harm to an individual
- Require media notification

To perform the analysis, Privacy Program workforce members will use the Risk Assessment Toolkit provided by the Risk and Integrity Services department to determine the level of probability of compromise by answering questions with a numerical score as outlined on the tool. Privacy Program workforce member may choose to notify members at any score. If the score is 15 or higher, member notification is required.

Corrective Action Plan

Privacy Program workforce members will work with the manager of the department involved with or responsible for any part of the breach. Privacy Program workforce members and department manager will, if possible, identify the root cause, determine any mitigation action that may be necessary, and develop a corrective action plan to address. (Refer to PROV-HR-422 Corrective Actions- Integrity, Compliance, Privacy or Security Policy) Manager will retain a copy of any documentation of any corrective actions taken with their workforce members.

Mitigation

Where an actual Privacy or Security Breach has occurred, attempts will be made to retrieve PHI that is disclosed in error or to receive a verbal statement that the unintended recipient will not keep, use or share the PHI and that it has been destroyed/shredded/deleted and not used or further disclosed. Other mitigation steps, such as offering affected members credit-monitoring services, will be taken when appropriate.

Notification

If notification is required, notification to members, state agencies, media and the Secretary of Health and Human Services through the Office for Civil Rights will be made in accordance with the applicable reporting requirements and timelines. Privacy Program workforce members shall, when required:

- Notify affected members in writing; no later than 60 calendar days after discovery of a breach.
- Company will notify the Secretary of Health and Human Services through the Office for Civil Rights by visiting the HHS web site and filling out and electronically submitting a breach report form.
    - If a breach affects 500 or more individuals, Company will notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

  - If, a breach affects fewer than 500 individuals, Company may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.
  - Company has made a business decision to notify the secretary as soon as possible and before the case is closed.
- Notify state agencies;
- Inform and support Companies Director of External Communications in notifying the media;
- Inform and support business relationship owner in notifying the Covered Entity according to contractual obligations where Companies are the Business Associate in a relationship;
- Notify any other required entities or persons as state law or contractual obligates may dictate.

Exception to notification timelines:
If a law enforcement official states to Company or its Business Associate(s) that notification would impede a criminal investigation or cause damage to national security, Company and its Business Associates shall document the statement and delay notification until the time period specified by the official or, if no timeline was stated by the official, no later than thirty (30) days from the date of the statement.

Reporting and Investigation requirements for Medicare:
Company Medicare Advantage Plans

- Privacy Program workforce members shall notify Medicare Compliance workforce members immediately if a potential breach is determined, through an informal Risk Assessment, to potentially be of high risk.
- Medicare Compliance Officer or their designee will immediately report (i.e. not wait until the mandatory reporting date to the Secretary of HHS) any breaches to the Regional Office Account Manager if there is the potential for significant beneficiary harm (i.e. a high likelihood that the information was or could be used inappropriately) or situations that may have heightened public or media scrutiny (i.e. a higher number of beneficiaries affected or particularly egregious breaches).
- Medicare Compliance Officer or their designee will provide concurrent notification of any breaches submitted to the Secretary to the Regional Office Account Manager. Notification to the Regional Office Account Manager will include the same information that was submitted in the electronic submission to the Secretary.
- Company shall take immediate remedial steps to protect Medicare Advantage Plans members when breaches occur. These steps will be communicated to the Regional Office Account Manager by the Chief Compliance and Risk Officer and/or the Medicare Compliance Officer.
- Company shall comply with direction given by the Secretary and Regional Office Account Manager as applicable to a breach.

Reporting and Investigation requirements for Health Share of Oregon (Medicaid):
Health Share of Oregon Coordinated Care Organization (Health Share)

- Privacy Program workforce members shall notify Health Share and Company Health Share business relationship owner of actual breaches as soon as reasonably possible but in no event more than (60) days after discovering the breach using the following contact information:

Email: Barbara@healthshareoregon.org
Hotline phone: (503) 416-1459
Fax: (503) 459-5749

Address:
Health Share of Oregon
2121 SW Broadway Suite 200
Portland, OR 97201

- Notification shall include, if known, the identities of affected Health Share members, the date of the breach, the scope of the breach and a description of Companies response to the breach.
- Health Share shall make final determinations regarding required notifications. Privacy Program workforce members shall support Health Share should notification be deemed necessary.
- Company shall, in consultation with Health Share, mitigate, to the extent practicable, any harmful effect of a breach affecting Health Share members.

REFERENCES:
CFR 164.400-414 Breach Notification Rule
PSJH-RIS-850 General Privacy Policy
PROV-HR-422 Corrective Actions- Integrity, Compliance, Privacy, or Security Policy
Knowledge Management System (Confidentiality and Privacy)
Office for Civil Rights Breach Portal
Privacy and Security Concern Form
State Data Breach Notification laws
Incident Response and Reporting Plan