The Commonwealth of Kentucky

kynect State-Based Marketplace

Privacy and Security Training Guide

August 20, 2021

Document Control Information

Document Information

Document Name	Privacy and Security Training Guide
Project Name	Kentucky Health Benefit Exchange
Client	Kentucky Cabinet for Health and Family Services
Document Author	Deloitte Consulting
Document Version	2.0
Document Status	Final
Date Released	8/20/2021

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised by
1.0	4/23/2021	Final Submission	Deloitte Consulting
2.0	8/20/2021	Revised Submission	Deloitte Consulting

Introduction

This training explains the privacy and security of handling Residents' personal information.

Table of Contents

1 Introduction to KHBE Privacy and Security

1.1 Introduction

This module reviews Privacy and Security policies and best practices when working with Residents applying for Medicaid and Qualified Health Plans. It is of the utmost importance to always abide by KHBE's Privacy and Security policies when handling Residents' personal information.

1. While performing Agent/kynector duties, Agents and kynectors are exposed to sensitive client information, or Personally Identifiable Information (PII).
2. Agents and kynectors 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, Agents and kynectors should use a shredder, not a trash can or recycling bin.

There are serious legal and personal consequences for violating Privacy and Security laws. It is important that Agents and kynectors understand the principal Federal guidelines in addition to the policies of the Kentucky Health Benefit Exchange.

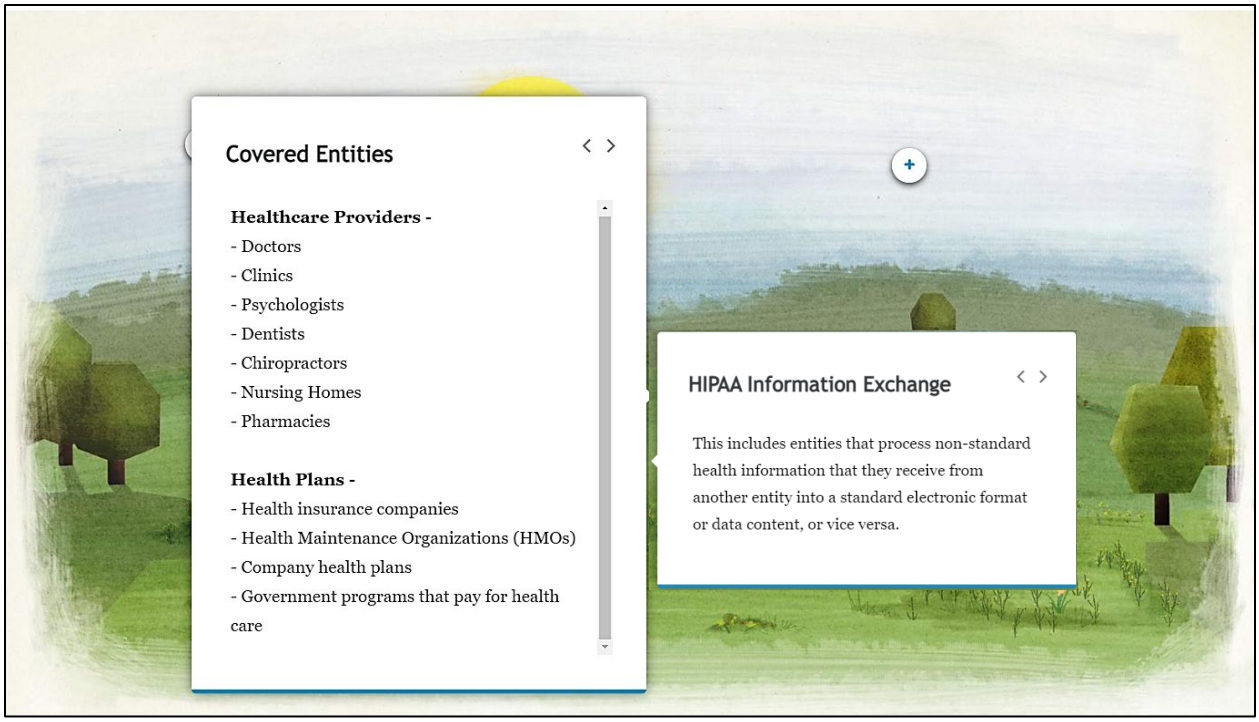
2 HIPAA Protection

Agents and kynectors should be aware of the Health Insurance Portability and Accountability Act (HIPAA). Established in 1996, HIPAA is a federal law that primarily aims to:

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

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, includes the rules’ requirements to protect the Privacy and Security of protected health information.



2.1 Protected Health Information (PHI) and Personally Identifiable Information (PII)

Personally Identifiable Information (PII): PII is defined as information which can be used to distinguish or trace a Resident's identity when it’s accessed alone, or when combined with other personal or identifying information which can be linked to a specific Resident.

Common examples of PII include the following:

- Name
- Date and Place of Birth
- Telephone Number
- Address
- Mother's Maiden Name
- Social Security Number
- Medical, Educational, Financial, and/or Employment Information
- Driver's License Number
- Email Address
- Biometric Records or Identifiers

2.2 Rules and Regulations

There are several rules and regulations that must be followed to maintain HIPAA compliance.

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

Table 1: HIPAA Rules

Rules	Description
Privacy Rule	• Establishes national standards to protect Residents' medical records and other personal health information.
Security Rule	• Establishes national standards to protect Residents' electronic personal health information that is created, received, used, or maintained by a covered entity. • Requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
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.
Incident Notification Rule	• Requires HIPAA covered entities and their business associates to provide notification following an incident of unsecured protected health information. • Similar 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.
Transactions and Code Sets Standards	• Creates a uniform way to perform Electronic Data Interchange (EDI) transactions for submitting, processing, and paying claims.
Employer Identifier Standard	• Requires employers to have standard national numbers that identify them on standard transactions. The Employer Identification Number (EIN) is the identifier for employers and is issued by the Internal Revenue Service (IRS).
National Provider Identifier (NPI) Standard	• The NPI is a unique identification, 10-digit number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use NPIs in the administrative and financial transactions adopted under HIPAA.

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

3 Protected Health Information (PHI) and Personally Identifiable Information (PII)

The HIPAA Privacy Rule's purpose is to protect Individually Identifiable Health Information (IIHI). This information is also known as Protected Health Information (PHI) and is a subset of Personally Identifiable Information (PII).

For information to be considered PHI, it must meet all of the following conditions:

3.1 Protected Health Information and PHI Identifiers

Public Health Information (PHI): 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:

Table 2: PHI Identifiers

Data Element	Description
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.
Dates	• This includes significant events in a Resident's life – birth, death, marriage, admission, discharge, etc. The year is generally considered fine for use except in the case of the

	very elderly (>89 years of age; in which case they would be represented by an aggregate category e.g.=>90).
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 Residents if one also knows the institution that assigned it.
Health Plan Beneficiary Numbers	• This includes things like an insurance card/member ID.
Certificate/License Numbers	• Driver's license, birth certificate, etc.
Account Numbers	• This includes specific bank account numbers, etc.
Vehicle Identifiers and Serial Numbers, Including License Plate	• This includes any vehicle characteristic that can help locate a Resident.
Device Identifiers and Serial Numbers	• This includes medical devices with unique serial numbers, personal electronics, etc.
Web Universal Resource Locators (URLs)	• Technology can now track Residents' locations and identities based on browser history and web site visits.
Internet Protocol (IP) Address Numbers	• Similar to above, an IP address is a unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.
Biometric Identifiers, Including Finger and Voice Prints	• Retinal images also fall into this category.

Full Face Photographic Images and Any Comparable Images	• This includes visual aids that identify a Resident.
Any other unique identifying number, characteristic, or code	• This category is a "catch-all" that corresponds to any unique features that are not explicitly listed above.

The Kentucky Revised Statutes of the Kentucky Legislature, (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
- Genetic print or image

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
- State identification card or other individual identification number issued by any agency
- Passport number
- Other identification number issued by the US government
- Individually identifiable health information as defined in 45 CFR 160.103 except for education records covered by the Family Educational Rights and Privacy Act

3.2 Agents and kynectors Handling PII

It is critical for Agents and kynectors to follow the handling requirements to protect PII. Listed below are tips Agents and kynectors should utilize when handling PII.

PII Handling Notice for Agents and kynectors
The office policies and procedures of Kentucky are based on the overarching guidelines set forth by the Federal government. It is of the utmost importance and a legal requirement to always be aware of the Privacy and Security of handling Residents' personal information. While performing agent/kynector duties, there is a high likelihood of being exposed to sensitive client information, or Personally Identifiable Information (PII). Agents and kynectors must handle PII carefully and should not leave it in public places or areas where others may be able to access it.

PII Handling Requirements for Agents and kynectors
Agents and kynectors must follow the below requirements at all times when working with PII: • Papers or copies containing PII must be left unsecured or in public places. • When discarding PII, Agents and kynectors must use a shredder, not a trash can or recycling bin. • Agents and kynectors must use a password protected computer. • Agents and kynectors must lock their computers when they are away from their screen. • Agents and kynectors never repeat PII aloud if others are nearby or could hear over a phone call. • PII is never to be shared unless there is a business need.

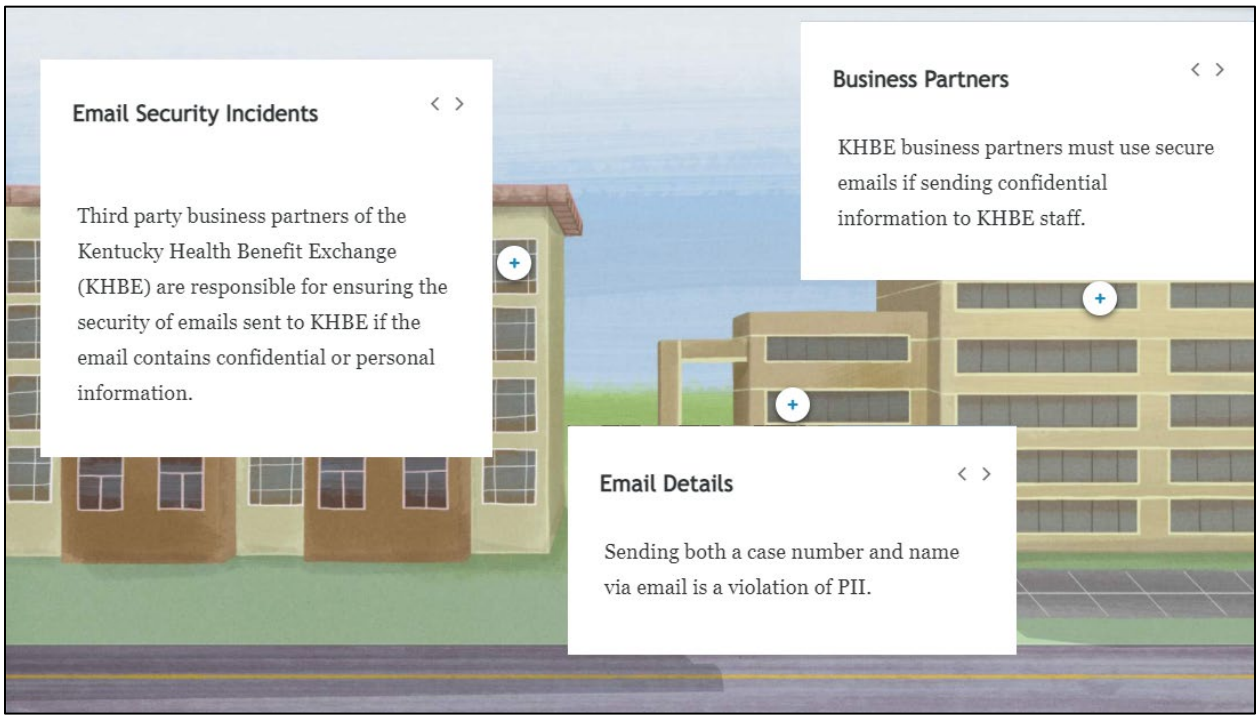
4 Security Incidents

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 agency 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.

4.1 Email Security Awareness for Agents and kynectors

See below information on email security awareness for Agents and kynectors.



5 Penalties and Violations

Agents and kynectors should be aware of the consequences of violating privacy rules and procedures.

5.1 Penalties for Violating Privacy Rules and Procedures

Details of the repercussion are listed below:

Civil Penalties
A violation that the covered entity was unaware of and could not have realistically avoided with a reasonable amount of care result 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.

Criminal Penalties

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 (IIHI) committed under false pretenses could be up to a $100,000 fine with up to 5 years of imprisonment.

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 10 years of imprisonment.

6 Additional Information and Resources

6.1 KHBE

Agents and kynectors may call the KHBE Call Center at 1 (855) 459-6328 for matters related to KHBE. Specifically, if there is a need to submit a complaint, call (502) 564-7940.

Agents and kynectors can reach the Experian Helpdesk at 1 (866) 578-5409 for additional help and troubleshooting with identity proofing information through KOG.

6.2 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 https://www.hhs.gov/ocr/index.html for more information on civil rights for health care and human services. U.S. Department of Health and Human Services (HHS)

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

The U.S. Department of Health and Human Services (HHS) aims to improve the health, safety, and well-being of America.

Visit https://www.hhs.gov/hipaa/index.html for more information on health information privacy, such as: HIPAA and COVID-19, Residents' Rights under HIPAA, care coordination, enforcement highlights, frequently asked questions, and more.

7 Assessment

1. Established in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a federal law that primarily aims to:
   a. 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
   b. Provide discounts on health care
   c. Help with daycare coverage
   d. Provide discounts for home security

2. What does the acronym HIPAA stand for?
   a. Health Insurance Portability and Accountability Act
   b. Hospital Industry Policy Affirmative Act
   c. Hospital Insurance Profitability and Affordability Act
   d. Health Insurance Policy Availability Act

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 bad guys

6. What should Agents and kynectors do to discard Personally Identifiable Information (PII)?
   a. Bury the information in a non-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. In this module, we learned that a security incident is:
   a. When someone trespasses through a restricted area
   b. 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
   c. When Residents hack their neighbor's cable subscription
   d. Something that only happens in James Bond movies

8. KHBE business partners must use _____ emails if sending confidential information to KHBE staff.
   a. Unprotected
   b. Spam
   c. Junk
   d. Secure

9. Wrongful disclosure of Individually Identifiable Health Information (IIHI) can incur a maximum fine of ____ with up to a 1 year of imprisonment.
   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 _____ of imprisonment.
    a. 10 years
    b. 6 months
    c. 3 years
    d. 7 years