Privacy and Security Employee Training

The following confidential and proprietary training materials are the property of CVS Health. Training materials, including but not limited to, the training assessment (questions and answers), should not be copied, reproduced, or shared with external parties without proper approval.

If you're using a screen reader and unable to go through the course to complete the course and receive completion credit, email the SO Learning Support mailbox. Include in the email the course name, course number and completion date.

Introduction

Welcome

Welcome to the Aetna Better Health® of Oklahoma training course for reporting privacy and security incidents. This training is mandatory for all Aetna Better Health of Oklahoma employees and contractors.

Member and customer data are at the heart of Aetna's business. We use data to drive decision-making and enhance our member care. A good steward of member and client data is critical to our business. We inspire trust by protecting data as if it were our own and following privacy and security practices daily.

Objectives

At the end of this training, Aetna Better Health of Oklahoma employees will:

- Identify how and when you report privacy and security incidents
- Recall the penalty for failure to comply with the contract reporting timeline
- Identify the anonymous reporting option for privacy and security incidents
- Differentiate between the Privacy Incident report and the Security Incident report
- Describe the types of incidents that must be reported

Agenda

- HIPAA basics
- Employee responsibilities safeguarding protected health information (PHI)

- What to report
- Privacy and security incident reporting contract requirements
- When and how to report incidents
- Next steps

Privacy and Security Basics

Privacy Matters!

Let’s talk for a moment about why privacy matters. We must look at the underlying risks to individuals, business areas and the enterprise to do that.

Privacy Risks

- For our members, several risks can occur. Identity theft, unintentional disclosures and medical fraud could lead to personal embarrassment, employment issues and reputational harm. Identity theft could also lead to financial implications.
- **Business**: Business areas found to be responsible for privacy incidents are responsible for fully assisting the Privacy Office in the investigation and documentation of the issue and its resolution. This may include:
  - Dedicating resources to assist with the investigation
  - Financial implications to business such as paying for credit monitoring services, providing dedicated phone and personnel or other associated costs (e.g., cost of lost/stolen packages and reshipping)
  - Consulting with the Privacy Office to develop corrective action plans to resolve issues or gaps identified and minimize the risk of similar incidents
- **Aetna/CVS Health**: Our reputation is essential. Members put their trust in us, and when we fail to protect their personal information, that trust is eroded. This can harm Aetna’s reputation and negatively impact our business. If you think about some large companies where your data may have been compromised, you know how it made you feel when notified of a breach. We always strive to be a company that earns the trust placed in us by our members.

Health Insurance Portability and Accountability Act (HIPAA) Basics

Before understanding how to report privacy and security incidents, let's review the basics of the HIPAA Privacy and Security Rule.

HIPAA was signed into law in 1996.

The Privacy Rule was established in 2003 and regulates how protected health information is used and disclosed. Additionally, the Privacy Rule establishes individual rights related to protected health information, also known as PHI.

The Security Rule was established in 2005 and relates to how PHI is used and disclosed in an electronic format.

HIPAA applies to

HIPAA applies to several different types of entities and customers.

Covered entities must comply with HIPAA's Privacy Rule, Security Rule and Breach Notification Rule which establish national standards for protecting the privacy and security of PHI. Compliance includes implementing safeguards to ensure the confidentiality, integrity and availability of PHI. It provides individuals with certain rights regarding their health information.

There are three main types of covered entities under HIPAA.

- Health plans
- Health care providers
- Health care clearinghouses

Health plans include:

- Health insurance companies
- Health maintenance organizations (HMOs)
- Employer-sponsored health plans
- Government programs like Medicare and Medicaid
- Other types of health benefit plans like veteran and military health plans

Health care providers include:

- Doctors
- Clinics

- Hospitals
- Nursing homes
- Pharmacies
- Other healthcare professionals or institutions

Information is electronically transmitted in connection with transactions for which the United States Department of Health and Human Services (HHS) has adopted standards.

Health care clearinghouses are entities that process nonstandard health information they receive from another entity into a standard format or vice versa. They might include billing services or entities that facilitate the processing of healthcare transactions.

A business associate, under HIPAA, refers to a person or entity performing certain functions or activities on behalf of a covered entity or providing certain services. Their functions involve using or disclosing PHI.

Examples of business associates may include:

- Vendors
- Third-party administrators
- Medical billing companies
- Legal, accreditation or financial services firms
- Health information organizations

Examples of the functions they perform may include:

- Printing
- Mailing
- Communications
- Claim payment
- Medical management

Defining PII and PHI

What is PII?

Personally Identifiable Information, or PII, is a non-HIPAA term used in the context of state law definitions. It’s information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual. Let’s look at some examples.

- Name
- Address
- Date of birth
- Gender
- Social Security number
- Photo
- Driver’s license
- Biometric information
- Account information

What is PHI?

PHI is information that identifies an individual and relates to any aspect of their physical or mental health. It’s PII plus a health component.

However, a note to make here is that we protect it the same regardless of whether information is considered PHI or PII.

Let’s look at some examples.

- Claim number
- Diagnosis description
- Procedure code
- Health ID/health insurance claim number (HICN)
- Provider name
- Case notes
- Claim amount paid
- Insurance status
- Prescription

When in doubt, ask Kristin Eeg, the privacy officer.

Here are a few examples of PII and PHI.

- An e-mail discussing J. Smith and a provider, Dr. Peterson, about a broken ankle.

  - The information *Smith* and *broken ankle* is neither PII nor PHI because you could not identify a specific person with this information alone.

- An e-mail discussing J. L. Smith, DOB 10/27/1989, male, residing at 123 Mail Street, Cheyenne, WY.
  - This one is PII because it's not related to health information.

- An e-mail discussing Joseph L. Smith, DOB 10/27/1989, residing at 123 Mail Street, Cheyenne, WY, about the claim status with provider Dr. Janice Peterson of Peterson Orthopedics regarding his broken ankle.
  - The information Joseph L. Smith, DOB 10/27/1989, 123 Main Street, Cheyenne WY, who consulted with Dr. Janice Peterson of Peterson Orthopedics about his broken ankle, is PHI.

How You Can Help

The Minimum Necessary Rule

The **minimum necessary rule** under HIPAA is a crucial privacy provision designed to protect the confidentiality of individuals' health information while allowing for the necessary flow of information for healthcare purposes. The rule helps balance safeguarding individual privacy rights and facilitating necessary healthcare activities. Limiting the unnecessary disclosure of sensitive health information aims to enhance patient trust and confidentiality in the healthcare system.

We use role-based access models to prevent employees from accessing areas of the system for which they lack authorization. Your access is based on your role.

You will apply the **minimum necessary rule** when disclosing PHI.

Respect privacy! Employees are authorized to access PHI solely based on business necessity.

No Snooping!

Protecting PHI – Employee Responsibilities

Every employee is responsible for safeguarding PHI, ensuring it remains secure and inaccessible to unauthorized individuals.

Familiarize yourself with all relevant Privacy and Security policies and procedures concerning using, disclosing and safeguarding PHI.

You should be aware of Oklahoma specific laws that might be applicable to your job. Based on your role, it's important to understand Federal and Oklahoma specific laws pertaining to privacy. You can reach out to the Oklahoma Privacy and Security Officer at 918-949-8354 or privacyaetna@aetna.com for more information.

Not Sure? - Report it!

What to Report? Example of Incidents

Let's examine a few instances that necessitate reporting.

Privacy incidents include any form of communication, written, electronic or verbal that involves PHI and leads to an unauthorized use or disclosure. Consider your daily interactions with PHI, whether it's transmitted via fax, mail, email or over the phone. Is it protected?

Examples:

- Fax
- US mail
- Web Intake forms
- Email
- Phone
- Oral discussions about PHI without **need to know**

Security incidents pertain exclusively to electronic information. They encompass any unauthorized attempt, whether successful or unsuccessful, to compromise the confidentiality and integrity of our member data and organizational systems.

Examples:

- Unauthorized access to data
- Malware attack (ransomware)
- Phishing
- Hacking
- Breaches of member or provider portals

- Incidents involving Lost or stolen company-owned devices such as laptops, cell phones, etc.

Oklahoma Health Care Authority: Privacy and Security Incident Reporting Contract Requirements

Immediate Privacy and Security Incident Reporting Protocol

- Unauthorized Acts
- Any Unauthorized Use or Disclosure of PHI
- Any Security Incident

As part of our partnership with the Oklahoma Health Care Authority, we must adhere to the stringent contractual obligations outlined in section 1.2.16.3 of the contract concerning reporting privacy and security incidents. Failure to meet these requirements can result in significant penalties, including potential fines of up to $2,500 for each instance of non-compliance.

Notification Timeframe

You must notify the Oklahoma Health Care Authority within one hour of discovering any incident. This means our dedicated Oklahoma Privacy and Security Officer must swiftly initiate the notification process to ensure compliance with this contractual obligation.

Your Role

Each team member plays a vital role in maintaining compliance with these reporting requirements. If you become aware of any incident falling within the scope outlined above, or if you are not sure it falls within your scope, you must report it immediately to the Oklahoma Privacy and Security Officer. Time is of the essence in these situations, and prompt action is essential to lessen potential risks and uphold our contractual obligations.

Support and Assistance

Should you require any assistance or clarification regarding incident reporting procedures, please do not hesitate to contact our dedicated Oklahoma Privacy and Security Officer at 918-949-8354 or privacyaetna@aetna.com. We are here to support you in fulfilling our obligations and safeguarding the integrity and security of our operations.

Ways to Report Privacy and Security Incidents

Privacy Incident Report Form-Preferred Method

Employees have various channels available to promptly report privacy and security incidents. Let's explore the immediate reporting options.

We highly recommend utilizing the Privacy Incident Report Form as the preferred and quickest method for reporting incidents. You can access this form via the Privacy Incident Form or by visiting the organization's Heartbeat page. The form is accessible from inside and outside the organization. Therefore, you can report incidents anytime and from any computer with Internet access.

The form guides you through a series of questions. While you may only have some of the information, complete as much of the form as possible.

Open the Privacy Incident Form. The reporter completes all required fields and submits the form. The form includes these fields.

- Reporter name, phone and email
- Date incident occurred (when it happened)
- Date of discovery (when we found out)
- How many impacted individuals
- Brief description
- Responsible department
- Recipient information (who received the data)
- Impacted member(s)
- Member/participant covered under one of the following: select OK Medicaid

It's important to select **OK Medicaid** as the impacted entity so the form will route to the dedicated Oklahoma Privacy Officer.

After selecting the **OK Medicaid** option, complete and submit the form. Upon submission, an automatic email will notify the Oklahoma Privacy Officer of the newly logged incident. This step is critical for meeting contractual obligations with the Oklahoma Health Care Authority.

Other fields to be completed by the receiver of the form:

- Action performed by the receiver (i.e., returned or destroyed data)
- Root cause (i.e., fax, mail, portal and email)
- PII/PHI included

We appreciate your cooperation in promptly reporting incidents which contribute to maintaining compliance with regulatory and contractual agreements.

Security Incident Report Form

To ensure thorough reporting of security incidents, we also provide a dedicated Security Incident Report Form, or the organization's Heartbeat page. The steps:

1. Visit Security Incident Report Form
2. If you get the Archer window, select Login.
3. From the Home page that displays, visit the Report Security Incident quick link at the top of the page.

Another way to find the report form is from the Heartbeat page. You can scroll to the bottom of the page, under report concerns or issues, visit the:

- Report a Compliance or Ethics issue
- Report a Privacy issue
- Report Information Security issue

The Security Incident Report form is exclusively for internal use.

The form guides you through a series of questions to gather pertinent details about the incident.

Fields to complete in the form:

- Impacted Region
- Incident Category
- Response Urgency
  - Select High immediate response
- Primary Contact
- Facts
  - Add Oklahoma Medicaid
  - No SSN, PHI, password or other restricted data

- Add attachment (if applicable)
- Save and Close

You must add **Oklahoma Medicaid** to the Fact's section.

You shouldn't enter sensitive data, such as social security numbers, passwords, PHI or other restricted data, directly into the Security Incident Report Form.

After completing the Security Incident Form, submit a Privacy Incident Form. Open the Privacy Incident Form and review it.

Reasons you must also complete the Privacy Incident Form:

- Incident details need to be captured in both systems.
- The Oklahoma Medicaid designation needs to trigger an email to the privacy and security officer.
- Mark **Security Incident** when filling out the Privacy Incident Form.

You can provide the security incident number. Once submitted, an immediate email is sent to the privacy and security officer.

Ethics Line Report Form – Only if Anonymous

We provide a confidential and secure means for employees to report privacy and security incidents through our Ethics Line anonymously. You should only use this option if you want to remain anonymous.

This service is managed by a trusted third-party administrator, ensuring employees can report concerns safely and confidentially.

You can access the Ethics Line via the provided link or by visiting the organization's Heartbeat page. It's accessible within and outside the organization. You can report incidents anytime and from any computer with Internet access.

The form will guide you through a series of questions to gather pertinent details about the incident.

To complete the form, enter:

- Business unit
- Country
- State-Oklahoma

- City
- Check I Agree
- Save and Close

It's crucial to emphasize that while the Ethics Line Report Form provides an anonymous option for reporting privacy and security-related matters, the information required by the Oklahoma privacy officer, as outlined in the Privacy Incident Report Form, remains vital. Even when choosing to report anonymously, we strongly encourage employees to gather as much relevant information as possible and include it in their Ethics Line Report.

Call or Email Incident Reporting

We provide additional avenues for reporting privacy and security incidents if you opt not to use the provided links or Heartbeat page. You can directly contact the dedicated Oklahoma privacy officer via phone or email. You can also contact the Security Operations Center (SOC) team.

We offer a phone and email option through our organizational Ethics Line for anonymous reporting. The Ethics Line also provides a teletypewriter (TTY) option for people who are deaf, hard-of-hearing or have severe speech impairment.

If using any of the email options available, you must include **Oklahoma Medicaid** in the subject line.

You should have the necessary information outlined in the Privacy Incident Report Form readily available or be prepared to provide it promptly if the privacy officer contacts you. (note to QA reviewer, the email addresses aren't active yet.)

Privacy

Phone: 918-949-8354 (Kristin Eeg)

Email: privacyaetna@aetna.com

Security

Phone: 401-770-3111

Email: SOC@CVSHealth.com

Ethics Line

Phone: 1-877-CVS-2040 (1-877-287-2040); TTY: 711

Email: Ethics.BusinessConduct@CVSHealth.com

Next Steps

Next Steps

- Share privacy and security expectations with your staff.
- Reporting Privacy and Security Incidents training begins April 2024
- Download the Reporting Privacy and Security Incidents handout. Once downloaded, thoroughly review its contents, paying particular attention to the contractual reporting requirements. It's imperative to retain a copy of the Reporting Privacy and Security Incidents handout for prompt incident reporting.

To successfully complete the course, acknowledge that you have downloaded, reviewed and saved a copy of the Reporting Privacy and Security Incidents handout.

Open and download the Reporting Privacy and Security Incidents handout.

In Closing

- Always protect member and client data.
- Stay up to date with privacy and security practices and procedures.
- Complete required training.
- Keep the Privacy and Security Incident Reporting handout.
- Report incidents immediately.

Resources

There are resources available to provide more information about privacy and security. You can save them to your Favorites folder. The resources include:

Privacy Office

Policy and Procedure Portal

Oklahoma Statute Title 63

Privacy and Security Reporting Infographic

Mastery Test

The transcript doesn’t include the mastery test for this course. If you’re using a screen reader and unable to go through the course to complete the mastery test and receive completion credit, email the SO Learning Support mailbox. Include in the email the course name, course number and completion date.

Course Information