Information Security Training

HIAWATHA BEHAVIORAL HEALTH

Designed for Hiawatha Behavioral Health & NorthCare Network

Meets requirement for- 45 CFR 164.308(a)(5)
Fulfills Topic Requirement: HIPPA Security Parts I, II and III

Updated 10/18/2024

Training Objectives

This training will:

- provide information about HIPAA Security requirements
- communicate the best practices for using IT resources
- review policies and guidelines relating to Information Security and Computing

After successfully finishing the training and a test, you will be credited with completing your yearly requirement for information security training.

Training Outline

1. HIPAA Overview
2. User IDs and Passwords
3. Workstation Physical Controls
4. Electronic Communication
5. Internet Use
6. Electronic Medical Record – Elmer Security
7. Data Management
8. Security of Portable Devices
9. Telecommuting
10. Reporting Security Incidents
11. Information Security Policies and Procedures

HIPAA HISTORY

- The Health Insurance Portability and Accountability Act (HIPAA) was signed into law on August 21st, 1996, by the United States Congress and signed by President Bill Clinton.

- The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

- The procedures for simplifying the administration of health insurance became a vehicle to encourage the healthcare industry to computerize patients´ medical records. This part of the Act spawned the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009, which in turn lead to the introduction of the Meaningful Use incentive program.

- The most recent legislation to affect HIPAA was the Final Omnibus Rule of 2013. The rule barely introduced any new legislation but filled gaps in existing HIPAA and HITECH regulations – for example, specifying the encryption standards that need to be applied to render electronic protect health information (ePHI) unusable, undecipherable and unreadable in the event of a breach.

What are we required to protect??

HIPAA refers to consumer/patient information as **Protected Health Information (PHI).**

PHI is confidential, personal, and ***identifiable*** health information that relates to at least one of the following:

- The individual's past, present or future physical or mental health
- The provision of health care to the individual
- The past, present or future payment for health care

"Identifiable" means that a person reading this information could reasonably use it to identify an individual. Eighteen factors can make consumer information identifiable. Here are a few of the most common:

- Name
- Address
- Birth date
- Telephone number
- Social Security number

Examples of PHI may include:

- Consumer charts (in paper form)
- A conversation between two clinicians
- Calendar entries in day planners
- Telephone conversations
- Incoming and outgoing faxes
- Clinician to consumer conversations

This training focuses on a subset of PHI called “electronic PHI”. For the proper and improper uses of PHI, please contact:

Elizabeth Eidenier (ext. 3715)
Recipient Rights Officer / Privacy Officer

Electronic Protected Health Information (ePHI)

ePHI is defined as confidential, personal and ***identifiable*** health information that is stored, transmitted or received *in electronic form*.

Healthcare organizations are required to maintain the confidentiality, integrity and availability of this information.

Examples of ePHI may include:

- Consumer information stored in ELMER.
- Consumer information being posted (transmitted) to Cafas, UPHP, etc.
- Consumer information e-mailed from one clinician to another.
- Consumer letter completed in Microsoft Word and stored in a home drive (H: Drive).
- A floppy disk or USB flash drive containing consumer data that is collecting dust on your bookshelf.
- Contact or calendar information stored on smartphones

Protecting PHI and ePHI

In reading about PHI and ePHI, you may have noticed that some information critical to Hiawatha Behavioral Health does not fit into either category.

This information may include:

Human Resource Documentation

- Employee Pay
- Employee SSN#
- Employee Disciplinary Actions

Financial Information

- Bank Routing and Transit Numbers
- Employee Deductions / Garnishments
- Employee Beneficiary Name / Address
- Employee Tax Status

It is important to understand that good practices in protecting PHI and ePHI should be applied to all categories of sensitive information at HBH.

User Credentials

User IDs are assigned to you to access the HBH's network and applications. User IDs are to be used by you and you ONLY. Sharing your user ID information undermines security of confidential information.

Auditing of computer logs will attribute all activity conducted under your user ID to you.

Do you want to be responsible for information accessed by a co-worker using your user ID?

Responsibility

The IT Department may request your username and password to resolve technical problems. This is necessary because some technical troubleshooting may require being logged into the computer *as you*. The user account is still your responsibility to protect. If a request for a username and password does not seem legitimate, you have the right and responsibility to deny the request.

The IT Department will NEVER ask you for your ELMER password. Do not give this password to anyone!

Passwords

To safeguard **YOUR** accounts, **YOU** need to take steps to protect **YOUR** password.

When choosing a password:

- Don't use a word that can easily be found in a dictionary. Words commonly found in a dictionary can be cracked in minutes.
- Don't share your password – protect it the same as you would the key to your residence. After all, it is a "key" to your identity.
- Use 13 characters at a minimum, a strong password contains Uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9) and special characters (!@#$% etc.).
- Your personal passwords (e.g. hotmail, myspace, facebook, on-line banking, etc.) should be different than the passwords you use at HBH.

Pass Phrase

A Pass Phrase is a good alternative to a complex password.

A pass phrase uses words to create a sentence—like phrase. For example, “MySummerFun95” is a pass phrase containing upper and lower characters and numbers. Unlike passwords, pass phrases cannot be found in the dictionary and are much harder to guess.

Staff members should use either pass phrases or complex passwords for HBH IT systems.

Physical control of your assigned equipment will also reduce the possibility of it being lost or stolen. Here are a few ways to maintain the physical control of your equipment:

Lock your workstation before leaving it unattended. This will prevent other individuals from accessing systems and ePHI under your User ID.

Press and Hold the "Windows Logo Key" + L on your keyboard and it will Lock your Computer

Close and Lock office doors and windows, and Lower and Close blinds in your office and shared area. These are considered the primary layers of defense against would-be robbers.

Staff must be extra vigilant in protecting laptops, tablets, or other mobile devices.

Mobile devices should never be left in a vehicle.

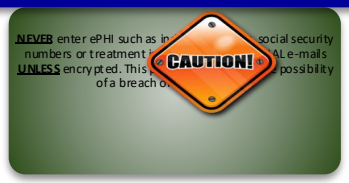
Maintain control of the key card to the building and keys to the office, cabinet or other storage area.

Safe and Secure E-mail Use

Electronic mail (e-mail) is a handy tool for communication. This tool also creates numerous risks of PHI being "leaked" outside of HBH's control. Here are a few tips to follow when using e-mail:

Using hotmail, yahoo, gmail, Charter, AT&T, or any other e-mail service for HBH business communication is **prohibited**.

Only "username"@hbhcmh.org EXTERNAL e-mail accounts shall be used for business communication.



ePHI should never be in the body of your e-mail, subject line, screenshots, or attachments.

EXTERNAL E-mail is a **prohibited** form of communication with consumers, parents and guardians **unless** the email is encrypted using Microsoft Outlook 365 e-mail encryption tool from within the Outlook 365 individual e-mail user account set up by the IT department. **ePHI should never be entered in the subject line of an encrypted email.**

However, best practice is to avoid sending ePHI in e-mail even if it is encrypted.

If you receive an encrypted e-mail containing clinically significant information, the information must be added to the clinical record.

E-mail Threats

Threats today have become more prevalent. If an e-mail or the attachment is suspicious, **don't open it!** Here are some nasty security bugs that can be transmitted via e-mail:

1. **Spam.** Unsolicited bulk e-mail, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers. **Do not reply and do not forward!**

2. **Phishing Scams.** E-mail pretending to be from trusted names such as Citibank, Paypal or Amazon; but directing recipients to rogue sites. A reputable company will never ask you to send your password through e-mail.

3. **Spyware.** Spyware/adware are software programs which can slow computer processing down; hijack web browsers; spy on key strokes and cripple computers.

   Some spyware programs, Trojan Horses, install backdoor access which allow unauthorized remote access to the infected PC by unwanted parties for malicious intent.

Text Message Use

Text Messaging (texting) is often a desired means of communication.
This tool also creates numerous risks of ePHI being "leaked" outside of HBH's control.
***** TEXTING CAN ONLY BE USED AS FOLLOWS**

Agency-issued cell phones are required for use for text messages **IF** the person served and/or parent or guardian chooses this form of communication

WITH THE 'INTENT TO' OR 'THE POSSIBILITY THEY MAY' SEND ePHI

and each have **SIGNED** an Electronic Communication Authorization (ECA) form.

TEXT MESSAGING is not a secure means of communication. Staff are required to inform the person served and/or parent or guardian who chooses to communicate via text messaging that this type of communication is not secure.

Staff may **never SEND ePHI** such as individual names or treatment information in texts.

If you receive a text message containing ePHI on

1) a non-agency device
2) an agency-issued device from a person served and/or parent or guardian who has not signed an ECA

or

any other sender

you **MUST REPORT** this to your supervisor and the HIPAA Security Officer immediately **AND INFORM THE SENDER** that this communication is prohibited.

Safe and Secure Internet Use

There are now thought to be more than 200,000 malicious programs in existence - the vast majority of which are aimed at subverting Microsoft Windows PCs. These problem programs can arrive via web browser if you visit the wrong website.

HBH blocks many harmful or inappropriate websites on the Internet. It is important to remember that many (billions!) of websites can't be instantly categorized and blocked. These sites will be readily available on the Internet. Protection of HBH electronic resources require that everyone use responsible practices when accessing online resources. Here are a few best practices:

- **Never access** sites offering questionable content. These often result in spam, viruses or spyware.
- **Never provide** sensitive or confidential information to a website that is not a trusted source.
- **Never accept** an e-mail or phone request to:
  - connect to a specific website and enter a code
  - accept a web conference invitation (such as webex, goto meeting, zoom, etc.) from an unknown entity. If you are not sure if it is a valid invitation, contact the IT department
  - give remote control of your computer without IT staff approval

  These are sure-fire means for a hacker to gain immediate remote access to your computer and the HBH network.

Web Sites

Black Listed Web Sites

These sites contain no legitimate content for HBH employees. Accessing these sites may compromise HBH equipment or consumer ePHI. Many sites in this category are blocked but some may not be restricted.

- Pornography
- Alcohol and Drugs
- Hacking
- Illegal Activity
- Hate
- Gambling
- Peer-to-Peer File Sharing (e.g., Lime Wire, Morpheus, Gnutella, Kazaa, etc.)

Gray Listed Web Sites

The content of many of these sites may be benign but may not benefit the mission of HBH. Accessing these sites are not recommended unless explicitly used for HBH work related purposes.

- Sports and Leisure
- News
- Shopping
- Video Sharing (e.g., YouTube, etc.)
- Social Networking sites (e.g., Myspace, Facebook, etc.)
- Web E-mail

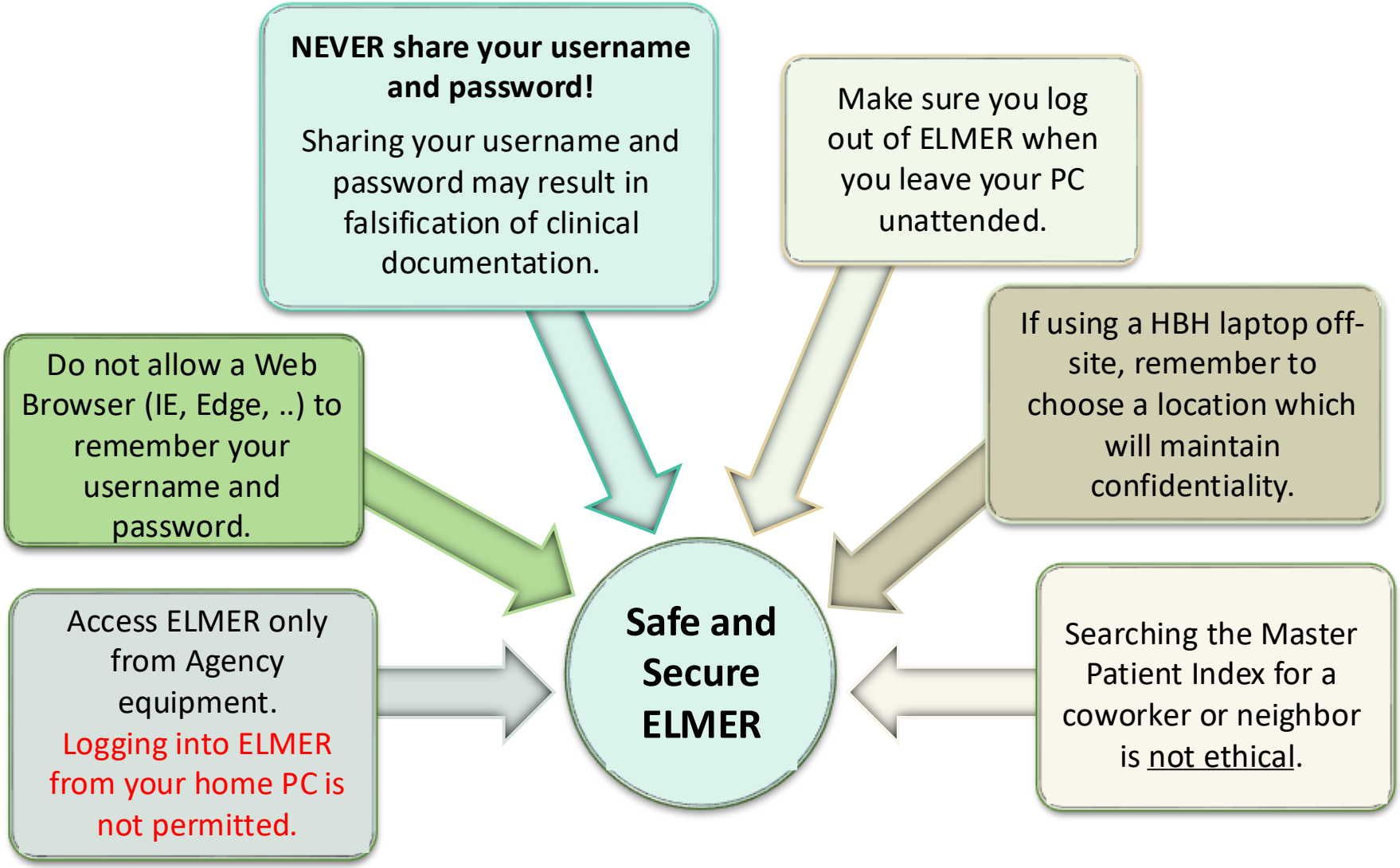
White Listed Web Sites

These types of sites are safe to access.

- Partner organization websites (e.g., MGH, NorthCare, MDCH, etc.)
- My Learning Pointe eLearning
- Any site necessary for completing your assigned job duties

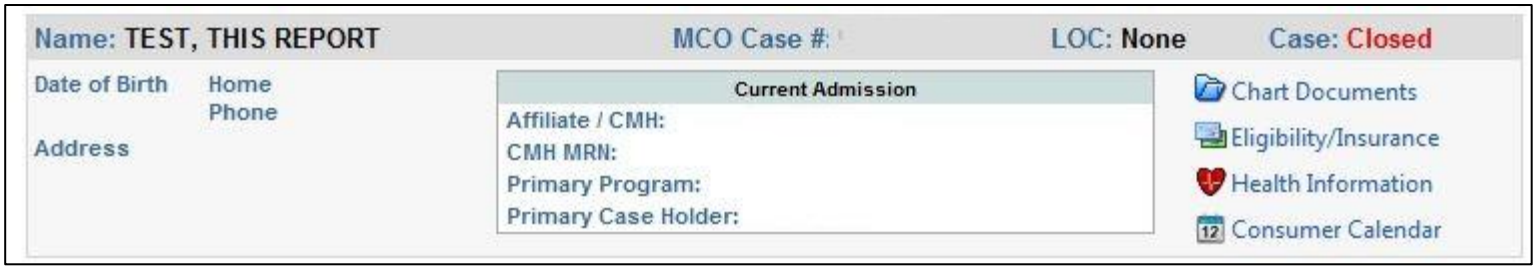
Under most circumstances, gambling sites would not be permitted for HBH employees to view. For a clinician serving a consumer with a gambling addiction, this may be a legitimate category or website to visit. If you require access to a blocked site or a category of sites, please contact the IT department.

In the age of electronic medical records, maintaining the security of ELMER is imperative. Here are a few rules to follow:



Elmer Security and Data Integrity

- Adding fake or test consumers is not permitted in the ELMER production system. Contact Elmer Support if you need assistance.



- Wondering which of your neighbors is receiving services at Hiawatha? Well, accessing charts you have no business accessing is unethical and against Agency policy. **ALL** access in ELMER is tracked and may be used in security and privacy investigations resulting in disciplinary actions.

- Uncertain on how the system functions or what you should do? Seek clarification from your supervisor.

- ELMER is an ever evolving system where new modules and functionality are added frequently. If you find that you have access to data that is beyond your authorization, please contact the Elmer Support. Your input will help to maintain the confidentiality and security of the system.

Data Management

Data Management is the development and implementation of systems, policies and procedures to effectively manage data needs of the Agency.

System back-ups are created to assure availability of ePHI in the event of a disaster or (in many cases) mistakenly deleting files. Data stored on the network shares (e.g. H:, W: drives) are backed up by the IT Department nightly.

The IT Department does NOT recommend storing files in your "My Documents" folder or on the "Desktop" of your workstation or laptop.

<u>These files are NOT backed up</u>.

In the event of your computer becoming inoperable, these files WILL be lost.

Unused or out-of-service floppy disks, CDs, DVDs, or any other data storage devices should be routed to the HIPAA Security Officer for recycling or destruction.

Data Management and Paper!

Information Security focuses on the electronic data. We need to remember that data management encompasses data in paper format too.

Transporting paper documentation in the community is common. Clinical staff have a wide array of documents containing PHI including, but not limited to; caseload “cheat sheets”, Med Data Sheets, releases, IPOSs, court documents, etc. Some departments use initials to reduce the probability of confidentiality breaches.

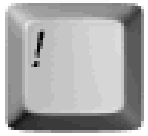
Ask yourself the following questions:

- Am I carrying only the minimum necessary consumer information in my day planner? If not, what would be the impact of losing my day planner? Can I carry less information to minimize the risk of a confidentiality breach? Can I use initials to reduce the probability of a confidential breach?
- Do I put consumer information in a locked office or locked filing cabinet at the end of the day?
- Am I carrying around clinical documentation (releases of information, court documents, etc.) in a locked case or how am I securing confidential documents?

Data Management and Devices!

- Mobile devices and portable media require extra vigilance in protecting against loss or theft. Many portable devices are small and easy to lose. To reduce the likelihood of loss or theft, the number of portable devices issued at Hiawatha is kept to a minimum.

- Employee-owned music players, cameras, laptops, flash drives, cell phones or other devices can **NOT** be connected to an Agency computer or the HBH network.



ONLY HBH ISSUED MOBILE DEVICES and PORTABLE MEDIA MAY STORE HBH INFORMATION OR BE CONNECTED TO AGENCY EQUIPMENT.






Mobile Devices

Mobile devices possess unique challenges for security and manageability!

- Files stored on mobile devices could be at risk if the device is lost or stolen.
- Many serious data breaches occur because laptops are stolen from homes, cars, airports, etc.
- Laptops disconnected from the HBH network do not receive software patches. Laptops should be connected to the HBH network at least once per week to receive the updates.
- Laptops are more delicate than a desktop PC. They require extra care. Laptops that are dropped, have a liquid spilled on them, etc. are often VERY expensive and difficult to repair. Protect these devices from damage!

What Is Telecommuting?

Telecommuting

Performing job functions with technology in varying worksites or facilities that are not owned, operated or under any control by HBH. Telecommuting may be transient in nature. Examples of worksites may include, but are not limited to, business partner facility (e.g. War Memorial Hospital, independent contractor), consumer residence, etc.

Remote Office Telecommuting

Performing HBH job functions with technology at a worksite dedicated to the HBH employee which resides outside of a HBHs' owned or operated facility. The worksite may include, but is not limited to, the employee's residence / home office.

Telecommuting continued

Telecommuting is a growing trend as clinical needs increase and telecommunication access expands.

Operating telecommuting equipment outside of a HBH facility has inherent security risks.

- There is the potential that data can be accessed while it's being sent or received from the laptop or tablet.
- 3rd party networks may not possess industry standard security measures to adequately protect your issued equipment.

In other words, telecommuting can be a hazardous affair. Here are a few precautions which will limit your risk:

- When selecting a workspace to telecommute, pick a space where you can have privacy.
- Your workspace should be quiet, clear of dirt, liquids or other debris.
- If you have been given permission to access the HBH network, choose a workspace which provides an Internet connection.

Telecommuting Authorization

Telecommuting and Remote Office Telecommuting are not universally granted to all employees. Using HBH equipment in a telecommuting fashion is **NOT** permitted unless specifically authorized by your Supervisor and the HIPAA Security Officer, **and** proper configuration of equipment has been completed by the IT Department **and** additional training has been provided.

Remote access to the HBH network or Elmer through the use of a personal device is **prohibited unless** approval has been received by the HIPAA Security Officer and a Personal Device agreement has been signed.

What is a security violation?

Here are a few examples of a security violation:

- E-mailing ePHI **to other organizations without proper encryption**.
- Transferring ePHI to a device that has not been approved by your supervisor and the HIPAA Security Officer.
- Logging into HBH's network or ELMER with **someone else's** username and password.
- **Not reporting** a security violation promptly to the HIPAA Security Officer.
- Connecting **non-HBH owned and operated hardware** to Agency equipment.
- Text messaging ePHI **to anyone**.
- Receiving text messages from person served and/or guardian or parent that contain ePHI **UNLESS** staff has received approval and receives an HBH issued texting device, an Electronic Communication Authorization has been signed by the person served and/or guardian or parent, and the ECA has been scanned into Elmer.

Consequence of a security violation

What is the consequence of a security violation?

- Loss of person served trust, employee trust, and public trust.
- Penalties, prosecution and potential for sanctions / lawsuits.
  - Anthem Inc. - $16 Million

  Anthem Inc. will pay the federal government $16 million to settle the largest health data breach in U.S. history, the Department of Health and Human Services announced. The settlement stems from a series of cyberattacks on the Blue Cross Blue Shield carrier that occurred between December 2014 and January 2015 that exposed the electronic health information of 79 million people. Anthem failed to implement appropriate measures for detecting hackers who had gained access to their system to harvest passwords and steal people's private information.
- Internal disciplinary action(s) up to termination of employment.
- Embarrassment, bad publicity, media coverage, news reports.
- Unavailability or corruption of information necessary for person served care, business, or an emergency situation.

Report Security Incidents

Reporting security incidents is required so that we can detect, prevent and mitigate security problems that pose risks to consumer privacy, availability of the information, and integrity of the data.

You are responsible for reporting security incidents as soon as possible. All reports need to be communicated to your direct supervisor and/or the HIPAA Security Officer.

When in doubt, report. As always, it's better to be safe (and secure) than sorry.

Your HIPAA Security Officer is:

Richard Gomes
635-3774
rgomes@hbhcmh.org

Policies

HBH employees are responsible for complying with all Agency policies and guidelines relating to information security. The next few slides contain an excerpt of the information security polices and procedures.

It is your responsibility to read and understand these documents in their entirety.

Information Security Policy:

Purpose: "Hiawatha Behavioral Health (HBH) shall ensure the confidentiality, integrity and availability of its information systems containing electronic protected health information (ePHI) by implementing appropriate and reasonable policies, procedures and controls to prevent, detect, contain, and correct security violations."

Sanction Policy:

Purpose: "Hiawatha Behavioral Health (HBH) staff must comply with all applicable HBH security policies and guidelines. HBH will have a formal, documented process for applying appropriate sanctions to staff who do not comply with its security policies and guidelines. Sanctions must be commensurate with the severity of the non-compliance with HBH security policies and guidelines"

HIPAA Security Guidelines

Access Control	Purpose: Develop and implement a formal process for authorizing and granting appropriate access to information systems containing ePHI. Access to HBH information systems must be limited to workforce members and third-party persons with a need for specific information to accomplish a legitimate task
Breach Notification	Purpose: Shall have a formal, documented process for notification of a breach of protected health information (PHI) that provides guidance for breach notification by covered entities when impermissive or unauthorized access, acquisition, use and/or disclosure of the HBH's client PHI occurs
Contingency Preparedness and Recovery	Purpose: Shall prepare for and be able to effectively respond to emergencies or disasters in order to protect the confidentiality, integrity and availability of its information systems
Device and Media Controls	Purpose: Electronic devices, such as servers, computers, mobile devices and removable storage media may contain electronic protected health information (ePHI). This guideline details mandatory actions to prevent the unauthorized disclosure of ePHI during the use and disposal of hardware and electronic media that contain ePHI
Electronic Mail Encryption	Purpose: Provides to staff, as deemed necessary, electronic mail (e-mail) encryption services for sending electronic protected health information (ePHI) through "external e-mail". E-mail encryption is required for all e-mail messages containing ePHI sent over "external e-mail" at HBH
Facility Access Controls	Purpose: Must appropriately limit physical access to the information systems contained within its facilities while ensuring that properly authorized workforce members can physically access such systems. HBH information systems containing ePHI must be physically located in such manner as to minimize the risk that unauthorized persons can gain access to them.

HIPAA Security Guidelines continued

Mobile Device Use	Purpose: Define standards, procedures, and restrictions for end users who have legitimate business requirements to access agency data from a mobile device connected to an unmanaged network outside of HBH's direct control.
Security Incident Response	Purpose: Shall have a formal, documented process for quickly and effectively detecting and responding to security incidents that may impact the confidentiality, integrity, or availability of HBH information systems:
Security Management	Purpose: Must ensure the confidentiality, integrity and availability of its information systems containing ePHI by implementing appropriate and reasonable controls to prevent, detect, contain, and correct security violations
Security Training	Purpose: Must develop, implement, and regularly review a formal, documented program for providing appropriate security training and awareness to its workforce members. All HBH workforce members must be provided with sufficient training and supporting reference materials to enable them to appropriately protect HBH information systems and data
Telecommunications Use	Purpose: Provide devices for telecommunication services. Telecommunication devices are defined as office phones, cell phones, smart phones, tablets, voicemail, fax machines, pagers and cellular internet cards owned or operated by HBH.
Text Messaging	Purpose: Provide an agency-issued device to personnel for text messaging and voice call purposes only. Staff issued a text messaging device shall follow standard guidelines to maintain the protection of electronic protected health information (ePHI) in regard to text messaging.

HIPAA Security Guidelines continued

Use of Electronic Mail

Purpose: Provide electronic mail ("e-mail") services. E-mail is a critical mechanism for business communications at HBH. However, use of HBH's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of HBH.

Use of Internet

Purpose: Provide access to the internet. Staff with access to the Internet must use it responsibly and consistent with their job duties and HBH's mission.

Workstation Use and Security

Purpose: workstations must be used only for authorized purposes. Workforce members must not use HBH workstations or portable computer devices to engage in any activity that is either illegal under local, state, federal, or international law or is in violation of HBH policy. Access to HBH workstations with ePHI must be controlled and authenticated

Telecommuting

Purpose: Provide staff with the ability to compete business duties while outside of a HBH office using mobile computer hardware and communication software.

Personnel Policy

Information Technology Resources

Purpose: The purpose of this policy is to set forth the agency's appropriate use of information technology (IT) resources and the agency's right to review or disclose information stored or communicated. IT resources are those facilities, technologies, and information required to accomplish information processing, storage, and communication, whether individually controlled or shared, stand-alone or networked. Included in this definition are computing and electronic communication devices and services, such as, but not limited to, computers, printers, storage devices, mobile devices, e-mail, facsimile, audio, video, and multi-media devices. Personal equipment used for agency communication is also subject to this policy.

Conclusion

As HBH employees, we are aware of the sensitivity of behavioral health information. We must be extra vigilant in our efforts to ensure that sensitive information does not fall into the wrong hands.

After finishing the following test, you will have completed Information Security Training.

Test

Upon closing this window, you will be taken to the test.