The Commonwealth of Kentucky
Presumptive Eligibility Program

Presumptive Eligibility Privacy and Security Training Guide

Document Control Information

Document Information

Document Name	Kentucky Presumptive Eligibility Privacy and Security Training Guide
Project Name	Kentucky Health Benefit Exchange
Client	Kentucky Cabinet for Health and Family Services
Document Version	1.0

Document Edit History

Version	Date	Additions/Modifications
1.0	March 31, 2025	Final Submission

Table of Contents

1. Introduction

Hello, and Welcome to Module 4 on Kentucky Presumptive Eligibility. In this course, we will focus on the rules regarding handling of information and best practices regarding Privacy and Security. When you are ready to begin, press the Start Button below.

2. Course Overview

In this course, we will be covering a number of topics, including:

- The Health Insurance Portability and Accountability Act, referred to as HIPAA
- Guidelines for Protected Health Information (PHI) and Personally Identifiable Information (PII)
- The handling of Security Incidents
- Violation and penalties for mishandling of protected information

Click next when you are ready to proceed.

2.1 Privacy and Security Policy

This module reviews Privacy and Security policies and best practices when working with Residents applying for Presumptive Eligibility. It is of the utmost importance to always abide by the Department for Medicaid Services' Privacy and Security policies when handling Residents' personal information.

- While performing Presumptive Eligibility Determiner duties, PE Determiners are exposed to sensitive client information, or Personally Identifiable Information (PII).
- PE Determiners must handle PII carefully and should not leave it in public places or areas where others may be able to access it. When discarding PII, PE Determiners should use a shredder, not a trash can or recycling bin.

Please Note: There are serious legal and personal consequences for violating Privacy and Security laws. It is important that PE Determiners understand the principal Federal guidelines in addition to the policies of DMS.

3. HIPAA

Let's take a look at the guidelines of the Health Insurance Portability and Accountability Act, commonly referred to as HIPAA

Click next when you are ready to begin.

3.1 HIPAA Overview

PE Determiners should be aware of the Health Insurance Portability and Accountability Act. Established in 1996, HIPAA is a federal law that aims to:

- Make it easier for Residents to keep health insurance.
- Protect the confidentiality and security of health care information
- Help the health care industry control administrative costs.

3.2 HIPAA Regulation

HIPAA is comprised of various rules and regulations, which apply to covered entities and their business associates.

- Residents, organizations, and agencies that meet the definition of a covered entity must comply with HIPAA's requirements to protect individually identifiable health information and provide patients with certain rights pertaining to that information.
- If a covered entity works with a business associate, the entity must have a contract or other arrangement with the business associate that establishes specifically what they will do.
- The contract should establish requirements for the business associate to comply with, including the rules for protecting the Privacy and Security of protected health information.

3.1 HIPAA Rules and Standards

It is important that PE Determiners are aware of specific HIPAA rules and standards that impact their day-to-day work life.

These rules are:

- The Privacy Rule
- The Security Rule
- The Enforcement Rule
- The Incident Notification Rule.

Click on the Privacy Rule button below to learn more.

3.1.1 Privacy Rule

The HIPAA Privacy Rule sets national standards to protect individuals' health information (PHI) by limiting how and when 'covered entities' and their business associates can use or disclose it without authorization. The rule outlines specific situations where PHI can be used or disclosed without patient authorization, such as for treatment, payment, and healthcare operations. Covered entities and business associates are generally required to take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.

Click on the Security Rule button to proceed.

3.1.2 Security Rule

The Security Rule establishes national standards to protect residents' electronic personal health information that is created, received, used, or maintained by a covered entity. Also required, is appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Click on the Enforcement Rule button to proceed.

3.1.3 The Enforcement Rule

The Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil penalties for violation of the HIPAA Administrative Simplification Rules, and procedures for hearings.

Click on the Incident Notification Rule button to proceed.

3.1.4 The Incident Notification Rule

The Incident Notification Rule requires HIPAA covered entities and their business associates to provide notification following an incident of unsecured protected health information. Similar to incident notification provisions implemented and enforced by the Federal Trade Commission (FTC), this applies to vendors of personal health records and their third-party service providers.

Click the Next button to proceed.

3.2 HIPAA Standards

Now let's take a look at some of the standards of HIPAA.

3.2.1 Transaction and Code Set Standards

The Transactions and Code Set Standards creates a uniform way to perform Electronic Data Interchange (EDI) transactions for submitting, processing, and paying claims.

3.2.2 Employer Identifier Standard

The Employer Identifier Standard requires employers to have standard national numbers that identify them on transactions. The Employer Identification Number (EIN) is the identifier for employers and is issued by the Internal Revenue Service.

3.2.3 National Provider Identifier (NPI) Standard

The National Provider Identifier (NPI) Standard is a unique 10-digit identification number for health care providers.

Health care providers and all health plans and health care clearinghouses must use NPIs in the administrative and financial transactions adopted under HIPAA.

Please Note: If covered entities and their business associates do not follow the HIPAA rules and regulations, they are directly liable and can face severe penalties for the release of that information.

4. PHI and PII

Let's look at some of the rules for PE Determiners regarding the handling of PII.

Kentucky's policies and procedures are based on the guidelines set forth by the Federal government.

It is of the utmost importance that Determiners be aware of the Privacy and Security policies for handling Residents' personal information.

While performing PE Determiner duties, determiners will likely be exposed to sensitive client data.

PE Determiners must handle PII carefully and should not leave it in public places or areas where others may be able to access it.

4.1 Handling of PII

It is critical for PE Determiners to follow proper handling requirements to protect PII. Listed below are some tips PE Determiners should utilize when handing PII.

PE Determiners must follow the below requirements at all times when working with PII:

- Papers or copies containing PII must never be left unsecured or in public places.
- When discarding PII, PE Determiners must use a shredder, not a trash can or recycling bin.
- PE Determiners must use a password protected computer
- PE Determiners must lock their computers when they are away from the screen.
- Determiners should never repeat PII aloud if others are nearby or could hear over a phone call.

- Finally, PII is never to be shared unless there is a legitimate business need.

4.2 Protected Health Information

Now let's look at what qualifies as Protected Health Information or (PHI)

The purpose of the HIPAA Privacy Rule is to protect Individually Identifiable Health Information.

This information is also known as Protected Health Information and is a subset of Personally Identifiable Information. For information to be considered PHI, it must meet all of the following conditions:

- The information is created, received, or maintained by a health provider or health plan.
- The information is related to past, present, or future health care or payment for that health care.
- The information identifies a Resident, or there is enough information to be able to identify the Resident.

4.3 PHI Identifiers

PHI is a subset of Personally Identifiable Information (PII). PHI is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium.

PHI includes the following 16 identifiers:

- **Name:**
    - This includes first name, last name, and maiden name combinations.
        - It could be possible to identify a Resident using a combination of data - e.g., first name, zip code, street address, etc.
- **Date:**
    - This includes the dates of significant events in a Resident's life including:
        - Birth
        - Death
        - Marriage
        - hospital admissions
        - discharges
- **Geographic Locators:**
    - This includes street address, city, precinct, zip code, latitude and longitude coordinates, etc.
- **Phone Numbers:**
    - This includes personal, work, other mobile or land line numbers linked to a Resident.

- **Fax Numbers and Email:**
    - This includes personal, work, and other email addresses and fax numbers linked to a Resident.
- **Social Security Number:**
    - A 9-digit number that links a Resident to their Social Security.
- **Medical Record Numbers:**
    - Medical record numbers can be used to identify a Resident, if one also knows the institution that assigned the number.
- **Health Plan Beneficiary Numbers:**
    - This includes things like an insurance card or member ID.
- **Certificate and License Numbers:**
    - This includes driver's license numbers and birth certificate numbers.
- **Account Numbers:**
    - This includes specific bank account numbers, etc.
- **Vehicle Information:**
    - This includes any vehicle characteristic that can help locate a Resident, including vehicle identifiers such as serial and license plate numbers.
- **Device Identifiers:**
    - This includes identifiers for devices such as serial numbers for medical devices and personal electronics.
- **Web Universal Resource Locators:**
    - (URLs) Technology can now track Residents' locations and identities based on browser history and website visits.
- **Internet Protocol (IP) Address Numbers**:
    - Similar to URLs, an IP Address is a unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.
- **Biometric Identifiers**:
    - This includes biometric identifiers such as:
        - Fingerprints,
        - Voice Prints,
        - and Retinal images
- **Photographic Images:**
    - This includes full face or comparable images and other visual images that could be used to identify a Resdident.

Kentucky Revised Statute (KRS) 61.931, further clarifies Personal Information to be one of the following:

- First name and last name
- first initial, and last name
- Personal mark
- Unique biometric information

- or a Genetic print or image when used in combination with one or more of the following data elements:
    - An account number
    - Credit card number or debit card number with required security or access code or password that grants access to the account
    - Social Security Number
    - Taxpayer identification number
    - Driver's license number
    - Any Other Unique Identifying Number, Characteristic, or Code

5. Security Incidents

Let's take a look at what a security incident is and how to handle these types of incidents. Click next when you are ready to begin.

5.1 Security Incidents

Let's discuss what a security incident is.

A security incident is:

- The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that has resulted in or is likely to result in the misuse of personal information.

If the organization has reason to believe that the records or data subject to the unauthorized access may compromise the security, confidentiality, or integrity of the personal information and has resulted in or is likely to result in the misuse of the personal information or likelihood of harm to one or more Residents, then the occurrence will be considered a security incident.

5.2 Email Security

- Email Security Awareness for PE Determiners:
    - It is best practice to emphasize the importance of clearing desks of confidential data, files, and papers at the end of the day.
- Email Security Incidents:
    - Qualified Entities of the Department for Medicaid Services (DMS) are responsible for ensuring the security of all emails sent if the email contains confidential or personal information.
- Email Details:
    - Sending both a case number and name via email is a violation of PII.
- Qualified Entities
    - Qualified Entities of DMS must use secure emails if sending confidential information.

5.3 Kentucky Online Gateway

The Kentucky Online Gateway also known as KOG, is an authentication services system for users requesting access to a variety of systems across the Commonwealth. PE Determiners must create an account in KOG in order to access kynect. Let's discuss password guidelines, Multi-Factor Authentication, and some KOG Security best practices.

Click on password guidelines to continue.

5.3.1 Password Guidelines

- A password must be at least 8 characters in length and contain at least one number, one lowercase letter, and one uppercase letter.
- Avoid using personal information, don't include things like your name, birthdate, your child's name, or anything else a person could easily guess.
- Don't reuse passwords, have a unique password for every account. This is especially important for your Determiner account so that if a personal account password is compromised, your Determiner account will be safe.
- Remember access to your account means potential access to your client's PII.

Click the Multi-Factor Authentication button to continue

5.3.2 Multi-Factor Authentication

What is Multi-Factor Authentication (MFA)?

- Multi-Factor Authentication is an authentication method that requires the user to provide two or more verification factors to gain access to an app. MFA is a core component of a strong Identity and Access Management (IAM) policy.
- As a Determiner you are required to use MFA to strengthen the security of your KOG account. There are 5 types of authenticators you may connect to your KOG account.

Please note: These options are role-based and automatically assigned by KOG, meaning that you may not see every MFA when setting up MFA on your KOG account.

You can find more information about Multi-Factor Authentication on the Facts and Resources page of the PE website.

Click the KOG Best Practices button to continue

5.3.3 KOG Best Practices

Do not create duplicate accounts when creating your KOG account for the Determiner role. If you have a KOG account for another non-citizen role you will not need to create a new one. You also may not use a citizen account for the Determiner role access.

Click the next button to proceed

6. Violations and Penalties

Let's take a look at what happens when you violate the privacy and security rules. Click next when you are ready to begin.

6.1 Civil Penalties

Penalties for Violating Privacy Rules and Procedures Determiners should be aware of the civil penalties of violating privacy rules and procedures. Details of the repercussions are listed below:

- A violation that the covered entity was unaware of and could not have realistically avoided with a reasonable amount of care results in a minimum fine of $100 per violation, up to a maximum of $25,000 per year.
- A violation that the covered entity should have been aware of by exercising reasonable diligence provokes a $1,000 fine for each violation, not exceeding $100,000 per year.
- A violation suffered as a direct result of “willful neglect”, in cases where an attempt has been made to correct the violation results in a minimum fine of $10,000, up to an annual maximum of $250,000.
- Violations due to willful neglect, not corrected, results in a minimum fine of $50,000 per violation, up to a $1.5 million fine per year.

6.2 Criminal Penalties

Determiners should also be aware of the criminal penalties that can result from violating security policy and procedures.

- Wrongful disclosure of Individually Identifiable Health Information (IIHI) can incur a maximum fine of $50,000 with up to 1 year of imprisonment.
- Wrongful disclosure of Individually Identifiable Health Information committed under false pretenses could be up to a $100,000 fine with up to 5 years of imprisonment. W
- Wrongful disclosure of Individually Identifiable Health Information committed under false pretenses with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm could be up to a $250,000 fine with up to 10 years of imprisonment.

7. Final Assessment

At the end of this training, users must complete a **final assessment** with a passing score of **80% or higher** to be certified as a **PE Organization Manager**.

Assessment Questions

1. What does the acronym HIPAA stand for?
    A. Health Insurance Portability and Accountability Act
    B. Hospital Industry Policy Affirmative Act
    C. Hospital Industry Policy Affirmative Act
    D. Health Insurance Policy Availability Act
2. Established in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a federal law that primarily aims to:
    A. Provide discounts on health care
    B. Help with daycare coverage
    C. Provide discounts for home security
    D. Make it easier for Residents to keep health insurance, protect the confidentiality and security of health care information, and help the health care industry control administrative costs
3. Which of the following describes the HIPAA Transactions and Code Set Standards?
    A. Establishes local laws to protect only Medicaid members' medical and personal records
    B. Allows health care providers to share Residents' medical records and other personal health information as they please
    C. Creates a uniform way to perform Electronic Data Interchange (EDI) transactions for submitting, processing, and paying claims
    D. Eliminates the ability for Medicare members to visit certain health care providers
4. Common examples of Personally Identifiable Information (PII) include:
    A. Local restaurants visited
    B. Favorite TV shows
    C. Name, date of birth, and telephone number
    D. Where they attended summer camp
5. The HIPAA Privacy Rule's purpose is to protect:
    A. Individually Identifiable Health Information
    B. Computers from viruses
    C. Children from bullying
    D. The police from the bad guys

6. What should PE Determiners do to discard Personally Identifiable Information (PII)?
    A. Bury the information in a no-disclosed location
    B. Shred
    C. Place information in the trash
    D. PII cannot be destroyed during the lifetime of the patient's great granddaughter
7. Determine if the following statement about privacy and security is true or false. A security incident is the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that has resulted in or is likely to result in the misuse of personal information. **(True or False)**
8. D.M.S business partners must use what type of emails when sending confidential information to D.M.S staff.
    A. Unprotected
    B. Secure
    C. Junk
    D. Spam
9. Wrongful disclosure of Individually Identifiable Health Information (IIHI) can be punished with up to 1 year of imprisonment and can incur a maximum fine of?
    A. $12,000
    B. $250
    C. $50,000
    D. $5
10. Wrongful disclosure of Individually Identifiable Health Information (IIHI) committed under false pretenses with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm could be up to a $250,000 fine with up to how many years of imprisonment?
    A. 10 years
    B. 6 months
    C. 3 years
    D. 7 years

8. Additional Information

Let's take a look at some additional information and resources that can help answer questions about security policy and rules.

Click next when you are ready to begin.

8.1 Helpful Resources

Below are some additional information and resources.

U.S. Department of Health and Human Services (HHS)

For more information on health information privacy, such as: HIPAA, Residents' Rights under HIPAA, care coordination, enforcement highlights, frequently asked questions, and more. Visit the link below: https://www.hhs.gov/hipaa/for-professionals/faq/index.html

Office for Civil Rights (OCR)

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces federal civil rights laws that protect the rights of Residents and entities from unlawful discrimination on the basis of race, color, national origin, disability, age, or sex in health and human services. Visit the link below for more information on civil rights for health care and human services. Visit https://www.hhs.gov/ocr/index.html for more information on civil rights for healthcare and human services.

D.M.S Resources

PE Determiners may email the PE Inbox at PE.Program@ky.gov for all matters related to Presumptive Eligibility. For fact sheets, training guides and more visit the PE Website link at https://khbe.ky.gov/PE/Pages/default.aspx

9. Conclusion

This training has equipped PE Determiners with essential knowledge and best practices for maintaining privacy and security. By adhering to these guidelines, we can protect sensitive information, uphold legal requirements, and ensure the trust of those we serve. For ongoing support and further information, please utilize the resources provided.