# CMHA-CEI Privacy and Security Training

Corporate Compliance

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# Privacy and Confidentiality: Major Governing Rules

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- There are four primary sources of rules governing the confidentiality of behavioral health records.
  - Health Insurance Portability and Accountability Act (HIPAA)
  - 42 CFR Part 2
  - The American Recovery & Reinvestment Act/The Health Information Technology for Economic and Clinical Health Act (ARRA HITECH)
  - Michigan Mental Health Code
- Some types of medical information have stricter privacy protections including:
  - HIV/AIDS/AIDS Related Condition (ARC) information
  - Reproductive Health information

# Health Insurance Portability and Accountability Act (HIPAA)

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- HIPAA is a federal law that provides privacy and security provisions for safeguarding Protected Health Information (PHI).
  - Protected Health Information (PHI) is any individually identifiable health information that is held by a covered entity or business associate in any form.
    - PHI includes medical and mental health information such as diagnosis and test results, and demographic information such as name, address, phone number, email, and consumer ID number.
- HIPAA also gives consumers certain rights such as:
  - The right to look at and get a copy of their medical and billing records.
  - The right to ask for an amendment of their medical records.
  - The right to ask for limits on how their PHI is used and disclosed.

# Health Insurance Portability and Accountability Act (HIPAA)

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- Any healthcare provider that conducts electronic transactions is considered a covered entity and must follow HIPAA.
  - Examples of covered entities include:
    - Doctors
    - Hospitals
    - Pharmacies
    - Health plans (insurance companies, Medicare, Medicaid)
    - Healthcare clearing houses (organizations that process PHI between healthcare providers and health plans)
  - Other organizations such as schools and law enforcement are not required to follow HIPAA.
- HIPAA defers to other federal or state laws that are more protective of health information or offer the consumer greater access to their health information.

# Health Insurance Portability and Accountability Act (HIPAA)

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- HIPAA has two main parts, the Privacy Rule and the Security Rule.
  - HIPAA Security Rule: "Covered entities must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits."
    - The Security Rule applies to safeguarding electronic PHI.
    - The Security Rule requires covered entities to protect against any reasonably anticipated threats or hazards and reasonably anticipated unpermitted uses or disclosures.
    - Entities must have administrative, physical, and technical safeguards, such as:
      - Administrative: policies and procedures regarding the use of electronic media that stores electronic PHI.
      - Physical: limited access to locked server rooms.
      - Technical: use of encrypted devices, automatic logouts after inactivity.

# Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA Privacy Rule: "A covered entity may not use or disclose protected health information, except as permitted or required…"
  - Use means internal review or use of PHI.
  - Disclose means release of PHI externally.
  - Uses and disclosures of PHI should contain only the minimum necessary information for the purpose of the use or disclosure and should only be used by or disclosed to those with a need to know.
    - Minimum necessary means using or disclosing the least amount of information to accomplish the intended purpose of the use or disclosure.
    - Need to know means that only those who need to know the information for the intended purpose are able to access the information.
      - As a CMHA-CEI employee, you must only access PHI when you have a valid work related reason to.
  - In general, uses and disclosures of PHI must be authorized by the consumer or their legal guardian, or required by statute.

# 42 CFR Part 2

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- 42 CFR Part 2 is a federal law that regulates the use and disclosure of substance use disorder treatment records.
  - It prohibits the disclosure of any substance use disorder treatment records without a specific release of information that is signed by the consumer or their legal guardian.
    - This includes even acknowledging that an individual is a recipient of services.
    - The MDHHS-5515 Consent to Share Behavioral Health Information is compliant with 42 CFR Part 2.
  - 42 CFR Part 2 offers greater privacy protection for substance use disorder treatment records than HIPAA, as it does not have the same exceptions to allow for use or disclosure without signed authorization from the consumer.

# ARRA HITECH

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- The Health Information Technology for Economic and Clinical Health Act (HITECH) was established as part of the American Recovery & Reinvestment Act of 2009 (ARRA).
  - The HITECH Act incentivized healthcare providers to change from paper records to electronic records.
  - It applied the HIPAA Privacy and Security Rules to business associates of covered entities, requiring them to sign Business Associate Agreements (BAAs) with the covered entity and to report any data breaches to the covered entities they contract with.

# Michigan Mental Health Code

- Michigan Mental Health Code – Confidentiality (MCL 330.1748) restricts the use and disclosure of mental health records.
  - "Information in the record of a recipient, and other information acquired in the course of providing mental health services to a recipient, shall be kept confidential and is not open to public inspection."
  - In general, information may only be disclosed with authorization from the consumer or their legal guardian.
  - The Michigan Mental Health Code does allow for disclosure for the purposes of treatment, coordination of care, or payment, without a signed authorization, in accordance with HIPAA*.

    *The Michigan Mental Health Code is more restrictive than HIPAA. HIPAA allows for the disclosure of information without authorization from the consumer for the purposes of treatment, payment, and healthcare operations (TPO). The Michigan Mental Health Code restricts healthcare operations to *coordination of care* only.*

# Other Privacy Restrictions

- HIV/AIDS/ARC
  - The Michigan Public Health Code at MCL 333.5131 requires that a consumer sign a release of information containing a specific statement if the release is to cover HIV-related information in the records before the information can be released.
    - Information related to a consumer's HIV/AIDS/ARC status cannot be used or disclosed without the specific release of information signed by the consumer or their legal guardian.
- Reproductive Health
  - The HIPAA Privacy Rule contains additional protections for PHI related to reproductive health care.
  - PHI related to reproductive health care cannot be used or disclosed for the following purposes:
    - To conduct a criminal, civil, or administrative investigation into any person for the act of seeking, obtaining, providing, or facilitating reproductive health care.
    - To impose criminal, civil, or administrative liability on any person for seeking, obtaining, providing, or facilitating reproductive health care.
    - To identify any person for the purpose of criminal, civil, or administrative liability or investigation.
  - When records containing PHI related to reproductive health care are requested, the requestor must sign an attestation that they will not use the PHI requested for the above purposes.

# Privacy and Security Safeguards

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- Use unique passwords for work that are different from those used for personal accounts.
- Never share your password with anyone.
- Lock computers and phone screens when you step away from them.
- Do not have discussions regarding consumers in hallways or waiting areas.
- When sending emails containing PHI to email address outside of CMHA-CEI, place “SECURE” in the subject line to encrypt the email.
- Do not place documents containing PHI in the regular trash, dispose of it in a locked bin for shredding.
- Retrieve documents containing PHI from printers and fax machines immediately.
- Carefully evaluate emails for their validity. Do not click links or download attachments from emails that you do not recognize or were not expecting. Report suspicious emails to IS by using the “Suspicious Email Alert” button in Outlook.
- Do not forward your work email to your personal email address.
- Double check email address and fax numbers for accuracy before sending PHI.
- Ensure your computer screen cannot be seen by those in a public area.
- Keep locked doors locked and be aware of your surroundings. Do not allow others to follow you into a secured area.

# Special Considerations for Working Off-Site

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- If you are working off-site, such as remotely or in the community, consider the following:
  - Position yourself so that others cannot see your computer screen.
  - Consider who may be able to overhear your conversations.
  - Do not leave paper documents, laptops, or other electronics unattended where others can access them. Store them securely when not in use.
  - Consider using headphones with a built in microphone when speaking with others through virtual communication channels, such as Zoom, to keep the other end of the conversation private.
  - Files containing PHI can only be placed on laptops or flash drives that have been encrypted by IS.
  - If any of your assigned CMHA-CEI equipment, such as your laptop, is lost or stolen, report it to IS as soon as you realize it is missing.

# Breach Notification Rules

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- A breach occurs when there is an unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of that information.
- Depending on the circumstances, a breach may require:
  - Notifying the consumer that their information was inappropriately released
  - Mitigation efforts
  - Notification to the local media
  - Notification to the Office for Civil Rights (OCR) and the U.S. Department of Health and Human Services Secretary.
- <u>Examples of Breaches:</u>
  - Mailing a treatment plan to the wrong consumer.
  - Viewing the chart of a consumer without a need to know.
  - Discussing consumers with others outside of work.

# Sanctions

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- A violation of confidentiality policies and procedures can lead to a breach that has negative consequences for our consumers, employees, and the agency.
- We are required by HIPAA and the HITECH Act to investigate suspected privacy violations and implement remedial action when necessary.
  - Remedial action can include additional training, changes to internal processes, and recommendations for disciplinary action.
  - Remedial action is based on the severity of the incident, intent, and pattern of behavior.
- Violations of HIPAA can lead to civil monetary penalties ranging from $100 to $1,500,000, depending on the severity of the violation.
- Severe violations that result in harm to a consumer can lead to criminal penalties including probation or imprisonment.

# Reporting

- Suspected or actual privacy violations must be reported.
- Reports can be made to CMHA-CEI's Compliance Office.
- Reports can also be made directly to the Office of Civil Rights (OCR):
  - Online: https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf
  - E-Mail: OCRComplaint@hhs.gov
  - Mail: Centralized Case Management Operations
    U.S. Department of Health and Human Services
    200 Independence Avenue S.W.
    Room 509F HHH Bldg.
    Washington, D.C. 20201
- HIPAA prohibits covered entities or business associates, including CMHA-CEI, from retaliating against any individual for filing a complaint or participating in an investigation, compliance review, proceeding, or hearing related to a complaint.

# Have Questions? Need to Make a Report?

Community MENTAL HEALTH
CLINTON • EATON • INGHAM

- Compliance Office Contacts:
  - Emily Ryan, Corporate Compliance Officer
    - Phone: (517) 346-8193
  - Virginia Kallweit, Corporate Compliance Specialist
    - Phone: (517) 237-7115
  - Email: Compliance@ceicmh.org
  - Fax: 517-237-7333

- Relevant Policies and Procedures in PolicyStat:
  - Privacy Violations and Mitigation Procedure, 1.1.04A: https://ceicmh.policystat.com/policy/18414684/latest
  - Confidentiality and Privileged Communication Procedure, 3.3.10: https://ceicmh.policystat.com/policy/17619445/latest

Community
MENTAL HEALTH
CLINTON • EATON • INGHAM

# THANK YOU!

**You have completed CMHA-CEI's Privacy and Security Training.**

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