

New York State  
Office of Mental Health

Bureau of Education  
and  
Workforce Development

HIPAA Awareness Training

This training material was prepared for internal use by the New York State Office of Mental Health (the “State”) and its employees and was not intended to serve as legal advice to any other individuals or entities.

The State expressly disclaims:

(a) any warranties or representations as to the accuracy or completeness of the information contained herein; and,

(b) any responsibility or liability to third parties who may rely upon it.

Individuals and entities who wish legal advice are advised to consult their own attorneys.

Please contact:

Counsel

New York State Office of Mental Health  
44 Holland Avenue  
Albany, NY 12229

if you wish to obtain information about, or  
permission for, the reproduction,  
distribution or use of this material.

The NYS Office of Mental Health does not discriminate on the basis of race, color, national origin, gender, religion, age, disability or sexual orientation in the admission to, access to, or employment in its programs or activities. Reasonable accommodation will be provided upon request.

# Health Insurance Portability and Accountability Act

(HIPAA)

# HIPAA Awareness Training

- Video
- Learning Guide and Activities
  - Supplemental Materials

Please Stop the Program and  
Refer to the Learning Guide for  
Learning Activity One

# Learning Objectives

- Recognize OMH policies regarding HIPAA.
- Identify the main policy reasons behind HIPAA.
- Recognize the three main areas of HIPAA: Privacy, Security, and Electronic Data Interchange transactions.

# Learning Objectives (continued)

- Understand new terms and language: e.g., Covered Entities, Business Associates, and Trading Partners.
- Identify what is expected of you as a member of the OMH Workforce.
- Recognize issues in the workplace related to HIPAA.
- Understand whom to approach for more information and assistance.

# Please Stop the Program and Begin Learning Activity Two

# HIPAA Overview

The purposes of HIPAA are to:

- Provide continuity and portability of health benefits to individuals in between jobs.
- Provide measures to combat fraud and abuse in health insurance and health care delivery.

# HIPAA Overview (continued)

The purposes of HIPAA are to:

- Reduce administrative expenses in the healthcare system; administrative costs have been estimated to account for nearly 20% of healthcare costs.
- Provide uniform standards for electronic health information transactions.
- Ensure security and privacy of individual health information.

# HIPAA Administrative Simplification Categories

- Privacy
- Security
- Electronic Data Interchange (EDI)

# HIPAA Sets National Standards for:

- Privacy of confidential health information, or what kind of information is protected.
- Security of health information, or how that information is protected via physical security, technical security and administrative security measures.
- Electronic exchange of health information.

# HIPAA Violations

- Law provides for federally imposed penalties ranging from \$100 to \$250,000 and up to 10 years in prison.
- Most severe penalties are for willful disclosure of private health information.
- OMH actions to address violations of policies and procedures related to HIPAA will be consistent with existing practices and disciplinary processes.

# Covered Entities must Comply with HIPAA and fall into Three Groups:

- **Health plans** - Insurance companies or similar agencies that pay for health care.
- **Healthcare providers** - Physicians, hospitals, or any other provider who has direct or indirect patient contact.
- **Healthcare clearinghouses** - Companies that facilitate the processing of health information for billing purposes.

# **Business Associates**

Contractors, agencies or other organizations that provide services to Covered Entities, and, in order to provide their services, need access to patient information.

# **Trading Partners**

Organizations that receive patient information via electronic transfer.

## Examples of OMH's Trading Partners:

- NYS DOH Office of Medicaid Management
- Empire Medicare

# HIPAA Applies To:

**Covered Entities** - Healthcare Providers, Health Plans, and Healthcare Clearinghouses.

**Business Associates** - Organizations or individuals working with a Covered Entity who must access patient health information in order to do their work.

**Trading Partners** - Organizations that exchange patient information via electronic transfer.

# **Please Stop the Program and Begin Learning Activity Three**

# LEARNING OBJECTIVES FOR PRIVACY

- Identify and understand terms associated with HIPAA Privacy Requirements:
  - Protected Health Information (PHI).
  - Treatment, Payment or Healthcare Operations.

# LEARNING OBJECTIVES FOR PRIVACY

(continued)

- Discuss OMH policies behind “authorization” and “Notice of Privacy Practices.”
- Recognize who is a Business Associate.
- Understand that HIPAA provides patients certain rights with respect to their PHI.

# Preemption Analysis

- Details differences between New York State Law and Federal Law
- Available through OMH Counsel's Office and on OMH's Internet site.

# A Covered Entity can only use or disclose Protected Health Information or PHI:

- For treatment, payment, or healthcare operations; OR,
- As specifically authorized by the patient in writing; OR,
- If HIPAA provides another exception.

Protected Health Information (PHI) =  
Health Information +  
Individually Identifying Information

# The General Use and Disclosure Rule:

Patient authorization is required for ALL uses and disclosures EXCEPT those for treatment, payment, or healthcare operations.

**Treatment** – Activities directly related to providing, coordinating, or managing the healthcare of patients.

**Payment** – Administrative activities associated with billing and reimbursement.

**Healthcare Operations** – Most other activities in support of core functions.

# Protected Health Information (PHI)

- PHI should be shared only with agencies and individuals who have a need for the information.
- “Minimum Necessary” Rule for PHI - Only the degree of information required should be released.

# Protected Health Information (PHI)

(continued)

- No “Minimum Necessary” restriction on release of information for treatment purposes.
- Written patient authorization is not required for purposes of treatment, payment, or healthcare operations.

# Patient Authorization

- Patient Authorization is required for ALL uses and disclosures EXCEPT those for treatment, payment, or healthcare operations.
- HIPAA provides some additional instances where patient authorization is not required.

## Some instances when patient authorization for release of health information is NOT required:

- Releases to health oversight agencies.
- For law enforcement purposes.
- For judicial proceedings.
- When otherwise required by law.

## The General Use and Disclosure Rule:

Unless the use or disclosure of PHI is for treatment, payment, or healthcare operations, patient authorization is required.

# Patient Authorization

- Part of OMH's Privacy Policy.
- “Authorization for Release of Patient Information” form in the Appendix of the OMH Privacy Policy.
- Contact your supervisor or facility Privacy Liaison with questions on use or disclosure of PHI.

# Notice of Privacy Practices (NPP)

- Developed by OMH Central Office.
- Distributed to all OMH facilities.
- Must be shared with OMH patients.
- Not required for forensic patients, but individual facilities may opt to provide NPPs to forensic patients.

# Working with Business Associates to Safeguard Protected Health Information.

# Business Associates

Organizations or individuals that provide services to Covered Entities; and, in order to provide their services, need access to patient information.

# Covered Entities

- Healthcare Providers
- Health Plans
- Healthcare Clearinghouses

# Business Associate Agreements

- Must be signed with all OMH Business Associates.
- Central Office has developed a standard Business Associate Agreement for all facilities to use.

# Patients' Rights related to PHI

- Right to access PHI.
- Right to amend or supplement PHI.
- Right to file a complaint.

# “Designated Record Set” is comprised of

- Documents containing information used to make healthcare decisions.
- Uniform case record, or any successor.
- Billing records.
- Other forms or records.
- Incident Reports are NOT part of the Designated Record Set.

# Patients' Rights to Access PHI

- Patients can be denied access to any or all of their records if it would result in harm to the patient or others.

# Patients' Right to Accounting of PHI Disclosures

- Patient is NOT entitled to an accounting of disclosures made for treatment, payment, or healthcare operations.
- Patient is NOT entitled to an accounting of disclosures that the patient allowed pursuant to written authorization.

# Patients' Right to Accounting of PHI Disclosures (continued)

- Patient IS entitled to an accounting of disclosures made
  - For purposes other than treatment, payment, or healthcare operations; or,
  - In other instances where no patient authorization is required.

See OMH Privacy Policy Patients' Rights,  
“Right to an Accounting of Disclosures”  
section for additional guidance.

# HIPAA Privacy Regulations Review

- Privacy and patient confidentiality in healthcare is not new.
- Privacy focuses on the permitted uses or disclosures of “PHI”.
- PHI is anything with both patient health information and individually identifying data.

# HIPAA Privacy Regulations Review

(continued)

- PHI Examples - admitting information, billing forms, clinical records - anything with both patient health information and individually identifying data.
- In general, patient authorization is required unless the disclosure of PHI is for treatment, payment, or healthcare operations.

# Notice of Privacy Practices (NPP)

- Written document informing patients how their PHI will be used or disclosed by OMH.
- Must be given to each patient at first time of first service delivery.
- NPP is not mandatory for forensic patients, but individual facilities may extend the right if they choose to do so.

# Business Associates

- Business Associates must agree to comply with HIPAA privacy guidelines.
- OMH enters into written agreements with each Business Associate concerning compliance with OMH privacy requirements.

# Patients' Rights related to PHI

- Right to access PHI.
- Right to amend or supplement PHI.
- Right to file a complaint.
- Patients can be denied access to any or all of their records if it would result in harm to themselves or others.

# Patients' Rights related to PHI

(continued)

- Right to an accounting of PHI disclosures EXCEPT those made for treatment, payment, or healthcare operations or where patient authorized the disclosure.

# Please Stop the Program and Begin Learning Activity Four

# Learning Objectives for Security

- Identify employee responsibilities with regard to safeguarding PHI (e.g. sharing, transmitting, printing, disposing, storing and transporting PHI).
- Understand OMH's policy regarding the use of software.

# Learning Objectives for Security

(continued)

- Explain the OMH e-mail policy as it relates to protection of PHI.
- Describe OMH's Information Security Event Response (ISER).
- Recognize how to protect a patient's PHI; when it may be at risk; and, how to ensure that privacy and security are maintained.

# OMH Security Management Framework

- **Applications** – Ensuring applications are appropriate and safe.
- **Physical** – Protecting the physical security of information (e.g., computers, files, etc.).
- **Communications** – Phones, e-mail, etc.
- **Administration** – Overall policies and procedures.

# OMH Information Security Policy

- Information is a key asset, critical to operations and patient care.
- Policy must balance privacy with sharing.
- Information takes many formats:
  - Verbal
  - Written
  - Computer (digital)
  - Voice mail and Fax

# Protecting Protected Health Information (PHI)

- When sharing PHI via telephone, verify who the other party is.
- PHI should not be left on voice mail or answering machines.
- Use only internal e-mail system, which has been secured, when sharing PHI.

# OMH Information Security Structure

- Central OMH Information Security Officer and team.
- Facility Information Security Liaisons.
- If questions, ask your supervisor or Facility Information Center Coordinator (FICC).

# Protecting Protected Health Information (PHI)

- Never include PHI in e-mail subject lines, headers, or the first few lines of the message.
- Change passwords regularly and keep them private.
- Use only OMH-trusted fax machines when sending PHI.

# Protecting PHI - Review

- When sharing PHI via telephone, verify who the other party is.
- PHI should not be left on voice mail or answering machines.
- Use only internal e-mail system, which has been secured, when sharing PHI.

# Protecting PHI - Review (continued)

- Never include PHI in e-mail subject lines, headers, or the first few lines of the message.
- Change passwords regularly and keep private.
- Use only OMH-trusted fax machines when sending PHI.

# Protecting PHI - Review (continued)

- Seek assistance from OMH Information Security Officer, Liaison or FICC.
- Additional guidance can be found in OMH's Information Security Policy and Standards.
- When printing PHI, be physically present at the printer unless the printer is in a secure OMH area.
- Clearly label all Protected Health Information as “**OMH PHI.**”

# Mailing PHI

**For Internal Mail:** Use a sealed envelope clearly labeled “Protected Health Information – To be opened by Addressee Only.”

# Mailing PHI

- **For External Mail:** If NOT intended for treatment, payment, or healthcare operations, use certified (or equivalent) mail or a bonded courier, to protect the PHI and document the disclosure.
- **For External Mail:** If intended for treatment, payment, or healthcare operations, protect PHI by taking reasonable precautions against inappropriate disclosure.

# Disposing of PHI

- Paper - Use a shredder.
- Electronic – Physically destroy the disk or cd.

# Storing or Transporting PHI

- Use a secured enclosure (e.g., store in a locked cabinet or desk, transport in a carrying case).
- When in digital format, data must be encrypted.

# For Guidance on Safeguarding PHI

- Ask for help from your supervisor, OMH Information Security Officer, Facility Information Security Liaison, or Facility Information Center Coordinator (FICC).
- Treat all PHI as if it were YOUR personal PHI.
- Talk to your co-workers and supervisors about security concerns and effective measures to maintain security.

Please Stop the Program and Complete  
Learning Activity Five

# PHI and Software Security

Do NOT install any non-OMH software including:

- Commercial software.
- Downloaded software.
- Software programs from vendors.
- Personal or “home grown” software.

# PHI and Software Security (continued)

Contact OMH Information Security Officer, Facility Information Security Liaison or Facility Information Center Coordinator (FICC) for approval and assistance prior to installing any outside software.

# PHI and E-Mail Security

- Use only OMH-approved e-mail product (GroupWise) when e-mailing PHI.
- Do NOT send PHI via e-mail to non-OMH recipients.

# PHI and your Personal Computer

Never store PHI on your hard drive. Personal hard drives have

- Limited security.
- Heightened risk of intrusion.
- No redundant back-up.

# Information Security Event Response (ISER) triggered by

- Damage to equipment, facilities, or utilities.
- Losing or misplacing computer diskettes, files, or other media containing PHI.
- Losing or misplacing removable or temporary storage devices (e.g., PDAs or “Palm Pilots”).

# Information Security Event Response (ISER) triggered by (continued)

- Inappropriate use of e-mail to send “spam” messages.
- An intrusion into OMH files, either digital or hard copy, by an unauthorized individual.

# Information Security Event Response (ISER)

Contact a supervisor, OMH Information Security Officer, Facility Information Security Liaison, or Facility Information Center Coordinator (FICC), if you suspect or know that PHI has been put risk.

# OMH Software, E-mail, and ISER Review

- **Software** - Do not install any non OMH-approved software.
- **E-mail** - Use only OMH-approved product (GroupWise).
- Do NOT use web-based e-mail systems.
- Do NOT send e-mail to outside networks unless authorized.

# Information Security Event Response (ISER) Review

- Damage to equipment or facilities.
- Losing files or computer diskettes.
- Losing temporary storage media.
- Inappropriate use of computer systems, and
- Any unauthorized intrusion into OMH information either digital or hard copy.

Please Stop the Program and Complete  
Learning Activity Six.

# General Program Review and Highlights

- An important purpose of HIPAA is to ensure patient confidentiality and safeguard patients' PHI.
- The portion of HIPAA of greatest concern to OMH employees is called Administrative Simplification.
- Administrative Simplification includes standards on Privacy, Security, and EDI.

# General Program Review and Highlights

- OMH is a Covered Entity and must comply with HIPAA.
- Business Associates require access to PHI in order to do their job.
- OMH must have Business Associate Agreements with each of its Business Associates.
- HIPAA's privacy regulations tell you what kind of information is protected – PHI.

Protected Health Information (PHI) =  
Health Information +  
Individually Identifying Information

# General Program Review and Highlights

In general, unless the use or disclosure of PHI is for treatment, payment, or healthcare operations, Patient Authorization is required.

# Patients' Rights related to PHI

- Right to access PHI.
- Right to amend or supplement PHI.
- Right to file a complaint.
- Right to an accounting of PHI disclosures EXCEPT those made for treatment, payment, or healthcare operations, or where patient authorized the disclosure.

# General Program Review and Highlights

- HIPAA's Security regulations tells you how to protect PHI.
- OMH's Information Security Policy and Standards provide additional guidance.
- OMH's Privacy Policy provides additional guidance.
- HIPAA compliance is everyone's responsibility.

# Questions about HIPAA?

Talk to your supervisor, Privacy Liaison or Officer, Information Security Liaison or Officer.

This Concludes the Video Portion of  
the HIPAA Training Program.

Please Stop the Program and Complete  
Learning Activity Seven.