

# Learning Guide

## New York State Office of Mental Health HIPAA Training Program

Developed by  
New York Wired for Education, Inc.  
in conjunction with the  
OMH Bureau of Education  
and Workforce Development

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 of 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, NYS 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.

# Table of Contents

Page

## **Introduction/Overview**

- I. Getting Started 4
- II. Conducting the Training: Facilitated Groups or Independent Learner 4
- III. Using this Learning Guide 5
- IV. Training Materials 6
- V. Training Program Objectives 7

## **Learning Activity One – Welcome** 8

## **Learning Activity Two – Identification of Learners’ Perceptions and Expectations** 9

## **Learning Activity Three – HIPAA Overview** 10

## **Learning Activity Four – HIPAA and Privacy** 13

## **Learning Activity Five – HIPAA and Security (Part One)** 18

## **Learning Activity Six – HIPAA and Security (Part Two)** 21

## **Learning Activity Seven – Wrap Up and Documentation** 23

# Introduction to the Learning Guide for the OMH HIPAA Training Program

## I. Getting Started

This document is the Learning Guide for the New York State Office of Mental Health (OMH) Health Insurance Portability and Accountability Act (HIPAA) Training Program. The Training Program consists of the following elements:

- 1) this Learning Guide;
- 2) the video portion of the program (on VHS tape, CD-ROM, or web-based streaming video); and,
- 3) supplemental materials (see pages 6-7 of this Guide under “Training Materials”).

**Please Note: The first step in the Training Program is reading this Learning Guide through page 7 and then completing Learning Activity One. PLEASE DO NOT START THE VIDEO PORTION OF THE VHS TAPE OR CD-ROM until you have done this. Following the completion of Learning Activity One, you will be directed to start the video portion of the Training Program.**

Please note that the Training Program is estimated to take approximately two and a half hours to complete.

## II. Conducting the Training

This Training Program has been designed to be taken either in a group setting (2 or more people) with one person acting as a Facilitator<sup>1</sup> or, independently, by individual Learners. The Learning Activities are written as if the training is occurring in a group setting with a Facilitator. Those Learners who are taking this training independently should ignore references to a Facilitator or group, and should complete the Learning Activities on their own, acting in effect as their own “Facilitator.” Regardless of whether the Training Program is conducted in a group or individual setting, this Learning Guide is to be used in combination with the video.

In a facilitated, group setting, the Facilitator will be in possession of this Learning Guide and will lead the Learning Activities contained within this Learning Guide. When the Training Program is taken independently, each individual Learner should have a copy of this Learning Guide to guide them through the training. Learners in facilitated, group settings may or may not be given the Learning

---

<sup>1</sup> Note that the “Facilitator” is not required to undergo any special training. Using the topics and questions provided in this Guide, the Facilitator is asked to begin, and then encourage, discussions among the Learners concerning HIPAA and related OMH policies and practices in their workplace. While no special training is required, the Facilitator should be someone designated prior to the start of the training, so he/she can review this Learning Guide to become familiar with the Facilitator’s role and responsibilities.

Guide at the start of the training, at the discretion of the Facilitator and/or those administering delivery of the training at the specific OMH facility or office. All Learners should, however, either be provided with a copy of the Learning Guide or be directed to where they can obtain or electronically access a copy for future reference.

Please note that the video is approximately 63 minutes in length and consists of the following:

- 1) HIPAA Introduction (4 minutes);
- 2) HIPAA Overview (14 minutes)
- 3) HIPAA and Privacy (22 minutes);
- 4) HIPAA and Security (Part One) (12 minutes);
- 5) HIPAA and Security (Part Two) (6 minutes); and,
- 6) HIPAA General Program Review (5 minutes).

At various points throughout the video, you will be directed to stop the video and complete “Learning Activities” that are contained in this Learning Guide. The Learning Activities are designed to reinforce the material covered in the video and to allow Learners an opportunity to discuss and consider HIPAA as it applies to their specific workplace. There are seven (7) such “Learning Activities” to complete during the Program. As noted previously, it is estimated that it will take approximately two and a half hours to complete the Training Program.

## II. Using this Learning Guide

Begin by familiarizing yourself with this Learning Guide. As mentioned, it contains seven (7) Learning Activities.

- **Learning Activity One.** This is to be completed prior to the start of the video training segment found on either the CD-ROM or on the VHS tape.
- **Learning Activity Two.** Following a brief introduction in the video segment, the second Learning Activity collects Learners’ thoughts and concerns about HIPAA.
- **Learning Activity Three.** This Learning Activity reviews the portion of the video providing an overview of HIPAA and some of the law’s important terms.
- **Learning Activity Four.** This Learning Activity reviews the portion of the video dealing with HIPAA Privacy.
- **Learning Activities Five and Six.** These Learning Activities review the portions of the video covering HIPAA Security.
- **Learning Activity Seven.** This Learning Activity provides a wrap up to the Training Program, and is the point where documentation of each Learner’s completion of the training, as mandated by HIPAA and OMH, should occur.

The video will indicate when to stop the video program and commence with each of the Learning Activities. Facilitators are to use the suggested discussion topics and questions as a means of reviewing the video instruction. During the Learning Activities, Learners should be asked to consider how HIPAA will affect their own workplace.

Those responsible for administration of the Training Program, Facilitators and Learners are encouraged to tailor the Learning Activities and discussions to their specific facility or office, or to the training group assembled. Accordingly, more or less time can be spent on Learning Activities of special relevance to a particular group of Learners.

**Please note that completing this HIPAA Training Program is mandatory for all OMH employees, regardless of job title or function.**

#### **IV. Training Materials**

The materials needed when this training is being conducted in a facilitated group or is being taken independently, are listed below. Those responsible for administering this Training Program at individual facilities and offices may also have additional facility, office and/or job function specific materials that they may wish to incorporate into this training and make available to all or select groups of Learners.

The materials needed are as follows:

- 1) This Learning Guide (As discussed above, the timing of distribution of the Learning Guide to Learners in a group setting is at the discretion of the Facilitator and/or those responsible for administering this training. Independent Learners must have the Learning Guide at the start of the training program.);
- 2) The appropriate means to view the video portion of the Training Program, e.g. a VCR, CD-ROM drive/monitor, access to the video via the Internet or local server, as determined by the individual facility or office;
- 3) Flipcharts and appropriate markers (for use by Facilitator in group settings only);
- 4) Note paper and a pen for each Learner;
- 5) Specific instructions and means to document each individual Learner's completion of this mandated training, in accordance with regularly accepted practices and procedures for such documentation and as determined and provided by those responsible for administration of mandated training at the individual OMH facility or office;
- 6) Supplemental Materials:

NOTE: In facilitated groups, each Facilitator will need copies of the following Supplemental Materials for reference/resource purposes. Copies may also be provided to Learners at the time of the training, as determined by the Facilitator and/or by those responsible for the administration of this Training at each OMH facility/office. Although it is not necessary for all Learners to have all of these materials at the time of the training, all Learners should be advised of where these materials may be obtained or accessed for future reference.

- a. OMH Privacy Policy
- b. OMH Information Security Policy
- c. OMH HIPAA Privacy Rule Preemption Analysis \*

- d. OMH HIPAA Training Video Script (text only)\*
- e. OMH HIPAA Training Video Script (text with graphics)\*
- f. OMH Privacy Liaison Functional Description
- g. OMH Information Security Liaison Functional Description
- h. PowerPoint presentation of slides contained in the video\*
- i. OMH Employee HIPAA Awareness Brochure\*
- j. Facility-specific materials at the discretion of each facility

**\*These materials can be found as PDF files on the CD-ROM containing this Training Program video and Learning Guide. Additionally, all Supplemental Materials developed centrally will be available on the OMH Internet or Intranet websites.**

## V. Training Program Objectives

At the end of the Training Program, Learners should be able to

- Understand that OMH’s commitment to quality healthcare and safeguarding patient information is supported by compliance with HIPAA and OMH policies;
- Identify the main reasons behind HIPAA, specifically, to provide continuity/portability of health benefits to individuals between jobs; to combat fraud/abuse in health insurance and healthcare delivery; to reduce administrative costs in healthcare; to provide uniform standards for electronic healthcare transactions; and, to ensure security and privacy of patient health information;
- Recognize Privacy, Security and Electronic Data Interchange or “EDI” transactions, as the three areas of HIPAA most relevant to OMH and its workforce;
- Understand significant terms and language, such as Covered Entities, Business Associates and Protected Health Information or “PHI.”
- Recognize and understand the importance of HIPAA and their individual roles and responsibilities with respect to HIPAA compliance:
  - Understand terms related to HIPAA Privacy requirements, such as “PHI” and “treatment, payment or healthcare operations;
  - Understand rules associated with the use and disclosure of patient information;
  - Discuss OMH policies behind “Authorization” and “Notice of Privacy Practices;”
  - Recognize who is a Business Associate;
  - Understand that HIPAA provides patients with certain rights with respect to their PHI;
  - Identify employee responsibilities with regard to safeguarding PHI;
  - Understand OMH’s policy regarding the use of software;
  - Explain OMH’s email policy as it relates to the 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.
- Understand where to go and whom to approach with questions or concerns about HIPAA, or for more information and assistance.

# LEARNING ACTIVITY ONE: Welcome

## Purpose/Objectives

The purpose of the first Learning Activity is to welcome Learners and to explain the general format of the Training Program.

### **Upon completion of this Learning Activity, Learners should be able to:**

- Understand the general format and length of the Training Program

## Actions

- 1) Introduce yourself, welcome the Learners to the training, and encourage Learners to introduce themselves.
- 2) Read the above objective for this Learning Activity to the Learners.
- 3) Describe to the Learners the Supplemental Materials related to this Training Program as discussed on pages 6-7 of this Learning Guide.
- 4) Let the Learners know that the video is approximately 63 minutes long and consists of the following:
  - 1) HIPAA Introduction (4 minutes)
  - 2) HIPAA Overview (14 minutes);
  - 3) HIPAA and Privacy (22 minutes);
  - 4) HIPAA and Security (Part One) (12 minutes);
  - 5) HIPAA and Security (Part Two) (6 minutes); and,
  - 6) HIPAA General Program Review (5 minutes).
- 5) Also inform the Learners that at various points, you will be stopping the video to complete “Learning Activities.” There are seven Learning Activities. The Learning Activities are designed to reinforce the material and concepts covered in the video and to solicit any inputs/questions from the Learners. Many of the questions may be answered based on the content of the video, this Learning Guide, and the supplemental materials. Learners with questions that cannot be answered should be encouraged to follow up with their supervisor, Privacy Liaison or Official, or Information Security Liaison or Officer.
- 6) Inform the Learners that it should take approximately two and a half hours to complete the Training Program (video and Learning Activities).
- 7) Review housekeeping matters such as restrooms, break time, etc. It is suggested that, when the training is delivered in group settings, a single ten-minute break be provided to Learners following the completion of Learning Activity Four.
- 8) Start the video.

# LEARNING ACTIVITY TWO: Identification of Learners' Perceptions and Expectations

## Purpose/Objectives

The purpose of this Learning Activity is to identify, acknowledge and address Learners' perceptions and expectations regarding both HIPAA and the Training Program.

### **Upon completion of this Learning Activity, Learners should be able to:**

- Understand that questions and concerns about HIPAA that remain unanswered at the conclusion of the Training Program may be addressed in the supplemental materials or the Learners can ask their supervisor, Privacy Liaison or Official, or Information Security Liaison or Officer.

## Actions

- 1) Read the above objective for this Learning Activity to the Learners.
- 2) Read to the Learners the Training Program's Objectives found on page 7 of this Learning Guide.
- 3) Discuss the following questions with the Learners and solicit their response:
  - What have you heard about HIPAA?
  - Do you think HIPAA will affect your job and if so, how?
  - What specific questions do you have regarding HIPAA?
  - What are your expectations regarding this training?
- 4) Summarize responses to the above questions on a flipchart and indicate to the group that many of these questions and perceptions should be addressed in the Training Program. These gathered responses should be saved – at the end of the Training Program, they will be used as part of a final review (Learning Activity Seven) to see if the Learners' concerns and questions have been addressed. Let the Learners know that, following Learning Activity Seven, if any of their particular questions have not been adequately covered, they should review this Training Program's supplemental materials or see their supervisor, Privacy Liaison or Official, Information Security Liaison or Officer for more detailed information.
- 5) After capturing their responses to the above questions, inform the Learners that the video will now cover an overview of HIPAA.
- 6) Restart the video.

# LEARNING ACTIVITY THREE: HIPAA Overview

## Purpose/Objectives

This Learning Activity reviews the portion of the video which provides an overview of HIPAA and discusses some important terms relevant to HIPAA.

**Upon completion of this Learning Activity, Learners should be able to:**

- State the fundamental purposes behind HIPAA.
- Recognize what the Preemption Analysis does.
- Understand that the Administrative Simplification section of HIPAA contains three standards -- Privacy, Security and EDI transactions.
- Understand that there are penalties associated with not complying with HIPAA.
- Discuss and give examples of Covered Entities, Business Associates and Trading Partners.

## Actions

- 1) Read the above objectives for this Learning Activity to the Learners.
- 2) Using the questions and material below, review the main points covered in the video with the Learners.

### **a. PURPOSES BEHIND HIPAA**

**Ask the Learners the following question:**

What are the purposes behind HIPAA?

#### **Potential Answers:**

- 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.
- 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.

### **b. HIPAA CONCERNS/MISCONCEPTIONS**

**Ask the Learners the following question:**

Were any of the concerns or misconceptions raised by Kevin in the video (listed below) similar to those held by the Learners?

- Incredibly complex law, thousands of pages in length;

- Drastically change the delivery of healthcare;
- Requires all new paperwork;
- Makes it harder for healthcare workers to discuss patient information; and,
- Patient's family members may not be able to pick up prescriptions.

Discuss other concerns raised by the Learners. Learners should be reminded of the following:

- HIPAA is a new federal law dealing with the privacy and security afforded to a patient's health information, among other things.
- Because of the health care profession's – and particularly New York State's – long-standing commitment to patient confidentiality, many healthcare workers and non-direct healthcare workers may not see a major impact on their work practices as a result of HIPAA.
- More than anything, HIPAA is an affirmation of the importance of patient privacy and confidentiality and as such, HIPAA details specific requirements to safeguard patient information.

#### **c. HIPAA VIOLATIONS**

Review that penalties and other actions may be taken in connection with instances of non-compliance. For example,

- Law provides for federally-imposed penalties ranging from \$100 to \$250,000.
- Most severe penalties are for willful disclosure of private health information.
- OMH will address violations of policies/procedures related to HIPAA in a manner consistent with existing practices and applicable collective bargaining agreements.

#### **d. PREEMPTION ANALYSIS**

Review with the Learners that in situations where both HIPAA and an existing New York State law apply, the law that will govern is whichever law provides greater rights and protections to patients.

#### **Ask the Learners the following question:**

When both HIPAA and an existing New York State law apply to a situation, is there a document which will assist us in determining which law to follow?

**Answer.** OMH has compared HIPAA with existing New York State laws regarding the protection of patient information and has detailed that comparison in a document referred to as the "Preemption Analysis." Anyone with questions regarding how HIPAA compares specifically with New York State laws, may want to review that document which is available on OMH's Internet site or through OMH Counsel's Office. Further questions can be addressed by the OMH Counsel's Office.

**e. ADMINISTRATIVE SIMPLIFICATION**

Let Learners know that the section of HIPAA of greatest concern to OMH employees is called “Administrative Simplification.” Within the Administrative Simplification section, there are three main areas:

- **Privacy**
- **Security**
- **Electronic Data Interchange or “EDI”**

**f. REVIEW OF TERMS: Covered Entities, Business Associates, and Trading Partners**

Review the following definitions of Covered Entity, Business Associate and Trading Partner with the Learners. Ask the Learners to identify examples of each.

**COVERED ENTITIES ARE:**

- **Health plans** - Insurance companies or similar agencies that pay for healthcare.
- **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 ARE:**

Contractors, agencies or other organizations that provide services to Covered Entities, and, in order to provide their services, need access to patient information – for example, an IT consultant who needs access to OMH patient information in order to test a computer system.

**TRADING PARTNERS ARE:**

Organizations that receive patient information via electronic transfer – this term is used in relation to EDI, or the electronic exchange of data portion of HIPAA – anyone to whom EDI transactions are sent, or from whom EDI transactions are received – examples of OMH Trading Partners include New York State Department of Health Office of Medicaid Management (Medicaid transactions) and Empire Medicare (Medicare transactions).

3) Restart the video.

# LEARNING ACTIVITY FOUR: HIPAA and Privacy

## Purpose/Objectives

This Learning Activity covers the fundamentals behind HIPAA's Privacy regulations and related OMH policies, procedures and forms.

### **Upon completion of this Learning Activity, Learners should be able to:**

- Identify and understand terms associated with HIPAA Privacy requirements:
  - Protected Health Information (PHI)
  - Treatment, Payment or Healthcare Operations
- Discuss OMH policies behind "authorization" and "Notice of Privacy Practices."
- Recognize who is a Business Associate.
- Understand that HIPAA provides patients with certain rights with respect to their PHI.

## Actions

- 1) Read the above objectives for this Learning Activity to the Learners.
- 2) Ask the Learners why patient privacy is so important in the provision of healthcare.

During their responses, Learners should identify and discuss situations in the workplace where patient confidentiality is an important consideration. Before and during this discussion, Learners should keep in mind that the concept of patient confidentiality is nothing new under existing New York State law, particularly with respect to the provision of mental health services. The privacy and security afforded to a patient's health information has always been a required cornerstone of OMH's mission – HIPAA does not change this commitment in any way.

- 3) Review the following concepts covered in the video with the group:

**a. PROTECTED HEALTH INFORMATION or "PHI":**

PHI = Health Information + Individually Identifying Information.

Identify some examples of PHI in the Learners' workplace.

**b. A COVERED ENTITY CAN ONLY USE OR DISCLOSE PROTECTED HEALTH INFORMATION OR "PHI":**

1. For treatment, payment or health care operations; OR,
2. As specifically authorized by the patient in writing; OR,
3. If HIPAA provides another exception.

**c. TREATMENT, PAYMENT or HEALTHCARE OPERATIONS (TPO)**

**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.

**d. When disclosing PROTECTED HEALTH INFORMATION, the following apply:**

- PHI should be shared only with agencies and individuals who have a need for the information.
- “Minimum Necessary” Rule – Only the degree of information required should be released.
- There is no “Minimum Necessary” restriction on release of information for treatment purposes.
- Written patient authorization for the use or disclosure of PHI is not required for purposes of treatment, payment or healthcare operations.

**e. PATIENT AUTHORIZATION - The General Use and Disclosure Rule:**

- Patient Authorization is required for ALL uses and disclosures EXCEPT those for treatment, payment or health care operations.
- Exceptions to General Rule: HIPAA provides some additional instances where patient authorization is not required. These include disclosures to health oversight agencies, judicial proceedings, and when otherwise required by law.

Remind Learners that the complete list of exceptions is found within the OMH Privacy Policy. Also remind Learners that the “Authorization for Release of Patient Information” form appears as an Appendix to the OMH Privacy Policy .

**f. NOTICE OF PRIVACY PRACTICES.**

Review with Learners the following points related to the Notice of Privacy Practices (NPP):

- Developed by OMH Central Office;
- Distributed to all OMH facilities;
- Must be shared with OMH patients;
- NPP included in the OMH Privacy Policy;
- Not required to be provided to forensic patients although, individual facilities may choose to do so;
- Each facility is responsible for developing its own procedure to distribute the Notice of Privacy Practice to patients and recipients of services; and,
- Every reasonable effort must be made to obtain written acknowledgement of the patient’s receipt of the notice.

4) **BUSINESS ASSOCIATE AGREEMENTS.** Review the following points from the video:

- Business Associate Agreements must be signed with all OMH Business Associates and under such agreement the Business Associate is obligated to protect PHI in the same manner as OMH would.
- Central Office has developed a standard Business Associate Agreement for facilities to use.
- If a Business Associate refuses to stop an inappropriate use or dissemination of patient PHI, then OMH and the Business Associate may not be able to continue their relationship, and in serious cases, OMH may report the problem to the Office of Civil Rights within the U.S. Department of Health and Human Services. Employees who become aware or suspect that a Business Associate has breached patient confidentiality should discuss it with their supervisor.

**Discuss with the Learners those organizations or individuals who work with OMH that would not be classified as a “Business Associate” and, therefore, do not require a Business Associate Agreement. Examples are:**

- Volunteers – treated as part of the OMH workforce.
- Contractors that do not need access to PHI to do their job – e.g., “the water cooler guy,” delivery people, etc.

5) **PATIENTS’ RIGHTS RELATED TO PROTECTED HEALTH INFORMATION.**

Review with the group the following key points regarding a patient's rights to access, amend, or supplement their Protected Health Information under HIPAA.

- Patients have the right to access their PHI, (e.g., that information comprising their “Designated Record Set”)

**Designated Record Set**

- Comprised of documents containing information used to make healthcare decisions.
- Note that it does not include incident reports.
- Patients have the right to amend or supplement PHI.
- Patients have the right to file a complaint if they find something in their PHI that they disagree with.
- Patients can be denied access to any or all of their records if it would result in harm to the patient or others.

## 6) PATIENTS' RIGHTS TO AN ACCOUNTING OF PHI DISCLOSURES.

Review with Learners that Patients are entitled to an accounting of PHI Disclosures

- **BUT NOT** for disclosures made for treatment, payment or healthcare operations
- **AND NOT** for disclosures that the patient allowed pursuant to written authorization.
- 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.
- Additional guidance may be found in the OMH Privacy Policy Patients' Rights, "Right to an Accounting of Disclosures" section.

## 7) PRIVACY LIAISONS AND PRIVACY OFFICIAL.

Review with Learners that each OMH facility has assigned staff to serve as a Privacy Liaison. If staff responsible for use or disclosure decisions have questions, they should contact their supervisor or their facility's Privacy Liaison. If the Privacy Liaison has questions, he or she should contact the OMH Privacy Official in Central Office. Every Covered Entity must have a Privacy Official; this is mandated in the HIPAA law. OMH has established a structure which includes a Privacy Official in Central Office and Privacy Liaison at each of its facilities.

A description of the "Privacy Liaison" functions has been developed by OMH Central Office and has been provided to each facility.

## 8) PRIVACY REVIEW.

During this Learning Activity, Learners have been asked to review and identify a number of HIPAA privacy requirements and related OMH policies. As a review, read the following summary of major points to the Learners:

- The importance of privacy and patient confidentiality in healthcare is not new. HIPAA reinforces many current OMH practices and policies.
- HIPAA applies to "Covered Entities" – OMH is a "Covered Entity."
- HIPAA privacy regulations focus on the permitted uses and disclosures of Protected Health Information or "PHI."
- Unless the use or disclosure of PHI is for treatment, payment or health care operations, specific written patient authorization is required.
- PHI Examples – admitting information, billing forms, clinical records – anything with both patient health information and patient identifying data.
- Notice of Privacy Practices (NPP)
  - Written document informing patients how their PHI will be used and 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 must agree to comply with HIPAA privacy guidelines; OMH enters into written agreements with each Business Associate concerning compliance with HIPAA and OMH privacy requirements.
- Patients' Rights with respect to their PHI
  - Right to access PHI.
  - Patient can amend or supplement PHI.
  - Patient can file a complaint.
  - Mental health patients and forensic patients can be denied access to any or all of their records if it would result in harm to the patient or others.
- Patient is not entitled to an accounting of PHI disclosures made for treatment, payment or healthcare operations or where patient authorized the disclosure.

8) Restart the video.

# LEARNING ACTIVITY FIVE: HIPAA and Security (Part One)

## Purpose/Objectives

The purpose of this Learning Activity is to review OMH security practices relating to HIPAA.

### **Upon completion of this Learning Activity, Learners should be able to:**

- Identify employee responsibilities with regard to safeguarding PHI (i.e., sharing, transmitting, printing, disposing, storing and transporting PHI).
- Explain OMH's e-mail policy as it relates to the protection of PHI.
- Recognize how to protect a patient's PHI; when it may be at risk; and, how to ensure that privacy and security are maintained.

## Actions

- 1) Read the above objectives for this Learning Activity to the Learners.
- 2) Review the Learners' perceptions of security. Possible questions to ask include:
  - What do you think of when you think of security?

Answers should recognize that security is not solely an information technology (IT) or computer concern but also a physical as well as administrative (policies/procedures) issue.

- Why is the protection of a patient's health information important?

Answer should realize that patients' health information is one of OMH's most valuable assets and the quality and safety of such information is key to our ability to provide healthcare. Effective treatment can only occur if patients believe that OMH will ensure proper protection to their information.

- Who is responsible for ensuring the proper security of PHI?

Answer: EVERYONE!!!

- 3) Use the following question and corresponding material below to review the security provisions covered in this portion of the video.

In each of the following areas, what security measures related to PHI do you need to remember?

Discussing PHI on the telephone;

Sending PHI via email;

Sending PHI via fax;  
Printing documents containing PHI;  
Labeling documents containing PHI;  
Mailing (within OMH and outside OMH) material containing PHI;  
Disposing of PHI; and,  
Storing/Transporting PHI.

### **Phone**

- When sharing PHI via telephone, verify who the other party is.
- PHI should not be left on voice mail or answering machines.

### **E-mail**

- Use only internal e-mail system, which has been secured, when sharing PHI.
- Never include PHI in e-mail subject lines, headers or the first few lines of the message.
- Change personal passwords in compliance with the OMH guidelines.

### **Fax Machines**

- Use only OMH-trusted fax machines when sending PHI.

### **Printing**

- Be physically present at printer unless printer is in a secure OMH area.

### **Labeling**

- All Protected Health Information should be clearly labeled “OMH PHI”

### **Mailing**

- Internal – use a sealed envelope clearly labeled “Protected Health Information – To be opened by addressee only.”
- External - use certified (or equivalent) mail or a bonded courier, when sharing PHI for purposes other than treatment, payment, or healthcare operations.
- External – if disclosure is made for treatment, payment, or healthcare operations purposes, certified mail is not required; however, use reasonable precautions to protect the PHI from inappropriate disclosure.

### **Disposing of PHI**

- Paper - use a shredder.
- Electronic - physically destroy the diskette.

### **Storing or Transporting PHI**

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

### **Getting Help on Safeguarding PHI**

- Ask for help from your supervisor, OMH Information Security Officer, Facility Information Security Liaison or Facility Information Center Coordinator (FICC).
- 4) Restart the video.

# LEARNING ACTIVITY SIX: HIPAA and Security (Part Two)

## Purpose/Objectives

The purpose of this Learning Activity is to review OMH security provisions related to HIPAA.

### **Upon completion of this Learning Activity, Learners should be able:**

- Explain the OMH software policy.
- Detail their responsibilities under the OMH Internet use policy.
- Understand OMH security policies related to computer usage.
- Describe an Information Security Event Response (ISER).

## Actions

- 1) Read the above objectives for this Learning Activity to the Learners.
- 2) Review with the Learners the following policies covered in the video:

### **PHI AND SOFTWARE SECURITY**

Do not install any non-OMH software including:

- Commercial programs.
- Downloaded software.
- Software from vendors.
- Personal software.
- Contact OMH Information Security Officer, Facility Information Security Liaison or Facility Information Center Coordinator (FICC) 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 personal computer hard drive. Computer hard drives have:
  - Limited security.
  - Heightened risk of intrusion.
  - No redundant back-up.

**INFORMATION SECURITY EVENT RESPONSE (ISER) is the OMH procedure to follow whenever someone suspects that PHI or other sensitive information has been put at risk.**

An ISER may be triggered by such things as:

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

If these or other similar situations occur, are suspected to have occurred, or are at risk of occurring, contact a supervisor, OMH Information Security Officer, Facility Information Security Liaison or Facility Information Center Coordinator (FICC) as soon as possible.

- 3) Review that the following support structure and functions exist to assist OMH employees with issues related to HIPAA security:
  - Central and Facility Information Security Officer and Liaisons
  - Facility Information Center Coordinator or “FICC”

Review with the Learners that there is a central, OMH Information Security Officer supported by a team of staff in Central Office. The OMH Information Security Officer is also supported by the network of Facility Information Security Officers or “Liaisons” at each OMH facility. Both the Central OMH Information Security Officer and facility-based Information Security Liaisons are considered Information Security Officers. They are part of the overall OMH Information Security Officer structure and function. If you don’t know who the Information Security Officer is, either your supervisor or Facility Information Center Coordinator, or FICC, will be able to help. All of these people are here to help with questions, concerns or issues related to HIPAA security.

- 4) Restart the video.

# LEARNING ACTIVITY SEVEN: Wrap-up and Documentation

## Purpose/Objectives

The purpose of this Learning Activity is to identify any remaining questions and to provide employees with additional resources to obtain more information relating to HIPAA. It is also where documentation of each Learner's completion of the training as mandated by HIPAA should occur or be confirmed.

### **Upon completion of this Learning Activity, Learners should be able to:**

- Identify any questions related to HIPAA that remain unanswered or a concern to the Learners.
- Understand that there are significant resources beyond this Training Program – supplemental materials and people – where they can learn more about HIPAA generally, about OMH's related policies, and about how their specific work practices may be affected.
- Document completion of this Training Program.

## Actions

- 1) Read the above objectives for this Learning Activity to the Learners.
- 2) Review the Learners' questions and concerns about HIPAA that were collected as part of Learning Activity Two. Determine if there concerns that have not been addressed by the Training Program. Learners with unanswered questions should be referred to the following supplemental materials identified as part of this Learning Program:
  - OMH Privacy Policy
  - OMH Information Security Policy
  - OMH HIPAA Privacy Rule Preemption Analysis
  - OMH HIPAA Training Video Script (text only)
  - OMH HIPAA Training Video Script (text with graphics)
  - OMH Privacy Liaison Functional Description
  - OMH Information Security Liaison Functional Description
  - PowerPoint presentation of slides contained in the video
  - OMH Employee HIPAA Awareness Brochure
  - Facility-specific materials at the discretion of each facility

3) Inform Learners of the following:

- Inform the Learners that all of these materials are available on the CD-ROM accompanying the Training Program or on the OMH Internet or Intranet websites. These materials are not only there to answer questions that have been raised as a result of this Training Program, but exist to provide continuing guidance on issues related to HIPAA and other workplace concerns.
- Learners should be advised that they will be kept informed if and when other centrally developed material and/or facility-specific guidance relevant to or affecting their specific job responsibilities becomes available.
- Inform Learners that OMH's Internet and Intranet websites contain HIPAA Frequently Asked Questions (FAQs) and OMH's Internet website will also have links to numerous other websites with information regarding HIPAA.
- Remind Learners that questions, now or in the future, can be directed to their supervisor, Privacy Liaison or Official, or Information Security Liaison or Officer.
- Inform Learners that, just as they frequently learn about changes in work practices or procedures in ways other than through formal training (such as advisory notices, memos, staff meetings, interactions with supervisors), they can expect to be provided with further information, instruction and direction as necessary about specific HIPAA-related changes affecting their individual work practices or procedures.

4) Document each individual Learner's completion of this mandated training, in accordance with the instructions you have received from those responsible for the administration of this training at your location.

5) Thank the Learners for their participation.