# Ensuring Privacy & Security at CMHA – CEI

Community

MENTAL HEALTH

CLINTON • EATON • INGHAM

Reviewed 09/2020

# Topics to Be Covered:

- What are privacy and security all about?
- What's confidential here?
- How can I protect confidential information?
- What should I do if I see a problem?
- How can I get more information?

# What are privacy and security all about?

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Standards for Privacy and Security

- HIPAA Privacy and Security
- ARRA HITECH
- Federal Law 42CFR Part 2
- MI Mental Health Code
- Accreditation Standards (CARF)

# What is HIPAA?

- "HIPAA" – (Health Insurance Portability and Accountability Act) is a federal law giving consumers certain privacy rights, such as
  - To look at and get a copy of their own medical and billing records
  - To ask for an amendment to these records
  - To ask for limits on how we use and release the patient's information

- HIPAA also requires healthcare organizations
  - To follow rules on use and release of consumer information
  - To keep consumer information private and confidential, safe, and accurate.
  - To continue to protect a deceased individual's personal health information for 50 years.

- HIPAA privacy rights and organization commitments are described in our "Notice of Privacy Practices." Know what's in our Notice and where to get a copy.

# What is ARRA HITECH?

The American Recovery and Reinvestment Act (ARRA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act of 2009) added new privacy regulations (*Subpart D of XIII*) regarding the electronic exchange of consumer clinical information. These regulations apply to both HIPAA and non-HIPAA entities.

# Federal Law 42 CFR Part 2

Federal Law 42 CFR Part 2 regulates access to substance abuse treatment records. 42 CFR is more restrictive than HIPAA regarding access. (Please review CMHA-CEI Confidentiality and Privileged Communication Procedure 3.3.10)

# Michigan Mental Health Code Act 258 of 1971

Michigan Mental Health Code section 748 states that mental health treatment records can only be released in certain circumstances specified in the Mental Health Code. (Please review CMHA-CEI Confidentiality and Privileged Communication Procedure 3.3.10)

# What is privacy?

- Information privacy
  - is about a person's control over their personal information
  - and the responsibilities of organizations that have personal data
- We care about everyone's privacy, but we need to take special care with our consumers.

# The connection between privacy and security

- Privacy and security are connected. We need security, especially confidentiality, in order to assure our consumer's privacy.

# What is security?

- Information security provides 3 important qualities:

1. ***Confidentiality*** – No one has access to the information unless authorized and a work-related need. Working in a healthcare organization does not entitle a person to access any and all information in an organization. You can only access information that you "need to know" to get your job done.

2. ***Integrity*** – The information can be trusted, and hasn't been changed or deleted by accident or through tampering. For example, lab results can be critical for consumer treatment.

3. ***Availability*** – Information is there when needed for work. For example, 24 hours access to clinical records (paper or electronic) is important for Crisis Services emergency care.

# Why am I reading & hearing this?

o HIPAA requires healthcare organizations to teach employees, staff, volunteers, students, residents, etc. about privacy and security so that consumer privacy is protected.

o Following good privacy and security practices is also good sense. It protects all important information at this organization.

o This training describes some key policies and what is expected of you. Each staff member is responsible for following our privacy and security policies and practices. Everyone's commitment is needed to maintain privacy and security in this organization.

# What’s confidential here?

# What is "confidential" here?

- Remember, "confidential" means people who need the information for work can get it, but others can't.
- CEI's policies protect confidential information including:
  - Consumer information
  - Some employee information – such as a person's social security number and salary
  - Certain business documents – such as business plans, legal cases, etc.
  - … and more
- Confidential information can be in any form: oral, paper, and electronic. It's in consumer and personnel records and also in conversations, phone message slips, email, faxes, laptops and thumb drives, just about everywhere!

# Confidential patient information = PHI

- In healthcare, we have always treated a consumer's medical information, such as diagnosis and test results, as confidential.
- But now HIPAA defines confidential patient information as everything about the consumer – including name, address, medical record number, and other demographic and billing information – as well as all of the consumer's medical and mental health information.
- Any piece of information that could identify a specific consumer is confidential, even if the consumer's name is omitted. For example, a consumer with a rare condition could be identified simply by that condition, and, perhaps, the month of admission or date of visit.
- HIPAA calls this <u>Protected Health Information</u> or **PHI**

# How can I protect confidential information?

# Where are the dangers?

- Natural & environmental: fire, earthquakes, power outages, burst water pipes, etc. damage confidential paper records and computer systems.  Systems may crash or "catch" a computer virus, potentially damaging information and causing systems to be unavailable when needed.

- BIGGEST threats come from **people**, both insiders and outsiders.

  - Accidents, carelessness, or curiosity lead to inappropriate conversations about consumers, unauthorized record access, failing to shred paper, or sending a confidential fax to the wrong number.

  - Deliberate actions such as using someone else's ID and password, maliciously changing or deleting data, or copying data such as consumer credit card details for identity theft.

# Practical steps for keeping information confidential and safe

- Lower your voice or have confidential conversations in a private place.
- Don't leave consumer records unattended in areas with consumers/visitors. Don't leave confidential papers on copiers, printers, fax machines.
- Always shred paper containing confidential information – including consumer information, even name and phone number – before throwing away. Shred fax machine ribbons or carbons, too.
- When faxing confidential information, always use cover sheet with a confidentiality notice, double check the recipient's fax number, and follow all procedures.

# More practical steps for keeping information confidential and safe

- Check your computer screen angle.  If visible to the public, adjust it or use a filter.
- When leaving your work area, lock up and put away confidential materials and log off, lock, or shut down your computer.
- Wear your badge and be aware of strangers who may not belong in a secured area (records file room, server room, private offices, etc.)
- Keep locked doors locked.  If you need to use a swipe card, for example, to enter a secured area, then close the door after you.  Don't allow tailgating.

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Take special care when releasing consumer information (PHI)

- Follow procedures, especially when releasing information to an outsider.  Be careful about giving out information about a consumer:
  - To someone working here
  - To family and visitors
  - To some other third party

  Remember: The receiving party **must be authorized** and have a "need to know" to obtain consumer information.

- Follow special procedures when using PHI used for research.
- Be sure you know what to do.  And follow the "minimum necessary" rule (without compromising consumer care).
- If it's not your job to give out the information, ask a manager or refer the requester to the Privacy Officer.

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Just because you *can* …

- Don’t abuse your access privileges. **Just because you can do something, doesn’t mean you’re authorized or permitted.**
- In a file room or database, only access specific records when there’s a work-related need. Example: **Consumer care staff may access their assigned consumers’ paper and electronic medical records. But they’re not permitted to access other consumers’ records, even if it’s for good intentions.**
- Administrator or super-user privileges: only use powers as required by your job. Examples: Super-users may be able to set up user accounts, but only when and as authorized. Email administrators may monitor when cause, but not permitted to browse email for non-work purposes.

# Choose good passwords and keep them secret

- Good passwords are easy for you to remember and hard for someone else to guess!

- Make up your own secret method. Pick a theme, then key phrases and initial letters. Your password will look meaningless, but you'll be able to remember it.

- Don't share your password with anyone, and don't write it down where it could be found and used. Change it whenever you think someone knows it.

- Follow standards for password length, content, and frequency of change. Be sure to use a mix of numbers, upper and lower case letters, and special characters.

- Don't use the same password everywhere – especially don't use the same password for home personal use and at work.

# Using computers and network

- Follow policies and only use work computers for legitimate business purposes. Incidental personal use is permitted as long as it doesn't interfere with job performance or affect or degrade system resources.

- Unless approved by your program director and the IS Department, don't install software or hardware on organization devices/network; don't set up web pages, electronic bulletin boards, or other public access to the network/resources.

- Our computing resources may not be used for personal or financial gain. Any activity that puts the organization at risk is prohibited unless it is documented part of the job.

- **Note: use of the organization's network & systems may be monitored.**

# Using portable computers and media

- Portables include laptops, tablets, PDAs, smart phones, CDs, flash or thumb drives, and even some MP3 players.

- Since these items are portable, they are easy to lose.  They're also high-theft items.  If lost or stolen, confidential data or access to our network could be compromised.

- No PHI data should be stored on a thumb drive, unless the drive has been encrypted to IS standards.  This is done automatically by CEI laptops, but not by other computers. **Any unauthorized use of portable  drives will be considered a privacy violation.**

- Don't leave these items unattended in your car, meeting rooms, public transportation, hotels, or elsewhere.  Lock them up and put them out of sight.

- **Any device or electronic medium that may be used to access or store confidential information must use encryption.  Protect your encryption key and keep it secret.**

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Working off-site

- If authorized and required for your job, you may work off-site, and you may need to access our network from your home or on the road. Like working with portable devices and media, working offsite carries some special risks, so it's important to follow policy.

- Don't copy and remove confidential information unless it is required by your job and has been authorized. For those authorized, IS will provide an encrypted jump drive that will "shred" electronic files when deleted. (Remember that clicking "delete" does not actually delete a file or folder.) If authorized to use jump drives, please note that they should be used to view files only and not used for moving files to a non-CEI computer.

- Transport paper documents securely. Shred paper copies containing PHI when no longer needed.

- **Transmission of confidential information over public networks including the Internet and wireless networks requires encryption. Ask for assistance from the IS helpdesk if you have questions.**

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Using email safely

- Don’t use personal email accounts (hotmail, gmail, etc.) for business, and don’t forward confidential business email to your home account. **(Setting up automatic forwarding rules from your CEI email to personal email accounts is prohibited.)**

- Be cautious about opening suspicious email and attachments since they may contain computer viruses and other malicious software. Also beware of “phishing” emails that ask you to click on a link taking you to a legitimate-looking, but fraudulent, banking or other business website where you are asked for personal information such as a bank account number, social security number, password or PIN, and so on. Legitimate organizations will not contact you this way.

- Do not use Instant Messaging or “chat” for personal or business purposes on CEI computers. **Instant Messaging on personal computers for CEI business is also prohibited.**

- Email confidential information such as PHI with care. **If the message is leaving our network, it must be encrypted.**

# Using email safely

- Any email containing consumer's personal information being sent outside our organization should be encrypted by using the word **SECURE: in the subject line**.

- As a reminder, even a simple first name is personal information. There are **18 specific types of electronic protected health information**, including patient names, addresses, Social Security numbers, email addresses, fingerprints or photographic images, among others. In addition, any past medical records or payment information is subject to the same degree of privacy protection.

- Attachments are also encrypted when using the word **SECURE: in the subject line**

# Using email safely

- Please keep in mind the following tips:

  - When replying to ALL in an email with client information ensure all recipients are using CEI email accounts, if not use **SECURE: in the subject line.**

  - When replying to an email with client information to a **NON-CEI email** account, either delete the client information prior to sending or use **SECURE:** in the subject line.

  - Check your email before sending it – if it contains client information and is being sent outside our organization, use **SECURE**: in the subject line.

- For more information, please refer to the Zix User Guide found here: http://intranet.ceicmhb/execute/reference_material.asp?SortBy=Name&StartPoint=IS Information/Training Manuals/Zix Secure Email

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# What should I do if I see a privacy or security problem?

# Mandatory incident reporting

- You must report any suspected or actual violation or breach of our privacy and security policies.

- This includes attempted or successful unauthorized access, use, disclosure, modification, or destruction of our information. It includes intrusion and interference with our computer systems.

- This also includes policy violations, even if you are unsure if the violation led to a breach. Examples includes finding consumer PHI unattended in a public area or tossing confidential papers in the waste basket instead of a shredding receptacle.

- **This organization must be able to respond whenever there is a privacy or security problem. But we may not know about it unless you report it.**

# Examples of incidents you should report

- Clinical records or documents are found in an unprotected area where they shouldn’t be
- Consumer-identifiable information is found in the trash
- A laptop, possibly containing confidential information, is stolen
- A staff member looks up a consumer in a computer system when they shouldn’t
- A computer is left logged on, “unlocked,” and the staff user has left the building
- A fax with confidential information is sent to the wrong number
- An email with consumer information is sent to a group of people when only one person should receive it
- A DVD or thumb drive with consumer information is lost
- A computer is infected with a virus

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Look for suspicious signs when you log on and use your computer

- If you share a computer, make sure you log out. Never use a computer when someone else is logged on. If you suspect someone is using your account, please notify helpdesk and change your passwords

- When you log on and there are new pop-ups or new non-CEI software that show up unexpectedly, report it. If at any point software pops up stating you are infected or if you are asked to scan your computer for viruses, do not click on anything and report this to helpdesk immediately. This could be a sign of malicious software ("malware.")

# Steps to reporting an incident

- Fill out a Privacy/Security Incident form. You can find the form by going to our Intranet Home Page and clicking on the Privacy Violation Reporting Form. Follow instructions for completing and submitting the form.

# Sanctions

- A violation of our policies can lead to a breach that has negative consequences for individuals, our consumers, and this organization.

- Therefore, when a member of our workforce is involved in a privacy or security incident, we are required by HIPAA and the HITECH Act to consider disciplinary action and further steps if appropriate. (Please review the CMHA-CEI Privacy Violations and Mitigation Policy, 1.1.17. and your employee handbook.)

- Our disciplinary actions will be based on the severity of the incident, intent, and pattern of behavior – along with fairness and consistency.

- HIPAA requires us also to consider notifying professional credentialing bodies if appropriate, as well as law enforcement and the U.S. Department of Health and Human Services. The HITECH Act requires covered entities to provide notification of a breach of unsecured information to affected individuals, the HHS Secretary, and, in certain circumstances, to the media.

- Violations of HIPAA regulations can lead to federal civil and criminal penalties including fines and imprisonment. The HITECH Act of 2009 civil penalties can range from $100 to $50,000 for each violation, with an annual cap of $1,500,000 for identical violations.

# How can I get more information?

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Questions?
# Ask us or look online.

- Our Privacy Officer is Stefanie Zin. (ext. 8193 or email zinst@ceicmh.org)

- Our privacy and security policies, forms, training materials, and Frequently Asked Questions (FAQs) are on our Intranet. Just click on "Privacy and Security" and then drill down to what you need.

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Thank you!

for completing
**"Ensuring Privacy & Security at CMH-CEI"**

You must complete the test to receive credit for this course.

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM