The Commonwealth of Kentucky

kynect State-Based Marketplace

Privacy and Security Certification Training Guide

May 8, 2026

Document Control Information

Document Information

Document Name	Privacy and Security Certification Training Guide
Project Name	kynect State-Based Marketplace (SBM)
Client	Kentucky Cabinet for Health and Family Services
Document Version	2.0
Document Status	Second Submission
Date Released	May 8, 2026

Document Edit History

Version	Date	Additions/Modifications
1.0	July 18, 2025	First Submission
2.0	May 8, 2026	Second Submission

Introduction

This Certification Course highlights some of the privacy and security rules, laws, and best practices for the handling of a Resident's protected information. Agents and kynectors need to familiarize themselves with privacy and security information to better assist Residents and protect their personal information.

Table of Contents

Document Control Information 2
Document Edit History 2
Introduction 3
Table of Contents 3
1. Policies, Standards, & Laws 5
1.1 Health Insurance Portability and Accountability Act (HIPAA) 5
1.2 Personally Identifiable Information (PII) 7
1.3 Protected Health Information (PHI) 8
1.4 Personally Identifiable Information (PII) and Protected Health Information (PHI) 9
1.5 Federal Protection and Kentucky Statutes 10
1.6 Principle of Least Privilege 11
2. Physical and Electronic Security 11
2.1 Account Security for Agents and kynectors 11
2.2 Email Security for Agents and kynectors 12
2.3 Data Encryption 13
2.4 Email Encryption 14
2.5 Internet Connections 14
2.6 What Makes a Clean Desk 15
3. Security Threats 16
3.1 Social Engineering 16
3.2 Types of Phishing 17
3.3 Insider Threats 18
3.4 What is Malware and How Does It Work? 19
4. Security Best Practices 20
4.1 Handling Personally Identifiable Information (PII) 20
4.2 Tips and Tricks 21
4.3 Penalties and Violations 22

5. Escalation Resources 23
5.1 Escalation 23

1. Policies, Standards, & Laws

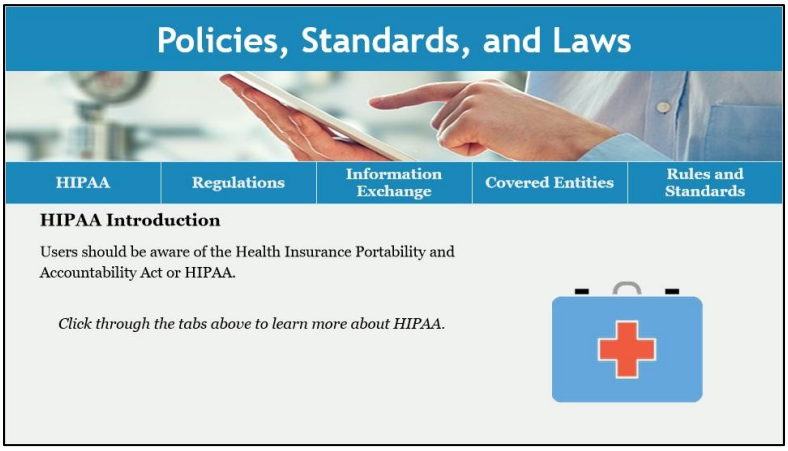
1.1 Health Insurance Portability and Accountability Act (HIPAA)

Slide Voice-over: Users should be aware of the Health Insurance Portability and Accountability Act (HIPAA). Below is key information to keep in mind:

- **HIPPA**: Established in 1996, HIPAA is a federal law with the following primary objectives:
  - Facilitate the retention of health insurance coverage for Residents.
  - Protect the confidentiality and security of health care information.
  - Assist the health care industry in managing and reducing administrative costs.
- **Regulations**: HIPAA consists of a set of rules and regulations that apply to covered entities and their business associates. Residents, organizations, and agencies identified as covered entities are required to comply with HIPAA's standards to protect Individually Identifiable Health Information (IIHI) and to provide patients with specific rights related to that information. When a covered entity engages with a business associate, it must formalize a contract or similar agreement that clearly defines the business associate's responsibilities. This agreement should specify the compliance requirements for the business associate, including those necessary to ensure the privacy and security of Protected Health Information (PHI).
- **Information Exchange:** HIPAA information exchange includes entities that process non-standard health information that they receive from another entity into a standard electronic format or data content, or vice versa.
- **Covered Entities:** Healthcare providers and Health plans are considered covered entities.
  - Examples of covered health care providers include: Doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies.
  - Examples of covered Health Plans include: Health insurance companies, health maintenance organizations or HMOs, company health plans, and government programs that pay for health care.
- **Rules and Standards:** Transactions and Code Set Standards: Creates a uniform way to perform Electronic Data Interchange 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.
  - **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. Also required is appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

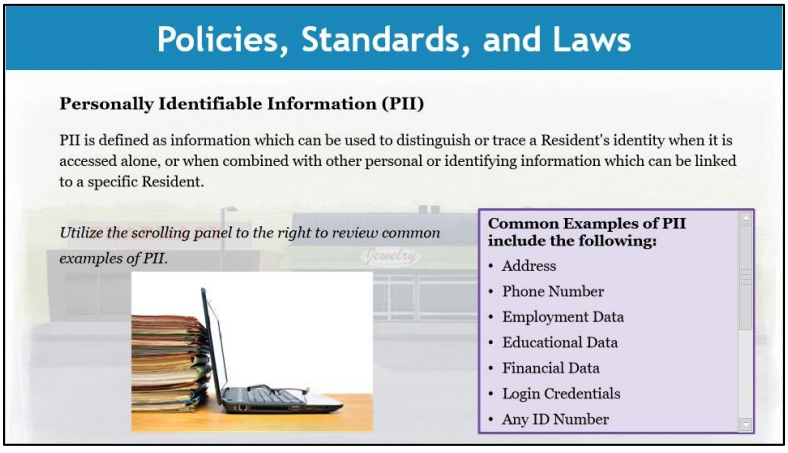
- **Enforcement Rule:** Contains provisions relating to compliance and investigations, the imposition of civil penalties for violation of the HIPAA Administrative Simplification Rules, and procedures for hearings.
- **Incident Notification Rule:** Requires HIPAA covered entities and their business associates to provide notification following an incident of unsecured PHI. 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.



1.2 Personally Identifiable Information (PII)

Slide Voice-over: Personally Identifiable Information *(*PII) is defined as information which can be used to distinguish or trace a Resident's identity when it is accessed alone, or when combined with other personal or identifying information which can be linked to a specific Resident. Below are common examples of PII.

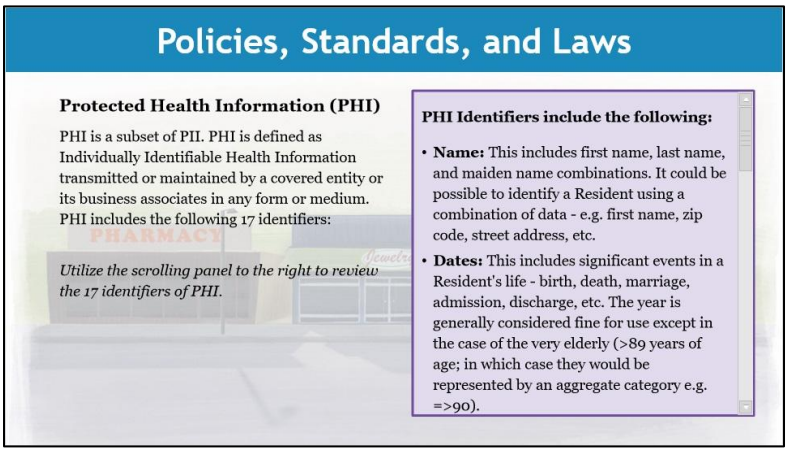
- **Common Examples of PII include the following:**
  - Address
  - Phone Number
  - Employment Data
  - Educational Data
  - Financial Data
  - Login Credentials
  - Any ID Number
  - Physical description
  - Biometrics
  - Social Security Number
  - Driver's License Number
  - Health Data
  - Credit Card Number
  - Photographs



1.3 Protected Health Information (PHI)

Slide Voice-over: PHI is a subset of 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 17 identifiers:

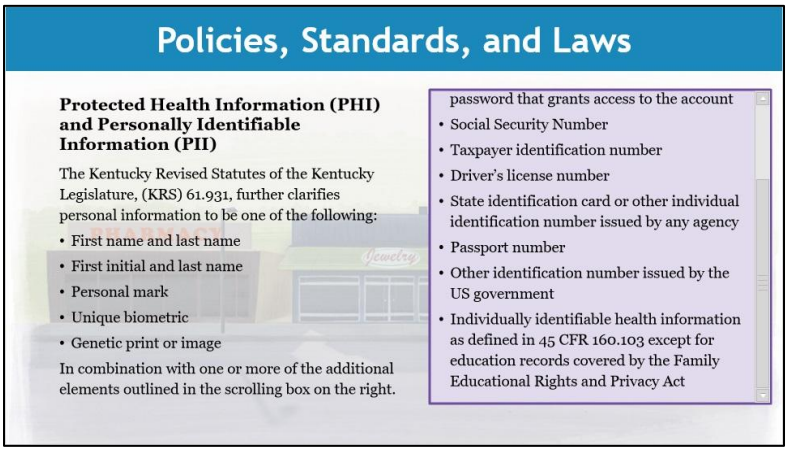
- **PHI Identifiers include the following:**
    - **Name:** This includes first name, last name, and maiden name combinations. It could be possible to identify a Resident using a combination of data - e.g., first name, zip code, street address, etc.
    - **Dates:** This includes significant events 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:** This includes 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 website 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.



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

Slide Voice-over: 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, or genetic print or image. In combination with one or more of the additional elements to the below:

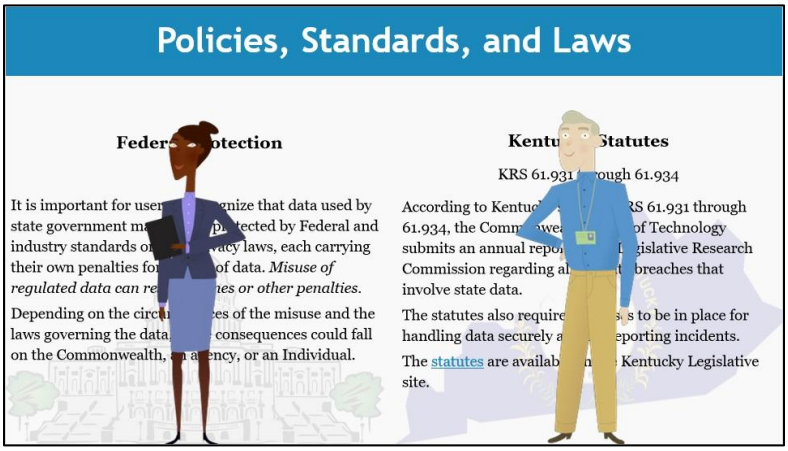
- **Additional Elements:** An account number, credit card number or debit card number with required security or access code or password that grants access to the account, Social Security Number (SSN), taxpayer identification number, driver's license number, state identification card or other individual identification number issued by any agency, passport number, other identification number issued by the US government, and/or individually identifiable health information as defined in 45 CFR 160.103 except for education records covered by the Family Educational Rights and Privacy Act.



1.5 Federal Protection and Kentucky Statutes

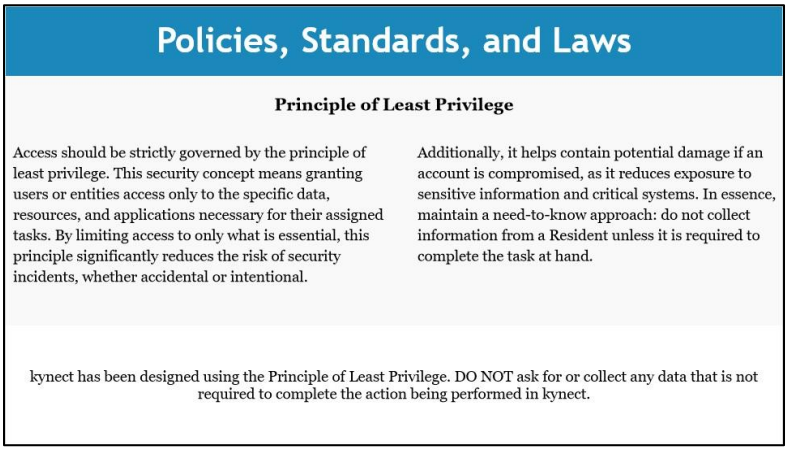
Slide Voice-over: **Federal Protection:** It is important for users to recognize that data used by state government may also be protected by Federal and industry standards or data privacy laws, each carrying their own penalties for misuse of data. Misuse of regulated data can result in fines or other penalties. Depending on the circumstances of the misuse and the laws governing the data, these consequences could fall on the Commonwealth, an agency, or an Individual.

Kentucky Statutes: According to Kentucky statutes KRS 61.931 through 61.934, the Commonwealth Office of Technology submits an annual report to the Legislative Research Commission regarding all security breaches that involve state data. The statutes also require processes to be in place for handling data securely and for reporting incidents. The statutes are available on the Kentucky Legislative site.



1.6 Principle of Least Privilege

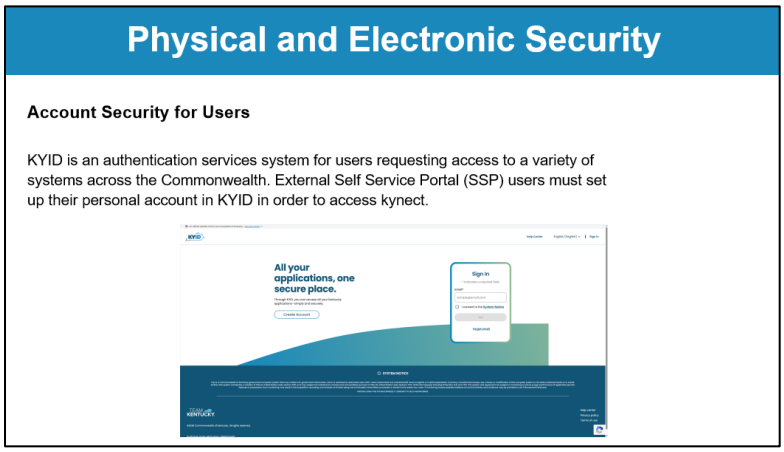
Slide Voice-over: Access should be strictly governed by the principle of least privilege. This security concept means granting users or entities access only to the specific data, resources, and applications necessary for their assigned tasks. By limiting access to only what is essential, this principle significantly reduces the risk of security incidents, whether accidental or intentional. Additionally, it helps contain potential damage if an account is compromised, as it reduces exposure to sensitive information and critical systems. In essence, maintain a need-to-know approach: do not collect information from a Resident unless it is required to complete the task at hand. kynect has been designed using the Principle of Least Privilege. DO NOT ask for or collect any data that is not required to complete the action being performed in kynect.



2. Physical and Electronic Security

2.1 Account Security for Agents and kynectors

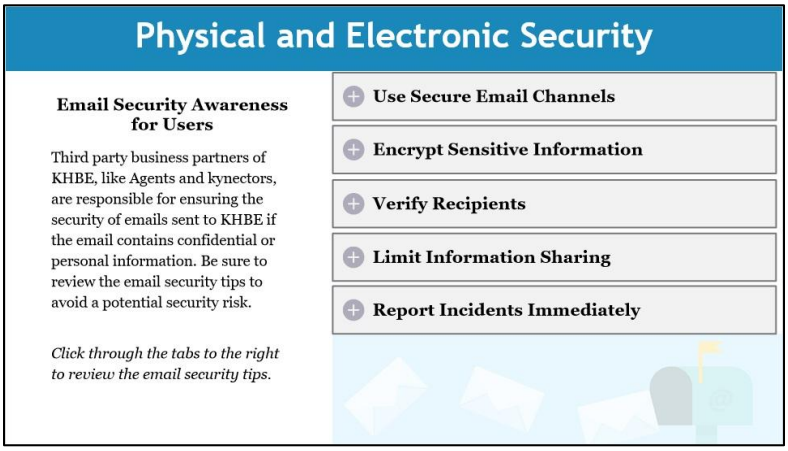
Slide Voice-over: KYID is an authentication services system for users requesting access to a variety of systems across the Commonwealth. External Self Service Portal (SSP) users must set up their personal account in KYID in order to access kynect.



2.2 Email Security for Agents and kynectors

Slide Voice-over: Add accordion feature third party business partners of KHBE, like Agents and kynectors, are responsible for ensuring the security of emails sent to KHBE if the email contains confidential or personal information. Be sure to review the email security tips to avoid a potential security risk to clean up the slide. Below are email security tips to keep in mind:

- **Use Secure Email Channels:** Always use your organization's secure email system for transmitting PII and PHI. Avoid using personal email accounts or unencrypted email services.
- **Encrypt Sensitive Information:** When sending emails containing PII or PHI, ensure that the information is encrypted. This adds an essential layer of protection against unauthorized access.
- **Verify Recipients:** Double-check email addresses before sending to ensure that the information is being sent to the correct recipient. Misaddressed emails can lead to unintended data breaches.
- **Limit Information Sharing:** Only share the minimum necessary information required for the task at hand. Avoid including unnecessary details that could increase the risk of exposure.
- **Report Incidents Immediately:** If you suspect that an email containing, PII, or PHI has been sent to the wrong recipient or compromised in any way, report the incident immediately to your manager, KHBE at KHBE.Program@ky.gov, and the CHFS Incident Response team at CHFSIncidentResponse@ky.gov.

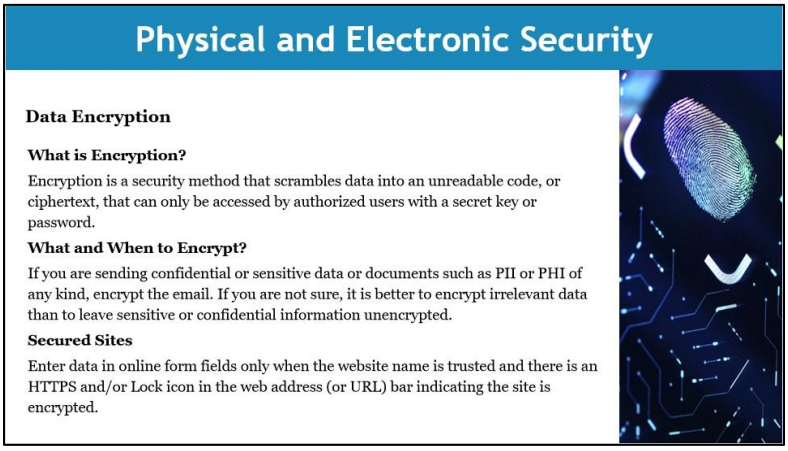


2.3 Data Encryption

Slide Voice-over: What is Encryption? Encryption is a security method that scrambles data into an unreadable code, or ciphertext, that can only be accessed by authorized users with a secret key or password.

What and When to Encrypt? If you are sending confidential or sensitive data or documents such as PII or PHI of any kind, encrypt the email. If you are not sure, it is better to encrypt irrelevant data than to leave sensitive or confidential information unencrypted.

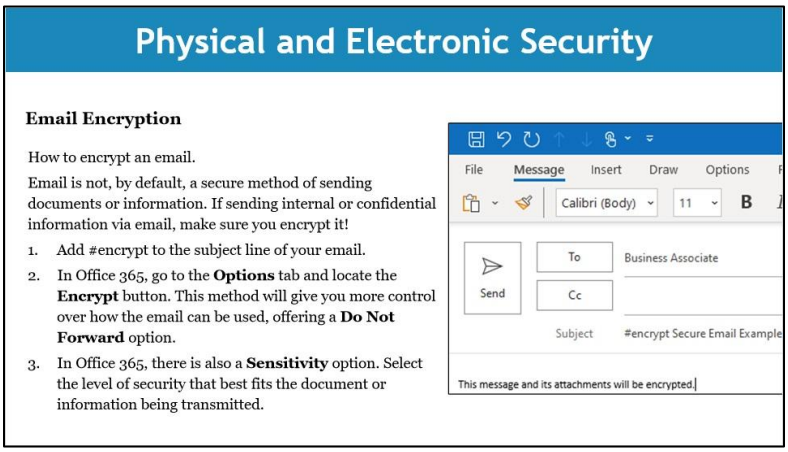
Secured Sites: Enter data in online form fields only when the website name is trusted and there is an HTTPS and/or Lock icon in the web address or URL bar indicating the site is encrypted.



2.4 Email Encryption

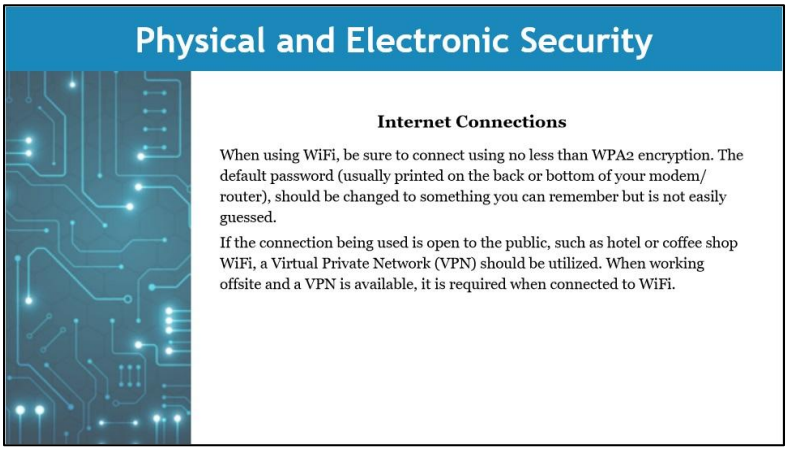
Slide Voice-over: How to encrypt an email: Email is not, by default, a secure method of sending documents or information. If sending internal or confidential information via email, make sure you encrypt it! Below are steps to encrypt an email:

1. Add #encrypt to the subject line of your email.
2. In Office 365, go to the *Options* tab and locate the **Encrypt** button. This method will give you more control over how the email can be used, offering a Do Not Forward option.
3. In Office 365, there is also a Sensitivity option. Select the level of security that best fits the document or information being transmitted.



2.5 Internet Connections

Slide Voice-over: When using WiFi, be sure to connect using no less than WPA2 encryption. The default password (usually printed on the back or bottom of your modem/router), should be changed to something you can remember but is not easily guessed.
If the connection being used is open to the public, such as hotel or coffee shop WiFi, a Virtual Private Network or VPN should be utilized. When working offsite and a VPN is available, it is required when connected to WiFi.

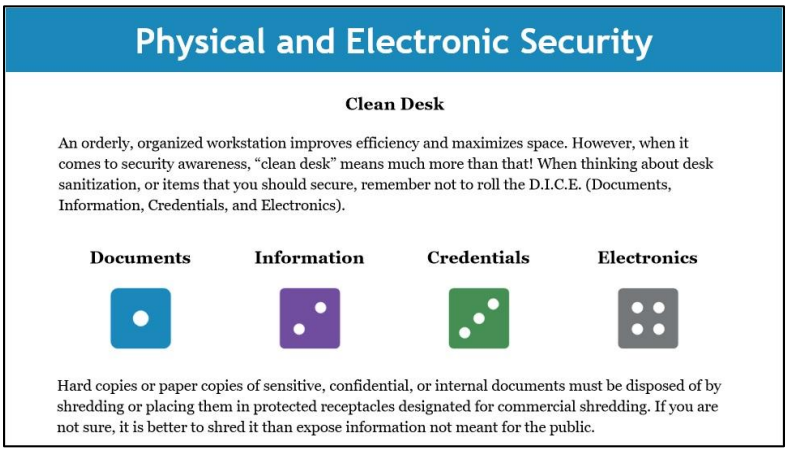


2.6 What Makes a Clean Desk

Slide Voice-over: An orderly, organized workstation improves efficiency and maximizes space. However, when it comes to security awareness, clean desk means much more than that! When thinking about desk sanitization, or items that you should secure, remember not to roll the DICE (Documents, Information, Credentials, and Electronics).

Hard copies or paper copies of sensitive, confidential, or internal documents must be disposed of by shredding or placing them in protected receptacles designated for commercial shredding. If you are not sure, it is better to shred it than expose information not meant for the public.

- **Documents:** Documents include any and all hard copies and files, including the cabinet they are stored in.
- **Information:** Information can be CDs, USB drives, written notes on a whiteboard or post-it note.
- **Credentials:** Credentials consist of login information, authentication tokens, badges, even keys!
- **Electronics:** Electronics consist of devices assigned or used to access or utilize information protected under HIPAA. Computers, phones, tablets, and printers all fall under this category.



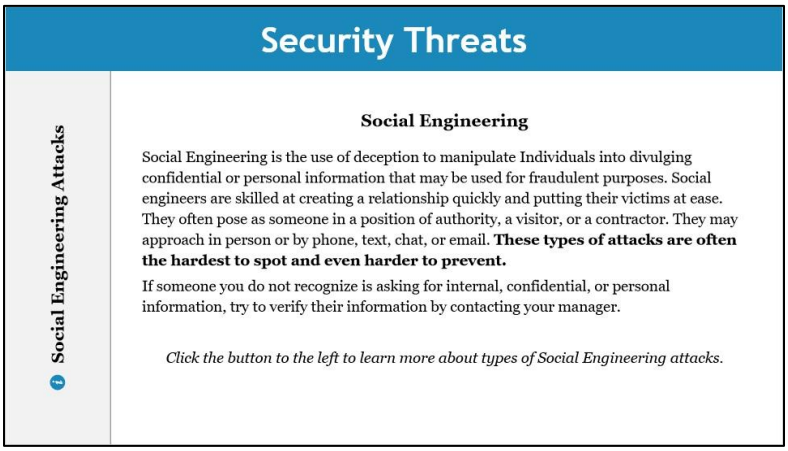
3. Security Threats

3.1 Social Engineering

Slide Voice-over: Social Engineering is the use of deception to manipulate Individuals into divulging confidential or personal information that may be used for fraudulent purposes. Social engineers are skilled at creating a relationship quickly and putting their victims at ease. They often pose as someone in a position of authority, a visitor, or a contractor. They may approach in person or by phone, text, chat, or email. These types of attacks are often the hardest to spot and even harder to prevent.

If someone you do not recognize is asking for internal, confidential, or personal information, try to verify their information by contacting your manager.

- **Social Engineering Attacks:**
  - **Pretexting:** Assuming an identity that gives access or privileges.
  - **Diversion Theft:** Redirecting a delivery to a different location or spoofing an email address to trick the target into sending sensitive information.
  - **Tailgating/Piggybacking:** Waiting for someone to come along that has access to a secure location and entering behind them.
  - **Honey Trap:** Tricking someone into believing they are romantically involved or otherwise interested.
  - **Baiting:** Offering something and asking for sensitive information in return.
  - **Phishing, Vishing or SMShing:** An email, call, or text designed to provoke a response.
  - **Scareware:** Pop-ups on websites that trick the user into believing they have a virus or computer issue.
  - **Watering Hole:** A legitimate website frequented by the intended target or targets that is infected by malware.



3.2 Types of Phishing

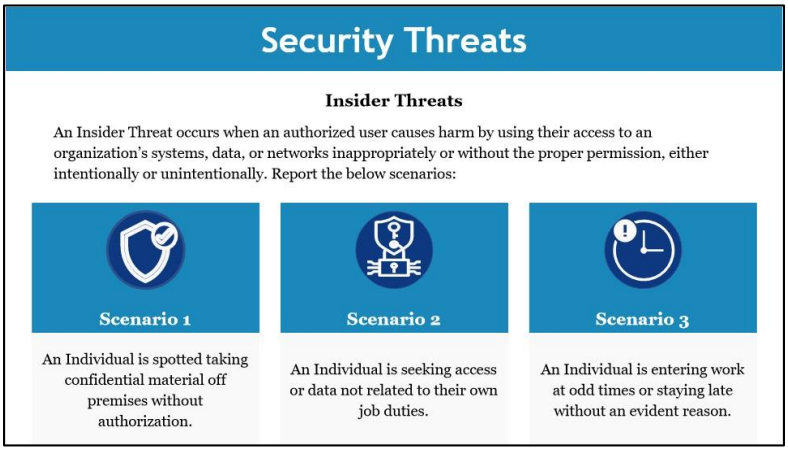
Slide Voice-over: Phishing is a type of cyber-attack where attackers impersonate legitimate organizations or Individuals to deceive recipients into providing sensitive information. These fraudulent communications often appear authentic and may include logos, language, and URLs that closely mimic those of reputable entities.

- **Email:** Email correspondence sent to entice the recipient into a response. Even if it appears nothing has happened, notify your manager immediately if you believe you responded to a malicious email! The criminal's purpose is to gain personal or confidential information or to infect the recipient's device with malware.
- **SMS (Text):** A text message sent by a threat actor with a link or request for information. In this form of attack, they are likely to impersonate a bank or other company where you have an account. Do not click any links or interact with the threat actor.
- **Voice (Phone):** A call from a malicious person with the intention of gaining information. The caller might speak with a sense of urgency, attempt to guilt the target, or try gaining a sense of comradery. If you receive a suspicious call, take down the number if you can and report the incident immediately!

3.3 Insider Threats

Slide Voice-over: Insider Threats: An Insider threat occurs when an authorized user causes harm by using their access to an organization's systems, data, or networks inappropriately or without the proper permission, either intentionally or unintentionally. Report the below scenarios:

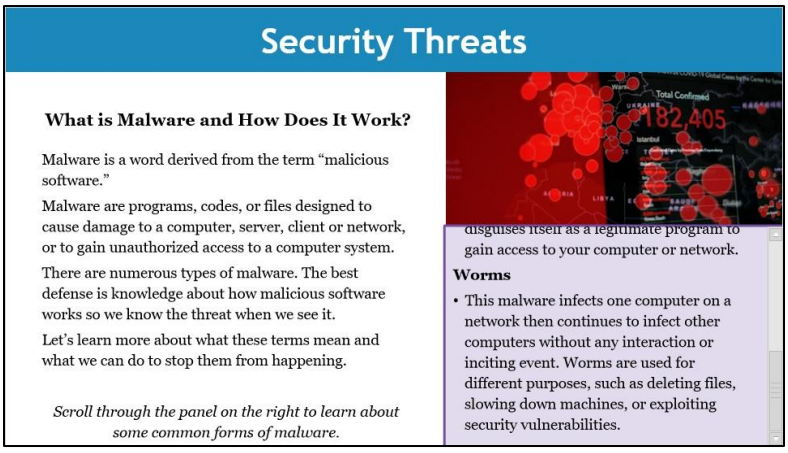
- **Scenario 1:** An Individual is spotted taking confidential material off premises without authorization.
- **Scenario 2:** An Individual is seeking access or data not related to their own job duties.
- **Scenario 3:** An Individual is entering work at odd times or staying late without an evident reason.



3.4 What is Malware and How Does It Work?

Slide Voice-over: Malware is a word derived from the term malicious software.
Malware are programs, codes, or files designed to cause damage to a computer, server, client, or network, or to gain unauthorized access to a computer system. There are numerous types of malware. The best defense is knowledge about how malicious software works so we know the threat when we see it. Let's learn more about what these terms mean and what we can do to stop them from happening. Below are common examples of malware:

- **Viruses:** Just like people, computers are typically very social creatures. They are designed to connect with other computers to share. A virus is a program designed to infect a computer by attaching to other software or files.
- **Trojans:** Named after a historical event where the Greeks gifted a wooden horse with soldiers hidden inside to the Trojans. This malware disguises itself as a legitimate program to gain access to your computer or network.
- **Worms:** This malware infects one computer on a network then continues to infect other computers without any interaction or inciting event. Worms are used for different purposes, such as deleting files, slowing down machines, or exploiting security vulnerabilities.

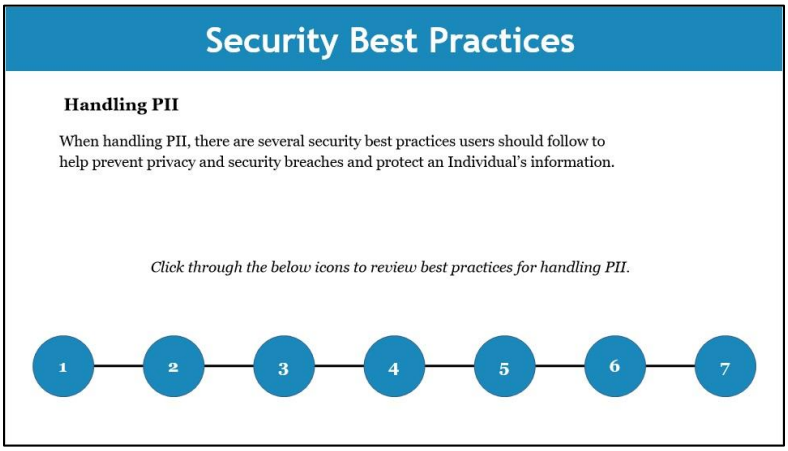


4. Security Best Practices

4.1 Handling Personally Identifiable Information (PII)

Slide Voice-over: When handling PII, there are several security best practices users should follow to help prevent privacy and security breaches and protect an Individual's information. Below are best practices for handling PII:

1. Papers or copies containing PII must never be left unsecured or in public places.
2. When discarding PII, users must use a shredder, not a trash can or recycling bin.
3. Users must use a password protected computer.
4. Users must lock their computers when they are away from the screen.
5. Users never repeat PII aloud if others are nearby or could hear over a phone call.
6. PII is never to be shared unless there is a legitimate business need.
7. When sending PII by email, it must be encrypted.



4.2 Tips and Tricks

Slide Voice-over: Please see below for security best practices.

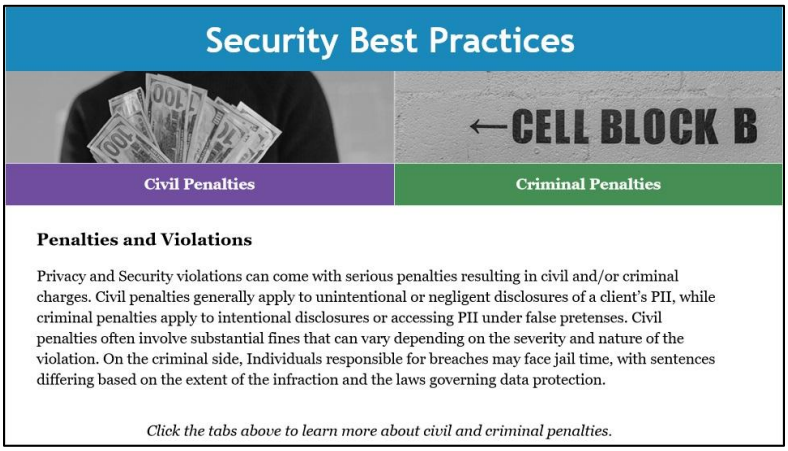
1. **Tip 1:** Use common sense. If you would not want someone sharing the information about you, do not share that information with others!
2. **Tip 2:** If you think there has been a security or privacy breach but are not sure it is always best to report the incident.
3. **Tip 3:** Not sure if a physical document, needing to be disposed, is PII? Stay on the safe side and shred it!
4. **Tip 4:** When sending a client's information via email, it is best to always encrypt the email to avoid any possible privacy or security breaches. Use a VPN when connecting to public WiFi. Do not have one? Connect to your personal hotspot instead.
5. **Tip 5:** If using a paper application, please ensure documents are safely secured until a computer can be accessed.
6. **Tip 6:** Set up where no one can look over your shoulder and see a client's PII.
7. **Tip 7:** Use a privacy screen to avoid unauthorized Individuals seeing your client's PII.
8. **Tip 8:** When possible, use a private space to avoid unintended exposure of a client's PII.

4.3 Penalties and Violations

Slide Voice-over: Privacy and Security violations can come with serious penalties resulting in civil and/or criminal charges. Civil penalties generally apply to unintentional or negligent disclosures of a client's PII, while criminal penalties apply to intentional disclosures or accessing PII under false pretenses.

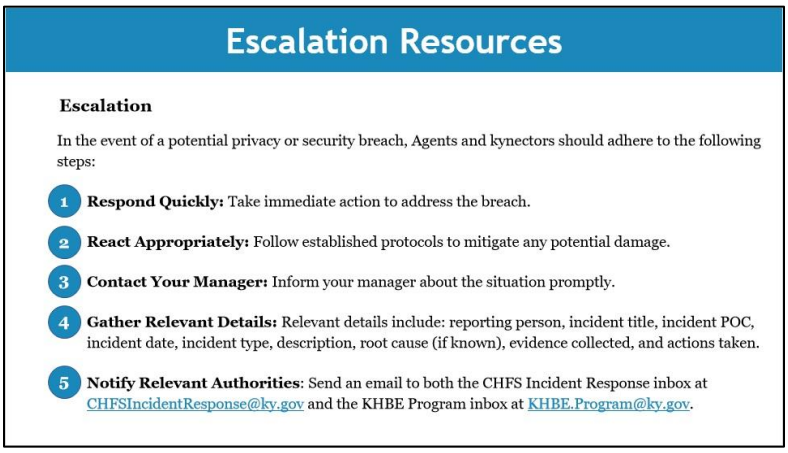
Civil penalties often involve substantial fines that can vary depending on the severity and nature of the violation. On the criminal side, Individuals responsible for breaches may face jail time, with sentences differing based on the extent of the infraction and the laws governing data protection. Below are possible civil and criminal penalties:

- **Civil Penalties:** 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.
- **Criminal Penalties:** Wrongful disclosure of Individually Identifiable Health Information can incur a maximum fine of $50,000 with up to one 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 five years of imprisonment. 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.



5. Escalation Resources

5.1 Escalation

Slide Voice-over: In the event of a potential privacy or security breach, Agents and kynectors should adhere to the following steps:

- **Step 1:** Respond Quickly: Take immediate action to address the breach.
- **Step 2:** React Appropriately: Follow established protocols to mitigate any potential damage.
- **Step 3:** Contact Your Manager: Inform your manager about the situation promptly.
- **Step 4:** Gather Relevant Details: Relevant details include: reporting person, incident title, incident POC, Incident date, incident type, description, root cause if known, evidence collected, and actions taken.
- **Step 5:** Notify Relevant Authorities: Send an email to both the CHFS Incident Response inbox at CHFSIncidentResponse@ky.gov and the KHBE Program inbox at KHBE.Program@ky.gov.