HIPAA Privacy & Security Overview

KENTUCKY
PERSONNEL
CABINET

Department of
Employee Insurance

Introduction

- Every member of the Personnel Cabinet should understand the laws related to HIPAA, especially those related to HIPAA breaches – what they are as well as the financial and professional impact they have – so they can report any suspected breach to their manager and the Department of Employee Insurance’s Privacy and Security Officers.

- As a self-insured health plan, everyone who has access to PHI transmitted to or maintained by the Kentucky Employees’ Health Plan (KEHP) must comply with HIPAA regulations related to Privacy and Security.

Annual HIPAA Training Requirement

All Insurance Coordinators (ICs), Human Resource Generalists (HRGs), Billing Liaisons (BLs), and Commonwealth of Technology technical support resources and staff (COT) are required to complete HIPAA training on an annual basis.

Why is HIPAA Training Required?

- ICs, HRGs, BLs, and COT technical support resources and staff have access to information that is classified as protected health information (PHI). PHI includes oral, written information and all information transmitted by electronic media or maintained in electronic media. This information generally includes: name, address, birth date, social security number (SSN), marital status, and dependent information.
- HIPAA requires that all PHI be handled with extreme care to protect KEHP members. This course meets the annual HIPAA training requirement.

Learning Outcomes

At the conclusion of this course you should be able to:

- Explain the impact HIPAA has on all organizations that interact with KEHP data.
- State the entities that must comply with HIPAA.
- List the penalties imposed for non-compliance.
- State key privacy requirements.
- Describe the security requirements.

Roles and Responsibilities

ICs, HRGs, BLs and COT technical support resources and staff.

ROLES:

As a representative of an agency/employer group that participates in KEHP, the **IC/HRG** is responsible for partnering with the Department of Employee Insurance (DEI) to ensure their employees are informed of the benefits, policies and processes of KEHP.

As a representative of an agency/employer group that participates in KEHP, the **BL** is responsible for partnering with the DEI to ensure bills are reconciled and premiums paid on a timely basis.

COT, as the centralized IT for the Enterprise, is responsible for many critical areas of IT to include: Active Directory, LAN/WAN, security, storage, backups and the transfer of data for the Commonwealth's most sensitive information that includes PHI. COT is the infrastructure hosting partner for KHRIS. COT has access to KEHP's data, which contains PHI for approximately 265,000 members and dependents. COT also serves KEHP by providing help desk services to assist members with IDs and passwords.

Roles & Responsibilities (Cont.)

ICs/HRGs need to:

- Know the benefits available – health insurance, flexible spending accounts, health reimbursement arrangements and waivers.
- Study the Administration Manual and quarterly updates.
- Understand HIPAA and the requirement to complete annual HIPAA training.
- Attend all IC/HRG training and view all webinars.
- Work with their BL to ensure enrollment and billing are in sync.

Roles & Responsibilities (Cont.)

Billing Liaisons need to:

- Reconcile and release health insurance premiums, administrative fees, flexible spending accounts and health reimbursement arrangements.
- Understand HIPAA and the requirement to complete annual HIPAA training

COT Technical Support Resource and Staff need to:

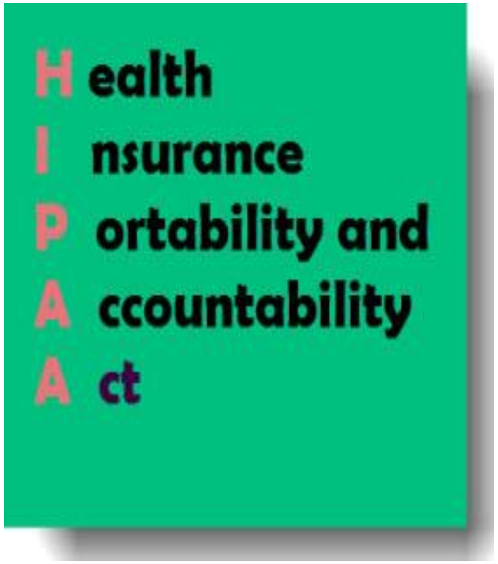
- Understand HIPAA and the requirement to complete annual HIPAA training
- Provide infrastructure hosting for KHRIS
- Provide security and maintenance of state government's servers and network
- Supports active directory, LAN/WAN, security, storage, backups and the transfer of data
- Provide general technical support

Regulatory Background: What is HIPAA?

“HIPAA” stands for the Health Insurance Portability and Accountability Act of 1996, a broad federal law that addresses many healthcare issues, including insurance benefits, medical savings accounts, and fraud and abuse.

It improves portability and continuity of health insurance coverage in the group and individual markets and helps combat waste, fraud, and abuse in health insurance and health care delivery. It promotes the use of savings accounts, improves access to long-term care services and coverage, and simplifies the administration of health insurance.

While the law outlines broad requirements for healthcare organizations, more detailed requirements are found in federal regulations. These regulations were developed by the Department of Health and Human Services (HHS) and written and enforced by Centers for Medicare & Medicaid Services (CMS) and the Office for Civil Rights (OCR).



Administrative Simplification

HIPAA also has requirements for healthcare information. The "administrative simplification" part of the law requires national standards for electronic transactions and the protection of health information that identifies individuals (also known as *protected health information or PHI*). PHI includes name, SSN, DOB, or other *individually identifiable health information*.

Protected health information (PHI) *is Individually identifiable health information transmitted or maintained by electronic or any other medium. PHI excludes individually identifiable health information in education records covered by the Family Education Right and Privacy act. Protected health information is individually6 identifiable health information that is:*

- *Transmitted by electronic media*
- *Maintained in electronic media*
- *Transmitted or maintained in any other form or media, such as on paper or even verbal conversations.*

Individually Identifiable Health Information *is information, including demographic information, which is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse.*

Information including demographic information, that:

- *Relates to the part, present or future physical or mental condition of an individual.*
- *Relates to the provision of healthcare to an individual.*
- *Identifies the individual (or there is a reasonable basis to believe the information can be used to identify the individual).*

Administrative Goals

HIPAA’s goal to reduce costs through administrative simplification will be achieved by streamlining administrative processes through the increased use of technology.

But, putting more patient information on computers comes with a risk. Because it is more accessible, electronic information is more vulnerable to large-scale breaches, such as identity theft. Congress recognized this and wrote the law to require additional protections for health information that identifies individuals.

Administrative Areas

The regulations developed by HHS outline standards in five key areas:

- Electronic transactions
- Code sets
- Unique identifiers
- Privacy
- Security

Two of the five key areas-privacy and security-have the most impact on Insurance Coordinators, Human Resource Generalists, Billing Liaisons, COT staff, and others with access to KEHP data.

Review Question

HIPAA includes requirements for healthcare information.

Which of the following is an example of Protected Health Information (PHI)?

a. Health information transmitted by electronic media
b. Health information maintained in electronic media
c. Health information transmitted or maintained in any other form or media, such as on paper or even verbal conversations
d. All of the above

Think of your answer…the answer is revealed on the next slide.

Review Question - Continued

a. Health information transmitted by electronic media

b. Health information maintained in electronic media

c. Health information transmitted or maintained in any other form or media, such as on paper or even verbal conversations

d. All of the above

d. All of the above

All of the answers are examples of protected health information.

The Omnibus Rule

The January 25, 2013 *Omnibus Rule* expanded penalties for HIPAA violations and added numerous additional notification requirements for breaches of unsecured PHI.

This new law also extended many of the HIPAA Privacy and all the Security requirements and penalties for non-compliance to *business associates*.

The January 25, 2013 *Omnibus Rule* expanded penalties for HIPAA violations and added numerous additional notification requirements for breaches of unsecured PHI. This new law also extended many of the HIPAA Privacy and all the Security requirements and penalties for non-compliance to *business associates*.

On January 25, 2013, the OCR published the Omnibus Rule. The Omnibus provisions were effective on March 23, 2013, and the compliance date is September 23,2013 for all provisions, except for some business associate agreements.

The new rules are the first update of the HIPAA Privacy and Security Rules since the current regulations were published more than 10 years ago. The Omnibus Rule combines, updates and finalizes four rules:

July 2010 Notice of Proposed Rule Making (NPRM) on HITECH privacy and security changes to HIPAA.

October 2009 Notice of Proposed Rule Making (NPRM) on Genetic Information Nondiscrimination Act (GINA) changes to HIPAA.

August 2009 Interim Final Rule (IFR) on HIPAA Breach Notification.

October 2009 Interim Final Rule (IFR) on HIPAA Enforcement Rule/

The Omnibus rule does not include the Privacy regulation for accounting for disclosures.

Persons or companies that perform a function for a covered entity involving the use or disclosure of individually identifiable health information. This includes billing or claims processing, medical transcription, utilization review, quality assurance, release of information and off-site storage. Business associates exclude persons who are part of the covered entity's workforce.

Examples include billing companies, transcriptionists, health insurance brokers and third party administrators (TPAs).

Compliance

KEHP

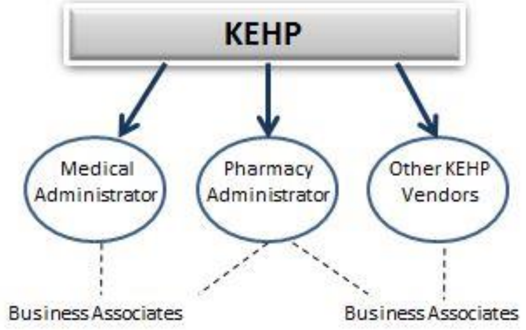
- DEI operates KEHP which is a Self-Insured Group Health Plan subject to HIPAA
- is a Covered Entity under HIPAA
- Maintains PHI, such as names, address, birth dates, marital status, dependent information and SSNs
- Has adopted Privacy and Security policies and procedures
- Issues a Privacy Notice each year
- Has HIPAA Business Associate agreements with
    - Anthem – Medical Third Party Administrator (TPA)
    - CVS/caremark – Pharmacy Benefits Manager (PBM)
    - WageWorks – Spending Account and COBRA Partner
    - HumanaVitality – Wellness Partner
    - Vitals – Transparency Partner
    - AON and Truven – Healthcare Consultants

Business Associates

To expand the reach of the regulations beyond covered entities, HHS developed the concept of "business associates." **Business associates are persons or companies that do work for a covered entity that requires them to have access to PHI.**

Business associates exclude persons who are part of the covered entity's workforce.

Under HIPAA, covered entities are required to have written agreements or contracts with their business associates to protect health information. The Omnibus Rule significantly expands the responsibilities of business associates to follow many HIPAA requirements. They now directly face the same fines and penalties as covered entities.



Examples of **KEHP business associates** include:

- Vendor Partners – Anthem, CVS/caremark, WageWorks, HumanaVitality, Vitals, AON Hewitt, Truven
- COT staff

Examples of workforce members or persons serving as agents of KEHP include:

- Agency ICs, HRGs, and BLs
- Personnel Cabinet Staff

Covered Entities

HIPAA imposes significant new requirements on nearly every organization that provides or pays for healthcare services. Under HIPAA, the organizations that are directly affected and must comply with the regulations are known as “covered entities.” These include:

- Health plans, which include self-funded employer plans and government programs like Medicare and Medicaid.
- Healthcare providers who transmit certain electronic transactions known as “covered transactions.”
- Healthcare clearinghouses, which translate healthcare electronic transactions between non-standard and standard transactions.
- Medicare Part D plans, which provide prescription drug coverage to Medicare beneficiaries.

Breach Definition

- A breach may occur any time there is unsecured PHI in either paper or electronic medical records.
- Breaches that affect 500 or more member records must be reported to the DEI Privacy & Security Officers and the Office of Civil Rights (OCR) immediately. Media would also need to be notified to alert impacted individuals.
- PHI must be secured:
    - Electronic PHI (ePHI): Encrypt when the information is at test and when it's being sent electronically.
    - Paper PHI: Keep it locked up in file drawers or a file room, and shred based on agency's retention schedule.

Breach Types

The Most Common types of breaches are:

- Unencrypted emails
- Hacking/IT incident
- Improper disposal
- Loss of paper or electronic PHI
- Theft of mobile devices and paper records
- Faxing to the wrong person

Locations of breaches include:

- Desktop computer
- Email
- Electronic Medical Record (EMR)
- Laptops, flash drives, etc
- Network server
- Tablet, smart phone
- Snail mail

Enforcement & Auditing

How will compliance with HIPAA be enforced? By the Office for Civil Rights (OCR).

If an individual files a complaint with the OCR, it will conduct an investigation, reviewing the circumstances of the complaint and what the organization has done to comply.

AUDIT

Notification of Audit

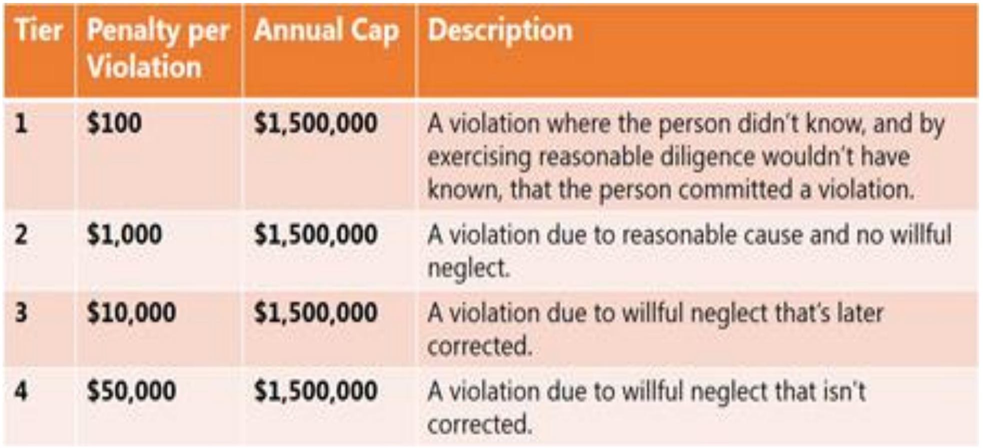
A full compliance review may be conducted, which could extend to every aspect of the organization's compliance with HIPAA regulations. Failure to comply with the regulations may result in a civil fine or criminal prosecution.

Note: The American Recovery and Reinvestment Act (ARRA) of 2009 requires the Department of Health and Humana Services (HHS) to perform periodic compliance audits to ensure that covered entities and business associates are meeting the HIPAA Privacy and Security provisions. This provision became effective February 17, 2010 and the OCR began audits in 2011, continued them in 2012 and stated that audits will now be a consistent part of OCR.

Compliance Violations – Civil Monetary Penalties and Fines

These are two categories of HIPAA violations: civil and criminal. HIPAA provides four levels of civil penalties for covered entities and business associates that fail to comply with the regulations. It’s important to know that HIPAA sets a minimum standard and each state has the flexibility to establish stricter requirements (and associated penalties).

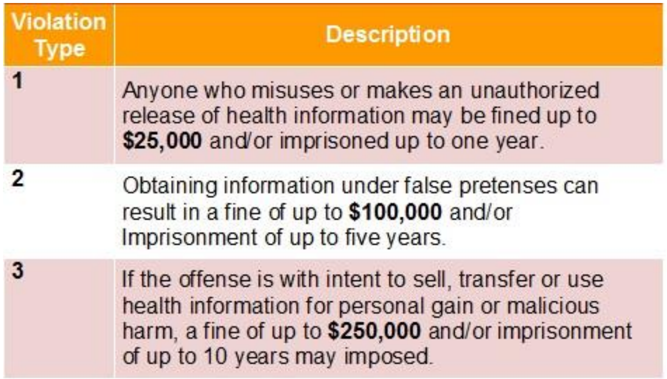
State attorneys general may also bring HIPAA enforcement actions against a covered entity or business associate that violates the HIPAA Privacy and Security Rules. Attorneys’ fees may be awarded against the violator in such proceedings.



Tier	Penalty per Violation	Annual Cap	Description
1	$100	$1,500,000	A violation where the person didn’t know, and by exercising reasonable diligence wouldn’t have known, that the person committed a violation.
2	$1,000	$1,500,000	A violation due to reasonable cause and no willful neglect.
3	$10,000	$1,500,000	A violation due to willful neglect that’s later corrected.
4	$50,000	$1,500,000	A violation due to willful neglect that isn’t corrected.

Compliance Violations – Criminal Penalties

There are three types of HHS violations that could lead to criminal penalties and fines:



Violation Type	Description
1	Anyone who misuses or makes an unauthorized release of health information may be fined up to **$25,000** and/or imprisoned up to one year.
2	Obtaining information under false pretenses can result in a fine of up to **$100,000** and/or Imprisonment of up to five years.
3	If the offense is with intent to sell, transfer or use health information for personal gain or malicious harm, a fine of up to **$250,000** and/or imprisonment of up to 10 years may imposed.

Review Question

Which of the following are NOT possible consequences of noncompliance?

a. OCR may initiate an investigation.
b. State and/or federal penalties may be imposed.
c. Your company may improve its reputation.
d. Remediation could cost in excess of $1,000,000

Answer is revealed on the next slide

Review Question - Continued

a. OCR may initiate an investigation.
b. State and/or federal penalties may be imposed.
c. Your company may improve its reputation.
d. Remediation could cost in excess of $1,000,000.

The answer is:

c. Your company may improve its reputation.

Impact of HIPAA on ICs, HRGs and Billing Liaisons

IC's and HRGs must:

- maintain PHI such as names, addresses, birth dates, marital status, dependent information and SSNs
- comply with HIPAA regulations
- comply with DEI policies and procedures
- have the ability to receive and send encrypted email
- complete HIPAA online training
  - Annually
  - Within 30 days of assuming IC/HRG duties
- protect a member's PHI by securing verbal and written information
- utilize sage computer skills and report suspected

Impact of HIPAA on COT staff

COT staff must:

- maintain PHI such as names, addresses, birth dates, marital status, dependent information and SSNs
- comply with HIPAA regulations
- have the ability to receive and send encrypted email
- complete HIPAA online training
    - annually
    - within 30 days of assuming COT duties
- protect a member's PHI by securing verbal and written information
- utilize safe computer skills and report suspected security incidents to the DEI Privacy and Security Officers

Review Question

Let’s assess your understanding of those required to follow HIPAA regulations.

Under HIPAA, which are not covered entities?

a. Kentucky Employees’ Health Plan
b. Employer (i.e. grocery store or other company)
c. Chiropractors
d. Hospitals

Review Question - Continued

a. Kentucky Employees’ Health Plan
b. Employer (i.e. grocery store or other company)
c. Chiropractors
d. Hospitals

THE ANSWER IS:

b. Employer (i.e. grocery store or other company)

Privacy Standard - Contact

KEHP's Privacy Officer

Sharron Burton, General Counsel
Sharron.burton@ky.gov
Personal Cabinet
Department of Employee Insurance
501 High Street, 3rd Floor
Frankfort, KY 40601

The Privacy standard is designed to protect patient's medical or health information, and give individuals more control over how their information is used. Under the Privacy regulations, PHI may not be used or disclosed unless:

- An Individual's permission or authorization is obtained.
- Disclosure is specifically required or permitted under HIPAA.

A covered entity, like KEHP, is not required to get patient consent to use or disclose information for treatment, payment or healthcare operations. However, a covered entity may obtain consent if it chooses to do so or if state law requires it.

New Rights – Individual Rights

HIPAA also gives individuals significant rights with respect to their health information.

This includes the right to:

- Receive notice about a covered entity's privacy practices.
- Request restrictions on the use or disclosure of PHI.
- Trust in confidential communications.
- Access health information including electronic information.
- Request amendments to health information.
- Obtain an accounting of the uses and disclosures of PHI.

Information about these rights in relationship to the KEHP can be found at KEHP.ky.gov and select Legal Notices.

Access to Protected Health Information (PHI)

An individual has the right to access the records used to make decisions about him or herself. These records are called a designated record set.

When accessing their records, individuals have the right to inspect the records and obtain a copy of them for which they may be charged a reasonable fee. However, there are some exceptions. Individuals do not have the right to access:

- Psychotherapy notes.
- Information compiled for a civil, criminal or administrative action or proceeding.
- Health records if they are an inmate.

Access to Protected Health Information (PHI) cont.

There are other circumstances under which individuals may be denied the right to access his or her records. For example, information that is part of a research project currently in progress may not be released to the individual.

If the covered entity uses or maintains an electronic health record (HER) with respect to PHI regarding that individual, the individual has the right to obtain that information in an electronic format if the records are readily producible in that format.

The individual may also request that a copy be transmitted to a third party, such as their spouse, child or lawyer. You may charge a reasonable labor and supplies fee for both paper and electronic copies, including postage.

Accounting of Disclosures

PHI is used and disclosed for many purposes,
but most people don't know how their information has been used.

Under HIPAA, individuals can find out who their health information
was shared with by requesting an accounting of disclosures.

Covered entities must account for disclosures of PHI for six years prior to the data on which the accounting is requested.

Not all disclosures are included in the accounting requirement. The following are ***examples of disclosures*** that do not need to be included in the accounting:

- *For treatment, payment and healthcare operations*
- *To the patient*
- *Authorized by the patient*
- *Facility directory or person involved in individual's care*
- *For national security or intelligence purposes*
- *To correctional institutions or law enforcement*.

Authorization for Use and Disclosure

Healthcare professionals often use the terms “*authorization*” and “*consent*” interchangeably, but they are different things.

Authorization: Written permission allowing the covered entity to disclose PHI to an outside entity. For example, an authorization would be required to disclose PHI for issuance of a life insurance policy.

Consent: Written permission allowing the covered entity to use and disclose PHI for treatment, payment and healthcare operations (this is optional for covered entities).

Permission for Use and Disclosure

The written authorization must also name the person or organization authorized to make the disclosure and the person or organization to which the disclosure may be made.

Uses and disclosures *requiring* an opportunity to agree or object:

There are certain circumstances in which consent or authorization is not required, but the individual must be told about the proposed use or disclosure and given an opportunity to agree or object. These circumstances include:

- Disaster relief.
- Use in the facility directory (E.g. Offering a patient's room number to a visitor).
- Disclosure to family members and others involved in the individual's care.

Uses and disclosures *NOT requiring* an opportunity to agree or object:

- There are certain circumstances under which consent or authorization is not required. This includes reporting required by law. And responding to subpoenas and court orders.

Minimum Necessary

The Privacy regulations require covered entities or business associates to restrict the use of PHI to the minimum amount of information needed. Access to information should be assigned on a need-to-know basis.

This means the individual or entity receiving the PHI should have a legitimate need for the information.

To ensure compliance, covered entities must identify which staff members need access to PHI and give them access to the information needed to do their jobs. For example, a billing clerk should have access only to a patient’s demographic and billing information, not the patient’s entire medical or clinical record.

NOTE: The Minimum Necessary requirement does not apply to providers who request information to treat a patient.

Notice of Privacy Practices (NPP)

HIPAA also requires providers and health plans to provide a Notice of Privacy Practices (NPP). This explains the individual's rights and covered entity's legal duties with respect to PHI. Providers are required to make a 'good faith' effort to obtain the patient's written acknowledgement of receipt of the NPP.

Some of the uses and disclosures stated in the NPP include:

- To obtain payment.
- To a public health authority.
- For Workers' Compensation.
- How to file a complaint.
- Rights of the individual.

Genetic Information

The Genetic Information Nondiscrimination Act (GINA) imparts the HIPAA Privacy Rule requirements in two ways:

- It prohibits health plans, except long-term care plans, from using genetic information for underwriting purposes.
- The definition of health information, and thus protected health information, now includes genetic information.

The Omnibus Rule also added new definitions for family member, genetic information, genetic service and genetic test.

Amend & Restrict

An individual has the right to ask a provider, health plan or business associate to amend PHI in a designated record set for as long as they maintain the information.

Be aware that:

- The individual may be asked to make the request in writing.
- Providers and health plans are not required to accept the requests.
- The requests may be denied in some situations.

Providers must comply with an individual’s request for PHI restriction of disclosure to a health plan if:

- The disclosure is for carrying out payment or healthcare operations, and is not otherwise required by law.
- The PHI pertains solely to a healthcare item or service that has been paid in full.

Administrative Requirements

The last section of the HIPAA Privacy regulation is the administrative requirements related to privacy including having a Privacy Officer who is responsible for the privacy requirements, periodic privacy training for your staff, and privacy policies and procedures that tell your staff how to use and disclose PHI, and how to report a problem they find or see happening in your office.

Administrative Requirements:

- Name a Privacy Officer-DEI’s Privacy Officer is Sharron Burton
- Train workers in Privacy Regulations
- Have a complaint process
- Sanction policy
- Refrain from intimidating or retaliatory acts
- Issue privacy policies and procedures
- Mitigation-Mitigate any harm caused by a breach

Security Standards-Contact

KEHP's Security Officer

Paula Chisholm
Assistant Director of Financial & Data Services
Department of Employee Insurance
Personnel Cabinet
501 High Street, 2nd Floor
Frankfort, Kentucky 40601

Security standards provide a framework for covered entities or business associates to develop information security programs. The standards are designed to be technology-neutral and scalable, so they can be used in a wide range of settings.

The standards apply to the electronic protected health information (ePHI) a covered entity creates, receives, maintains or transmits.

Security Basics – Why?

Information security focuses on three types of safeguards:

Administrative –Formal, documented practices to protect ePHI. This includes policies and procedures to manage conduct of users.

Physical – Procedures to protect computer systems, buildings and other equipment from fire and other natural and environmental hazards, as well as from intrusion or theft.

Technical –Processes to control and monitor access to ePHI, such as passwords, as well as limit unauthorized access to data that is transmitted over a communications network.

Keeping PHI secure is every user's responsibility. Failure to follow established security policies and procedures can result in inadvertent disclosure of this confidential information, which could lead to substantial regulatory penalties. Sanctions for violating HIPAA policies could include discharge from your job.

Security Basics – What Is Information Security?

Information security includes all activities to control and protect information assets from misuse, theft, the destruction or damage. This includes:

- Disaster planning
- Technical measures and controls to detect, document and counter threats.

Effective information security consists of:

- Meeting the goals of Confidentiality, Integrity and Availability (CIA)
- Instituting and following policies and procedures that balance information and confidentiality against cost, usability and availability.

*With each technical advancement, we increase the risk of security violations and threats to our information technology (IT) environment.

Security Basics – Who Is Responsible?

Everyone with access to KEHP data is responsible for protecting that data. While the Security Official has oversight responsibility, compliance hinges on each employee's day-to-day actions. As a reminder, DEI's Security Officer is Paula Chisholm.

Most security breaches are accidental, not intentional, and usually occur because someone is casual or careless with an individual's Phi.

Think about where you have PHI. Is it secure? Consider computers, tablets, smart phones, PDA devices, diskettes, external disk drives, wireless devices, Internet connections, remote access – all of these are potential areas of risk.

Security Basics – Risk Analysis

All staff members should know where ePHI is stored. Information security includes performing a risk analysis of where your ePHI is stored, and how it's electronically transmitted into and out of your office. Think creatively about where ePHI is stored, especially as technology grows and changes. It can be stored in:

- Servers and networks
- An Electronic Health Record (EHR) system
- Mobile devices (e.g. laptops and smart phones)
- Cloud storage
- Excel spreadsheets
- Hard drives of printers, fax machines and copiers
- Social media pages, email and text messages

Proper Workstation Use

The term “workstation” is used for a variety of computer-related equipment, such as desktops, laptops, tablets and smart phones.

The guidelines in this section apply to all devices, particularly if they contain PHI.

If you work at home, and have access to your work files and servers, all the same security precautions apply.

Appropriate Uses:

Workstations should only be used for their intended business purpose. Organizations define this differently, however, it generally means not using the device for personal reasons-personal email, viewing pictures, listening to music, surfing the Internet for non-business purposes, downloading unauthorized software, etc.

Secure Printing, Faxing & Copying

PHI must remain protected throughout its life cycle – in both electronic and hard copy form. If you're printing confidential information print it to a secure machine from which you personally control who retrieves the output. When printing to a group printer, there is a risk that the output could be picked up by someone else unless you retrieve it immediately.

Faxing has similar concerns. Follow your internal policies and procedures to ensure a fax foes to the intended recipient and that the faxed information is not left on the fax machine after it's transmitted. Faxing PHI to the wrong party is one of the most common sources for accidental disclosures reported today.

Finally, fax machines, printers, and copy machines today have hard drives that retain information from what you have transmitted, printed or copied. Again, follow your policies and procedures to make sure the hard drive is erased or destroyed when it is no longer used in your organization.

Computer and other machine hard drives can be easily shredded as paper.

Storage Devices

Hard drives, dictation tapes, USB flash drive (i.e. jump or thumb drive), CD ROMs, DVDs, backup/storage disks are all examples of storage devices that can be used to store ePHI. These devices are often the greatest source of loss, since in many cases they potentially contain thousands of records and can be easily removed. Follow these simple guidelines to ensure storage devices are properly protected.

Deleting Records – Deleting a file off a hard drive of a computer or a USB flash drive doesn't necessarily remove the information. Make sure old tapes (data or voice), computer hard drives, flash drives and all other hard drives from electronic devices go through a proper cleansing or destruction procedure before giving it to someone else. Contact your IT representative for more information on this procedure.

Unintentional Storage Devices – Hard drive or copiers, printers, and fax machines often have hard drives that retain information from what was copied and/or sent. Follow your organization's policy to make sure the hard drives are erased or destroyed when the machine (s) will no longer be used in your organization.

External Storage devices – Unless authorized, don't bring external storage devices into the organization. This represents the potential risk of introducing viruses and creates risk that ePHI will leak out of the organization. In today's world, this is called Bring Your Own Device (BYLD).

Asset Tracking – Make sure the responsible person according to your policy is aware of any movement, increase or decrease in electronic devices (such as desktops, laptops, hard drives, etc) so that an accurate accounting of all information assets can be maintained and tracked.

There is a new storage type called "cloud" storage. Cloud storage is virtual storage often mixed with other entities' data and has all of the security concerns other types of storage devices carry.

Additionally, another type of storage moves a copy of your data electronically from your server(s) to an off-site server. This shares the same security concerns as the other types of storage.

Foreign Programs

Installation of foreign programs – like games, music, web-mail (e.g. Yahoo! And Gmail) and chat room – may affect your computer and the entire network. You should never install software on your computer without permission from your IT department.

Viruses & Spyware – A computer virus is a computer program that gets loaded on your PDA or computer without your knowledge. These programs can allow access to your computer, send information to outsiders or harm data stored on your computer or PDA. They can even allow access to your network exposing your whole organization to an outsider.

Viruses and spyware can be transmitted via email attachments or inside of other programs you choose to download, such as games, music or social media.

Portable Devices

Portable devices such as PDAs, laptops, tablets and smart phones are becoming more and more common in the workplace. Remember, most of these devices are wireless and thus open to the Internet. Users of these devices need to understand the additional risks involved. The greatest risk in that the device is lost or stolen. It's critical that all these devices utilize the password features that are built in and that good password policies are followed to minimize the risk of protected information getting inappropriately disclosed.

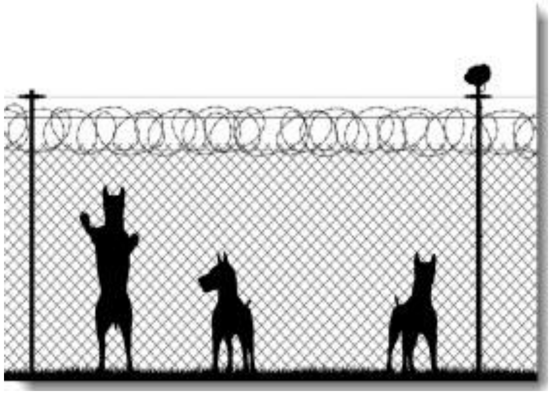
Safety: Any portable device that has the capability of storing and transmitting ePHI must utilize encryption to prevent confidential data from being intercepted and recognized. Consult your organization's policies to determine which portable and/or wireless devices are allowed (and under what conditions) before using one.

Physical Controls

In the Security Rule, physical controls are also important, such as physically limiting access to those devices that contain individual health information. This is a critical component of any overall security plan.

Here are some other simple guidelines to help keep information physically secure:

- Don't share access devices (e.g. badges, keys, combination codes).
- If you are in charge of physical access, keep access up-to-date (e.g. as employees terminate).
- Angle your computer away from public access.
- Keep all PDAs, laptops and media locked up when not in use.
- Lock all desks, files and doors as appropriate.
- Keep the paper shred container locked.
- Lock the office at the end of the day.
- Use common sense security.



System Controls

A key part of the HIPAA regulations is the Minimum Necessary Rule. The Security Rule supports this requirement with:

User, application and network – passwords.

Role-based access to parts of an individual’s PHI assigned to your role in the organization (role-based access control).

Password –protected screensavers.

Automatic log-off procedures.

NOTE: While it may seem inconvenient at times, it’s important to not try to bypass these controls (logging in as someone else, turning off screensavers, etc.)

Password Management

Choosing an effective password is important. It should not be easily guessed and must meet your organization’s policy and procedures. Stay away from assigning your name, name of your children, birthdays and anniversaries, pet names – anything that can be easily guessed.

To reduce the risk of hackers, de-coding your password, include upper-and lower-case characters, numbers and make it at least eight characters long.

Pick a subject that you like and can remember – maybe a sport, book or author – then use lower and upper case characters and add several numbers to it. Use things like “2” and “4” for the words “to” or “too” and “for” respectively.

If you have to write down the password in a secure place that only you can access. Never put it on your computer, under your mouse pad or in your work area (including the wall or ceiling). Change it as often as your organization’s procedures require.

Remember: Treat your computer password just like your ATM PIN. NEVER share it.

Proper Handling of ePHI & Electronic Media

Email is a common way to communicate with patients, providers, health plans and business associates. However, it carries special risks when it comes to protecting ePHI.

You would assume that all email being sent outside your facility is unprotected, and it if contains PHI, it will need some encryption to be safe.

The regulations leave the decision to encrypt up to each organization.

Refer to your internal policies and procedures to understand what is permitted for your organization (if it’s permitted at all) and what type of encryption is required. DEI requires all emails containing PHI be encrypted.

Reporting Security Incidents

Employees are the first line of defense in any organization to prevent information security breaches. Notify the Security Officer or your Information Security representative when you see something that's against policy or procedure or is an outright security violation.

Seemingly harmless acts such as sharing electronic pictures of family could accidentally introduce a virus into an organization's system. Any breach or attempted breach of your firewall, including by social media, should be reported to your supervisor.

Review your organization's specific policies and procedures on how to respond to a security incident. Contact your supervisor if you need help reporting an incident.

If you become award of a potential security breach, notify Sharron Burton, KEHP HIPAA Privacy Officer and Paula Chisholm, KEHP Security Officer immediately.

Sharron.Burton@ky.gov
Paula.Chisholm@ky.gov