Office of Mental Health HIPAA Training Program

VIDEO SCRIPT with Graphics Included – Final

Developed by
New York Wired for Education, Inc.
in conjunction with the
NYS Office of Mental Health
Bureau of Education and Workforce Development

January 2003

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.

VIDEO	AUDIO

OMH HIPAA Training Program

Introduction (Jane)

This is an important time in healthcare. The Health Insurance Portability and Accountability Act, or HIPAA as it is commonly known, provides unprecedented patient rights and assurances for the protection of a patient's health information. For the staff of the New York State Office of Mental Health and our partners, HIPAA reminds us of our commitment to provide the best in care and services for New York State's mental health patients and service recipients. Physicians, therapists, and all OMH staff share in the administration and practice of HIPAA policy.

New York State is – and always has been - a leader in ensuring and safeguarding patient information. The trust placed in us by the residents of New York State is a responsibility we hold close, and this training program is an important step in putting that responsibility into action. I encourage all of you to engage your co-workers in dialogue regarding HIPAA. Working together, OMH staff can continue to be leaders in healthcare and among the nation's most-trusted, most-respected professionals in mental health.

VIDEO	AUDIO

Jane –
Throughout this program you will be presented with various facts behind HIPAA, the reasons HIPAA is in place, and OMH's policies concerning HIPAA.

Accompanying this program is a learning guide. At various points, you will be directed to stop the program and complete a series of learning activities. Once you've completed the learning activities, restart the program and continue.

So, what exactly will you learn in this program? After you've completed this training you'll be able to:

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.
- 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.

- Recognize OMH policies regarding HIPAA.
- Identify the main policy reasons behind HIPAA.
- Recognize the three main areas of HIPAA as privacy, security and Electronic Data Interchange transactions.
- Use new terms like 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 regarding HIPAA.

VIDEO	**AUDIO**
.	Jane – continued The training program is in three parts: This first part is an overview. When we've completed this section, you'll be presented with the details behind OMH implementation of HIPAA's privacy regulations and the final section covers OMH's approach towards HIPAA's security provisions. Whether you're a physician, clinical specialist, mental health direct care worker, medical records staff person, administrative or support staff member, HIPAA affects you and how you do your job. We'll be covering a number of terms, definitions and other issues. These will be covered in more detail further in the program.
PLEASE STOP THE PROGRAM AND BEGIN LEARNING ACTIVITY TWO	My name is Jane and I'll be leading you through this Training Program.

VIDEO	**AUDIO**
	Jane – Let's begin with a typical conversation that you could be a part of in the very near future. Hi Kevin, so what can I help you with? Kevin – I've heard some things about HIPAA, and it sounds very confusing. Jane – Well first, let me ask you what you've heard about HIPAA? Kevin – I've heard that HIPAA is an incredibly complex law, thousands of pages in length and will drastically change healthcare delivery. Jane – Okay, what else?

VIDEO   **AUDIO**

Kevin –
Well, staff will have to do just about everything differently. Agencies will have to establish entirely new contracts and paper work in order to comply with HIPAA. And I heard that nurses and others won't be able to discuss patient issues at nurse's stations or in private areas because of HIPAA or share information the way they need to.

Jane – (smiling and/or laughing) Okay…anything else?

Kevin –
I read that patients will no longer be able to have a friend or family member pick up a prescription for them.

Jane –
Thanks for that overview Kevin. What you have just shared are a number of the popular misconceptions about HIPAA. In reality, none of those statements are true! 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. HIPAA is really an affirmation of the importance of patient privacy and confidentiality and as such, HIPAA details specific requirements to safeguard patient information. Let's take a quick look at some of HIPAA's basic facts.

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.
- 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.

Jane –
The Health Insurance Portability and Accountability Act is a federal law passed in 1996. It has several purposes, among them to provide protection to people between jobs in the form of health insurance portability, and to combat fraud and abuse in health insurance and healthcare delivery. Additionally, the law seeks to reduce paperwork associated with health care, which has been estimated to be nearly 20% of all healthcare costs. To make the electronic transfer of health information more efficient, HIPAA establishes new uniform standards for sharing that information via computer. Most importantly, HIPAA provides new federal requirements to ensure the confidentiality and privacy of health information.

VIDEO	**AUDIO**
	Kevin – Well, that clears it up. I understand everything now. Jane – It's only an overview Kevin. HIPAA is a federal law that allows people to maintain their medical insurance coverage while switching jobs, but more importantly to us, it also simplifies health care administration and provides protection to health information. Kevin – Does HIPAA provide **_more_** protection than current New York State laws? Jane – Sometimes yes. Sometimes no. In some cases, New York State law and HIPAA address the same issue and they may provide different guidance. When this occurs, it is necessary to compare the laws to figure out whether HIPAA or State law is "more stringent," that is, to determine which law provides greater protection to health information. Kevin – So how do you know which law must be followed?
HIPAA Administrative Simplification Categories • Privacy • Security • Electronic Data Interchange	Jane – Well, here, it is important to remember that one of HIPAA's main purposes was to provide greater rights and protections to health care patients. So, whichever law does that - HIPAA or New York State law - is the one that applies. OMH's Counsel's office 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 a "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. Kevin – Okay, so getting back to HIPAA -- how is it organized? Jane – The area of HIPAA affecting us the most concerns the privacy and protection afforded to patient health information. This area – called Administrative Simplification – contains three standards identified as Privacy, Security and Electronic Data Interchange, or EDI for short.

VIDEO	AUDIO
	Kevin – Privacy, Security and….
	Jane – EDI, electronic data interchange. EDI is that part of HIPAA that establishes standards for transferring health information via computer. EDI is highly specialized and concerns primarily information systems professionals and those directly involved with electronic billing. This training program focuses on what every member of the workforce needs to be aware of to safeguard the privacy and ensure the security of patient health information.
	Kevin – So HIPAA has three areas: Privacy, Security and EDI.
	Jane – Right.
	Kevin – You mentioned privacy. Aren't health records already private and confidential?
	Jane – Yes, health information is confidential under New York State law, but HIPAA tells us how patient's health information can be used or shared with others, and it provides patients with certain rights concerning their health information. For example, under HIPAA, people have the right to receive written notice of how their healthcare provider can use their healthcare information.
	Kevin – And… security… what's new about security and HIPAA?

VIDEO	AUDIO
	Jane – HIPAA's security standard mandates how health information is protected. One way to think about the difference between privacy and security is this – the privacy standard allows a patient to control who has access to his or her health information. The security standard makes sure that the information is kept safe from unauthorized access, whether that information is in paper or electronic form. Each organization or entity subject to HIPAA, like OMH, is required to translate HIPAA's security standard into security practices that their own organization and their own workforce will use to keep a patient's health information safe. Kevin – Like using locked cabinets, or offices. Jane – Right. HIPAA's security standard establishes administrative, physical and technical safeguards for patient data and information. Kevin – I think I understand. What about EDI – that sounds very technical. Jane – EDI really should not be a concern to most OMH employees. At the facility level, the HIPAA EDI standard doesn't change the way patient data is entered into the OMH system. In fact, only employees within the OMH Central Office will really notice anything different – on a regular basis, they will roll-up patient and related payment data provided by OMH facilities and convert the data into the format required by HIPAA. While it won't affect the work of most OMH employees, once each organization subject to HIPAA, like OMH, makes the EDI systems adjustments it needs to make, this process is expected to save the healthcare system a great deal of money.

VIDEO	**AUDIO**

Kevin –
That's reassuring.

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.

Jane –
So, thus far:
HIPAA is a federal law that sets national standards for the privacy of health information or what kind of information is protected, the security of health information, or how that information is protected, and it sets national standards for the electronic exchange of data.

Kevin –
Before we get into more specifics Jane, I've got one more question.

Jane –
Sure.

Kevin –
If HIPAA is a law, then . . . there must be penalties for not following it. Are OMH employees at risk for not following HIPAA?

HIPAA Violations

- Law provides for 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.

Jane –
Depending on the severity of the offense, penalties for not following HIPAA regulations can be as much as $250,000 and 10 years in prison.

Kevin –
Wow! This is serious!

Jane –
Protecting patient healthcare information is serious. The most severe penalties are for those incidences when an individual ***willfully*** discloses private health information. For example, if someone disclosed private health information in return for payment or for commercial advantage, he or she could face a $250,000 fine and ten years in prison.

Kevin –
What if someone simply makes, you know, an "honest mistake?"

VIDEO	**AUDIO**
	Jane – That's one of the main reasons we are here today, Kevin. Every OMH employee has a role in protecting patient privacy. Protecting that privacy means that all staff need to follow OMH policies and procedures. In the event an employee does not follow procedure or policy, the response will be consistent with existing practices. For example, the response could include verbal or written counseling or disciplinary action, including penalties based on the severity of the violation. And, penalties could range from reprimands, through fines or suspensions without pay, to termination of employment. Actions taken by OMH in any such cases will be consistent with existing practice and disciplinary processes contained in applicable collective bargaining agreements.

VIDEO

AUDIO

Kevin –
Thanks, Jane – it's good to know that. Now let me ask about who and what organizations HIPAA applies to. Does HIPAA apply to everybody? I mean, do these new privacy and security regulations affect everyone?

Jane –
HIPAA policies and procedures affect virtually everyone and every organization working in healthcare. Certainly, some individuals and businesses will be affected more than others.

Kevin –
Like who?

Jane –
Generally, individuals or organizations involved with the provision and/or administration of healthcare must comply with HIPAA. You may have heard the term "Covered Entity." Covered Entity is the term used by HIPAA to define who must comply with HIPAA requirements.

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

Kevin –
I have heard that term. What is a "Covered Entity?"

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.

Jane –
Simply put, Covered Entities are those organizations that must comply with HIPAA. They fall into three groups:

Covered Entities include health plans such as insurance companies or similar agencies that pay for health care.

Covered Entities include most healthcare providers like hospitals, physicians or outpatient health programs who have direct or indirect patient contact that use electronic transactions to engage in the business of health care, such as to do their billing.

The last group of Covered Entities is healthcare clearinghouses. These are companies that facilitate the processing of health information for billing purposes.

VIDEO	**AUDIO**
	Kevin – So the Office of Mental Health would be a Covered Entity because OMH operates a number of psychiatric centers.
	Jane – That's right. Throughout this training and while discussing HIPAA, you will hear the term "Covered Entity" quite often.
	Kevin – Another term that I have heard being used is "Business Associate." What are they?
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.	Jane – Business associates are contractors or organizations that provide services for or on behalf of a Covered Entity like OMH and in order to provide their services they need access to patient information. For example, some OMH contractors, depending on their need to access patient information, may be classified as Business Associates.
	Kevin – Like an IT consultant who needs access to OMH patient information on our computers in order to test the system might be a Business Associate?
	Jane – Right. Since they need access to patient information to do their job, they would, under those circumstances, be Business Associates.
	Kevin – What about physicians who some of our OMH patients are referred to for things like emergency or dental care?
	Jane – Generally, doctors who provide patient care are Health Care Providers, so under those circumstances, the doctors would be Covered Entities – not Business Associates – and therefore as Covered Entities, HIPAA directly applies to them.
	Kevin – How about the guy who fills the water coolers on a patient ward?

VIDEO	AUDIO
	Jane –
	Well, since that contractor does not need patient information to do his job, he is NOT a Business Associate. Business Associates are those contractors or organizations that must have access to patient information in order to do their job.
	Kevin –
	In our facility, we have many people like students, interns or volunteers that work alongside us. Are people like this, you know, people who work with us, but aren't OMH employees, are these individuals Covered Entities or Business Associates?
	Jane –
	For the purpose of HIPAA, students, interns or others that function under the direction of OMH are considered part of the OMH workforce. So, these individuals are part of a covered entity and must abide by all HIPAA regulations just as if they were OMH employees.
	Kevin –
	What's the big deal about being a "Business Associate?"
	Jane –
	A Business Associate, even though it may not be a Covered Entity, still must agree in writing to safeguard patient information. OMH, as the Covered Entity, must ensure that written agreements are in place with its Business Associates. These agreements are called "Business Associate Agreements" – we will discuss them some more later on.
	Kevin –
	OK, I guess it does make sense that OMH has to ensure that everyone who needs patient information to do their job must properly safeguard it.

VIDEO	**AUDIO**
	Jane – Right. Kevin, let me ask you another question. Does the term "Trading Partner" mean anything to you?
	Kevin – No. What's that?
Trading Partners – Organizations that receive patient information via electronic transfer.	Jane – A "Trading Partner" is another term that you may hear related to HIPAA. It is used in relation to the EDI, or the electronic exchange of data portion of HIPAA, and "Trading Partner" simply refers to an organization that receives EDI transactions. OMH, and anyone OMH sends EDI transactions to, or receives EDI transactions from, could be called a "Trading Partner." Most "Trading Partners" are covered entities, under HIPAA, in their own right. In New York State, the main Trading Partners of the public mental health care system are the Department of Health's Office of Medicaid Management for Medicaid and Empire Medicare for Medicare transactions. In Trading Partner agreements, the parties agree to use only the standard electronic transactions, in effect, a standard "vocabulary," when they engage in electronic transactions with one another.
Examples of OMH's Trading Partners:	
• NYS DOH Office of Medicaid Management.	
• Empire Medicare.	Kevin – So there are at least three types of organizations that are either directly or indirectly covered by HIPAA.

VIDEO	AUDIO
HIPAA APPLIES TO:	Kevin –
Covered Entities: Healthcare Providers, Health Plans, and Healthcare Clearinghouses.	The first group is referred to as Covered Entities. These are healthcare providers, like physicians, and hospitals, health plans, or healthcare clearinghouses.
Business Associates: Organizations or individuals working with a Covered Entity who must access patient health information in order to do their work.	Jane – Right. Covered Entities are directly responsible for complying with all of the HIPAA requirements. The Office of Mental Health, including all of its inpatient and outpatient facilities, is a Covered Entity.
Trading Partners: Organizations that exchange patient information via electronic transfer.	Kevin – Next are Business Associates. These are organizations or individuals who work with a Covered Entity and during the course of the contract, these Business Associates come into contact with patient information in order to do their work.
	Jane – Right again. They are indirectly covered by HIPAA pursuant to a Business Associate Agreement with a Covered Entity.
	Kevin – The third group is Trading Partners. Trading Partners are organizations that exchange patient information in order to conduct an electronic transaction for certain business purposes.
	Jane – And the New York State Department of Health is responsible for managing Medicaid in New York and, therefore, is a good example of a Trading Partner. Similar to Business Associates, they are, as Trading Partners, indirectly covered by HIPAA pursuant to a Trading Partner Agreement. Although, many are in fact Covered Entities in their own right, in which case HIPAA would apply to them directly.
PLEASE STOP THE PROGRAM AND BEGIN LEARNING ACTIVITY THREE	Kevin – Thanks, Jane. It's starting to make more sense.

VIDEO	AUDIO
	Jane – Hello again. So far, we've covered just the basics of HIPAA including Privacy, Security, EDI and those groups or individuals covered or affected by HIPAA like Covered Entities, Business Associates and Trading Partners.
	Kevin – I'm still not sure how HIPAA will change my job, or what I'm supposed to be doing differently.
	Jane – That's okay. It's important to have a good overview of and appreciation for HIPAA in general. Now, we're going to explore HIPAA's privacy standard.
	Kevin – I'm ready.
	Jane – Let's get started.

LEARNING OBJECTIVES FOR PRIVACY
• 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 certain rights with respect to their PHI.
	When we're finished with this section, you will be able to:
	• Identify and understand terms associated with HIPAA's privacy requirements such as Protected Health Information or PHI and the phrase "treatment, payment or healthcare operations".
	• Discuss the policy behind "authorization" and "Notice of Privacy Practices."
	• Recognize who is a Business Associate.
	• Understand that HIPAA provides patients certain rights with respect to their Protected Health Information

	Kevin – Before we start, I have a question.
	Jane – Sure.

VIDEO   **AUDIO**

Kevin –
Privacy of patient information is not new. Everyone working in healthcare from support personnel to clinicians already protects patient information. During orientation, employees receive training on the importance of privacy. How is what we're about to cover any different?

Jane –
Good question. You're right Kevin. The concept of patient confidentiality is nothing new under existing New York State law, particularly with respect to mental health. Revealing that an individual is receiving mental health services risks more than simply breaking confidentiality. Effective and lasting therapy can often only occur in an environment of confidentiality and trust.

Kevin –
Right. So how does HIPAA change this?

Preemption Analysis

- Details the difference between New York State Law and Federal Law.

- Available through OMH Counsel's Office and the OMH Internet site.

Jane –
It really doesn't – the privacy and security afforded to certain types of health information has always been at the cornerstone of OMH's mission – HIPAA does not change this commitment in any way. However, for the first time, HIPAA establishes at the federal level a set of rights that individuals have regarding the disposition or sharing of their health information. Some of HIPAA's rights and protections were not covered under existing New York State Law and some are more or less stringent than what New York State law already provided. As we discussed earlier, the differences between HIPAA and New York law are spelled out in the "Preemption Analysis" which is available through OMH Counsel's Office and on OMH's Internet site.

Kevin –
So, under HIPAA, do people have the right to know who gets their patient information?

.

VIDEO	AUDIO
	Jane – Yes. As a general rule, unless the patient gives express permission, a Covered Entity can only use or disclose protected health information for treatment, payment or healthcare operations purposes. Otherwise, with a few specific exceptions, any use or disclosure must be specifically authorized by the patient in writing. In other words, individuals generally have the right to control their personal health information and covered entities…
A Covered Entity can only use or disclose Protected Health Information or PHI: • For treatment, payment or health care operations; OR, • As specifically authorized by the patient in writing; OR, • If HIPAA provides another exception.	
	Kevin – Covered entities like OMH….
	Jane – Right, covered entities like OMH have the duty to guard protected health information. And HIPAA extends that duty to each member of a Covered Entity's workforce – that's why it is so important that all employees know and understand what HIPAA is all about.
	Kevin – There's that term again. What exactly is "protected health information?"
Protected Health Information (PHI) = Health Information + Individually Identifying Information.	Jane – Protected health information, or its abbreviation "PHI," is any type of health information that contains something that could identify the individual.
	Kevin – What are some examples of PHI?
	Jane – Patient notes and records, pharmacy information, billing information, background and histories would all be examples of PHI.
	Kevin – And, under HIPAA, what sorts of things should OMH employees know about using or disclosing a patient's PHI?
	Jane – "Use PHI," you mean as in within OMH?

VIDEO	**AUDIO**
	Kevin – Right. And "disclose PHI" as in when someone has to share a patient's PHI outside OMH like with another agency.
The General Use and Disclosure Rule:	
Patient Authorization is required for ALL uses and disclosures EXCEPT those for treatment, payment, or healthcare operations.	Jane – OK. Well the key point for all OMH employees to remember, and the General Use and Disclosure Rule, is that unless the patient has provided his or her specific written permission, protected health information can be used or disclosed only for treatment, payment or healthcare operations.
	Kevin – Excuse me Jane, but treatment, payment or healthcare operations sounds kind of broad.

VIDEO	AUDIO
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.	Jane – Treatment refers to those activities directly related to providing, coordinating or managing the healthcare the patient. It also includes the referral of a patient from one healthcare provider to another. "Payment," as you might suspect, are the various administrative activities associated with billing and obtaining payment or reimbursement from insurance companies, Medicaid or Medicare. Examples of healthcare operations are maintaining medical records, quality management reviews, discharge planning-all of the things that OMH must do to support its core functions of treatment and payment. In other words…things it must do to keep its hospitals "operating."
	Kevin – Can we still get patient information from providers OMH regulates?
Health Oversight Agency	Jane – Yes. In addition to being a Covered Entity, OMH is a "health oversight agency." HIPAA allows covered entities, like those providers we license or fund, to continue to provide us with any patient information that we, as a "health oversight agency," need in order to oversee the public mental health system.
	Kevin – So, who can OMH employees share PHI with?

VIDEO	AUDIO

Jane –
Only with those individuals or agencies that have an operational need for the information.

PROTECTED HEALTH INFORMATION

Kevin –
Is there any limit on how much PHI can be released?

- PHI should be shared only with agencies and individuals who have a need for the information.

Jane –
Another good question. Not only HIPAA, but both New York State Law and OMH policy direct that only the minimum amount of information required be released when it is being shared for purposes other than for treatment. This is called the "Minimum Necessary" rule. For example, an insurance company may only need certain sections of a patient's entire treatment record in order to determine if payment for a particular service can be made. However, the "minimum necessary" rule doesn't apply to the use or disclosure of health information for treatment purposes, because healthcare providers need to have access to complete health information in order to provide quality care.

- "Minimum Necessary" Rule for PHI – Only the degree of information required should be released.

- 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.

Kevin –
Does the patient have to authorize the release of this kind of information?

Jane –
No – as long as the use or disclosure is for treatment, payment or healthcare operations. However, remember… The General Rule is that patient authorization is required for other types of use or disclosure.

PATIENT AUTHORIZATION
- Patient Authorization is required for ALL uses and disclosures EXCEPT those for treatment, payment, or healthcare operations.

Kevin –
Such as…

- HIPAA provides some additional instances where patient authorization is not required

Jane –
Such as most research studies. All research must be approved by an Institutional Review Board which assures, among other things, that an appropriate authorization is included as part of the study. In some instances, the law provides that an authorization is not required. For example, in the case of research involving deceased patients, an authorization may not be required.

Kevin-
You mentioned before that there are some other "exceptions" to the General Rule? Other times when we are able to disclose health information for reasons other than when it's needed for treatment, payment or

healthcare operations purposes?

VIDEO	**AUDIO**
	Jane-
	Yes. Other examples of when a patient's authorization is not required include releases to health oversight agencies, for law enforcement purposes, for judicial proceedings, and when otherwise required by law – and this is not really any different than before HIPAA; it is similar to what existing New York State law had already provided.

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.

Kevin-
Well, it sounds like it could be a bit confusing.

Jane-
It may help to think of them in this way…many of the exceptions relate to the public responsibilities of a Covered Entity, like OMH… for example, to report child abuse or certain communicable diseases to the Department of Health.   Another important exception allows us to disclose information to Law Enforcement officials, for purposes such as identifying or locating someone suspected of a crime or a missing person. HIPAA also allows us to disclose protected health information about our forensic patients to correctional institutions or to law enforcement in order to provide care to them or ensure the safety of our patients. We can also disclose PHI if we are ordered by a court to do so, or if the use or disclosure is required by law.   There are other exceptions which allow us to disclose information to family members without express patient authorization, but in that case we must give the patient the opportunity to agree or object to the disclosure.

Kevin-
Thanks. Those examples do help.

Jane-
And, a complete list of exceptions is contained in the official OMH Privacy Policy.

Kevin-
Well, with all of the discussion of exceptions, you'll be happy to know that I still remember the General Rule, Jane.

General Use and Disclosure Rule:
Unless the use or disclosure of PHI is for treatment, payment, or healthcare operations, a patient authorization is required.

Jane-
Which is?

Kevin-
That unless the use or disclosure of Protected Health Information is for treatment, payment or health care operations, you must obtain a written authorization.

VIDEO	**AUDIO**
	Jane- VERY good, Kevin.
	Kevin – Okay, so protected health information can only be released to those individuals and organizations that have a need for it and only when it is required for the treatment of the patient, payment for services and healthcare operations. The information released should only be the "minimum necessary," unless, of course, it is for treatment purposes where there is no such "minimum necessary" restriction. For all other types of uses or disclosures, except as specifically provided by HIPAA, the patient must provide written authorization to release his or her PHI.
PATIENT AUTHORIZATION • Part of OMH's Privacy Policy. • "Authorization for Release of Patient Information" form in the Appendix of OMH Privacy Policy • Contact your supervisor or Facility Privacy Liaison with questions on use or disclosure of PHI.	**Jane –** The OMH Privacy Policy defines specifically those criteria to which staff responsible for making decisions about the use or disclosure of PHI should refer. To make implementation of this requirement easier, OMH has developed a simple form for patients to sign. The "Authorization for Release of Patient Information" is found in OMH's Privacy Policy. 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.
	Kevin – All of these practices are in place to protect patients' privacy. . .
	Jane – That's right.
	Kevin – But how will a patient know what his or her rights are?

VIDEO	**AUDIO**
	Jane – Mmmm…good question. Under HIPAA, all patients must receive a copy of a facility's privacy practices. This is called a "Notice of Privacy Practices."
	Kevin – What's that?
.	Jane – A "Notice of Privacy Practices", or "NPP" for short, is a document stating an organization's privacy practices. It provides the patient with an overview of how that organization protects his or her PHI.
	Kevin – So…who has to write the NPP?

VIDEO	**AUDIO**

	Jane – OMH's privacy policy includes a Notice of Privacy Practices as an appendix – this is available to each facility and office. It is the responsibility of individual facilities to establish a procedure to distribute the Notice of Privacy Practice to patients and recipients of services.
NOTICE OF PRIVACY PRACTICES • Developed by OMH Central Office. • Distributed to all OMH facilities. • Must be shared with OMH patients.	
	Kevin – So, the OMH privacy policy includes the Notice of Privacy Practices and individual centers will establish a procedure for providing it to patients.
	Jane – Correct. Every reasonable effort must be made to obtain written acknowledgement of the patient's receipt of the notice.
	Kevin – Must all patients receive a Notice of Privacy Practices? OMH has some patients who are being treated as a result of a criminal court order or are otherwise incarcerated. Do they have the same right under HIPAA?
NOTICE OF PRIVACY PRACTICES • Not required for forensic patients, but individual facilities may opt to provide NPPs to forensic patients.	Jane – Our forensic patients ***do not have a legal right*** to receive a Notice of Privacy Practices under HIPAA. However, individual OMH sites ***may opt to provide their forensic patients with NPPs.***

VIDEO	AUDIO

Working with Business Associates to Safeguard Protected Health Information.

Kevin –
All right Jane, we've talked about Protected Health Information and how the OMH Privacy Policy sets standards for protecting patients' records.

Jane –
Right.

Kevin –
But OMH works with so many different providers, contractors and vendors. How can we ensure that patients' private medical records are protected by all of our partners?

Jane –
What you're talking about, Kevin, are Business Associates. Remember, Business Associates are entities providing services for, or on behalf of OMH that involve access to PHI.

VIDEO	**AUDIO**
	Kevin – Remind me again about the difference between a Business Associate and a Covered Entity . . .
Business Associates – Organizations or individuals that provide services to Covered Entities; and, in order to provide their services, need access to patient information.	Jane – Sure. A Business Associate is any individual or organization that works for, or on behalf of a Covered Entity, like OMH and has to have access to Protected Health Information in order to provide that service. Some examples would be lawyers or accountants, or certain consultants. Remember, Business Associates are often not Covered Entities and therefore, HIPAA may not directly apply to them.
	Kevin – And a Covered Entity is…
Covered Entities: • Healthcare Providers. • Health Plans. • Healthcare Clearinghouses.	Jane – Covered Entities are individuals or organizations that provide care, like doctors or medical groups; organizations that pay for healthcare like insurance companies; or, companies that administer healthcare information, like healthcare clearinghouses. HIPAA directly applies to all Covered Entities.
	Kevin – So, how will OMH ensure patient confidentiality among all of its Business Associates?
	Jane – OMH may disclose PHI to a Business Associate if OMH first obtains adequate assurance that the Business Associate will safeguard the PHI in accordance with HIPAA requirements.
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.	Kevin – In other words, Business Associates can receive PHI as long as they sign an agreement that stipulates they will protect PHI in the same manner as OMH would.
	Jane – Correct. And OMH Central Office has developed a standard Business Associate Agreement that satisfies this new regulation.
	Kevin – What would happen in the unlikely event that a Business Associate does not follow OMH policy in regards to protecting a patient's PHI?

VIDEO	**AUDIO**
	Jane – As a Covered Entity, OMH is required to take steps to remedy any known breaches of patient confidentiality. If a Business Associate refuses to stop the 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.
	Kevin – Should psychiatric centers and individual OMH sites have Business Associate agreements with all its vendors? What about contractors that simply deliver food or office supplies?
	Jane – Contractors and vendors who do not need access to PHI in order to provide their service to OMH are not "Business Associates" and therefore, Business Associate Agreements are not needed.
	Kevin – So the guy who refills the water cooler is not a Business Associate, but the medical lab that we send our patient's blood sample to for analysis would be.
	Jane – That's right.
	Kevin – So the watercooler guy doesn't need access to PHI to do his job -- but suppose he's in our facility and he happens to see information about a patient. What happens then?

AUDIO	**VIDEO**
	Jane – Like every mental health facility, OMH has a responsibility to adequately safeguard patient information. However, under those circumstances if a vendor or contractor happens to come across patient information incidentally, either directly or indirectly, they should treat it as confidential. And it's the individual OMH facility's responsibility to inform all of its contractors of their duty to protect patient information.
	Kevin – So if a Business Associate is working with PHI, they must sign a Business Associate Agreement. All other contractors or vendors should be made aware that if they or anyone working for them comes into contact with a patient's PHI, they must treat it as confidential.
	Jane – Good summary Kevin.
	Kevin – Thanks. It is beginning to make sense. Now, we've been discussing OMH's procedures for protecting a patient's PHI. But what about the patient's right to access or view his or her own PHI?

VIDEO

AUDIO

Patients' Rights related to PHI
- Right to access PHI.
- Right to amend or supplement PHI.
- Right to file a complaint.

Jane –
Under HIPAA, patients can access and amend or supplement their Protected Health Information, and the law provides patients the right to file complaints if they find something in their PHI that they disagree with. Patients also have the right to access their records, that is, information in their Designated Record Set, although that right can be restricted under certain circumstances.

Kevin –
What is a "Designated Record Set?"

Designated Record Set Comprised of
- Documents containing information used to make healthcare decisions.
- Uniform case record, or any successor.
- Billing records.
- Other forms or records.

Jane –
The "Designated Record Set" is a term used in, and defined by, the HIPAA regulations – it is comprised of all the documents that contain information used to make healthcare decisions. For OMH's purposes, that generally means the billing record and the clinical record information contained in the Uniform Case Record. If a facility uses additional or modified forms to record information to make healthcare decisions, that would also be included in the Designated Record Set.

Kevin –
What about incident reports?

Incident Reports are NOT part of the Designated Record Set.

Jane –
Good point – incident reports are not considered part of the Designated Record Set.

Kevin –
So, are you saying that for the first time, mental health patients are going to be able to see what is in their medical record?

VIDEO

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 heathcare operations.

- Patient is **NOT** entitled to an accounting of 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.

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

AUDIO

Jane –
Although this is a new right in some states, it is not new in New York State. Patients have been able to access their mental health treatment information for some time now. HIPAA also makes provisions regarding a mental health patient's right to access his or her PHI. Similar to New York State Law, access can be denied if there is a reasonable likelihood that allowing access would endanger the life or physical safety of the individual or another person. And, like New York State law, under HIPAA, forensic patients can be denied access to their PHI if such access would place others in danger.

Kevin –
I've heard that at any time a patient wants to know who has seen his or her PHI, we have to tell them. Wouldn't that mean we would have to record every single use and disclosure? That seems like a paperwork nightmare!

Jane –
What you're talking about Kevin is a "right to an accounting of disclosures." If a patient requests to know who we have disclosed their information to over the past six years, we have to tell them. But there are a lot of exceptions. We don't have to account for disclosures made for treatment, payment or healthcare operations, nor do we have to account for disclosures made where the patient already gave his or her written authorization. But, we do need to account for other disclosures which are not for treatment, payment or health care operations or where no patient authorization is required such as those made to law enforcement authorities or health oversight agencies such as the Joint Commission on the Accreditation of Healthcare Organizations or to the Commission on the Quality of Care for the Mentally Disabled.

VIDEO	AUDIO
.	

HIPAA PRIVACY REGULATIONS REVIEW

VIDEO	AUDIO
	Jane – Time to review HIPAA privacy regulations.
Privacy or patient confidentiality in healthcare is not new.	Kevin – We began by stating that an individual's right to privacy in regards to healthcare is a long-standing principal. What's more, especially with respect to mental health, confidentiality is required for the patient to feel safe and maintain trust with his or her caregivers.
	Jane – That's a good point Kevin. And HIPAA reinforces those rights by allowing patients the right to know who is getting their health information.
Privacy focuses on the permitted uses or disclosures of "PHI."	
PHI is anything with both patient health information and individually identifying data.	Kevin- The privacy regulation applies to Protected Health Information, or PHI for short. PHI is any kind of health information that is accompanied by individually identifying information such as a person's name, social security number or some other identifying data.
PHI Examples - admitting information, billing forms, clinical records -anything with both patient health information and individually identifying data.	
	Jane – What are some examples of PHI, Kevin?
In general, patient authorization is required unless the disclosure is for treatment, payment, or healthcare operations.	Kevin – PHI would include admitting forms, billing information, or transfer forms.
	Jane – Good. And PHI generally can't be released or disclosed without patient authorization unless the disclosure is for treatment, payment, or healthcare operations.

VIDEO	AUDIO
Notice of Privacy Practices (NPP)	Kevin – To keep patients informed of these rights, OMH has developed a Notice of Privacy Practices, and…
• 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.	Jane – … and every OMH facility and site will use a standard written "Notice of Privacy Practices-" or "NPP." An NPP informs patients on how OMH can use and share PHI. Every reasonable attempt should be made to document that OMH patients have received an NPP. Forensic patients do not have the right under HIPAA to receive an NPP, but sites may wish to extend this right to forensic patients if they choose to.
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.	Kevin – Business Associates…since OMH works with many vendors and contractors, OMH has the responsibility to ensure Business Associates manage PHI in a manner consistent with OMH's own practices and to make sure our other vendors and contractors know about the need to respect the privacy of our patients and to keep any information they may come across strictly confidential. Jane – OMH has taken steps to ensure that all agreements with Business Associates contain required language to ensure that the PHI used by the Business Associate is appropriately protected. Standardized language for use in Business Associate Agreements has been provided to all OMH facilities and sites.
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. • Right to an accounting of PHI disclosures except those made for treatment, payment, or healthcare operations, or where patient authorized the disclosure.	Kevin – Under normal circumstances, patients have the right to access their PHI, they can supplement their records and they can file complaints. Although, both HIPAA and the New York State Mental Hygiene Law provide that patients do not have the right to view their medical records when it is reasonably likely to cause physical harm to themselves or others in the opinion of a clinical professional. Additionally, a patient can ask for an accounting of disclosures of their PHI – but NOT when the use or disclosure of PHI is for treatment, payment, or healthcare operations or where the patient authorized such disclosure.
PLEASE STOP THE PROGRAM AND BEGIN LEARNING ACTIVITY FOUR	Jane – This has been an overview of HIPAA privacy regulations and policies. To review and reinforce the concepts that we have been discussing, please stop the program now and complete learning activity four.

VIDEO

AUDIO

Jane –
Hello again and welcome to the next portion of the HIPAA training program. We will explore security practices as they apply to HIPAA and specifically within the Office of Mental Health. My name is Jane. With me is Kilene. Hi Kilene.

Kilene –
Hi Jane. I know that protecting someone's privacy is important, but as far as security goes, I'm not sure security applies to most OMH employees. Isn't security the responsibility of administrators and specific departments?

Jane –
As with Privacy, compliance with HIPAA and OMH's Security requirements is the responsibility of _**ALL**_ OMH employees.

VIDEO

AUDIO

Kilene –
How so?

Jane –
Security policies and procedures are only pieces of paper – ultimately, they must be carried out by employees. Even the best system or policy is achievable only when employees stay mindful of their responsibilities.

Kilene –
What's covered in this section?

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.
- 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 PHI may be at risk; and, how to ensure that privacy and security are maintained.

Jane –
In response to HIPAA, and to safeguard OMH patients' privacy, a number of new policies and standards are in place now. Upon completing this section, you'll be able to:
- Identify employee responsibilities with regard to safeguarding PHI – for example when you share, transmit, print, dispose, store, or transport PHI.
- Understand OMH's policy regarding the use of software.
- Explain the OMH e-mail policy.
- Describe OMH's Information Security Event Response (or ISER for short.)
- And perhaps most importantly, you'll be better able to recognize when PHI is at risk or not being secured appropriately, and act accordingly . . . whether it means raising concern with supervisors, taking specific steps to correct the problem, or modifying your own practices or behavior.

Kilene –
Mention security, and most people think of security guards, padlocks, things like that. How does HIPAA define security?

VIDEO	**AUDIO**
	Jane – HIPAA regulations stipulate that covered entities like OMH must have a Security Management Framework. There are four main elements:
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.	First – Applications. This covers all software programs that store or process PHI like word processing programs and the Mental Health Automated Record System, or MHARS, for short. Second – Physical protection of PHI, for instance protecting laptop PCs and floppy disks. Third – Ensuring the communication networks like phones and e-mail are secure. And fourth – The overall policies and standards that guide our security operations.
	Kilene – What do these policies and standards mean to OMH employees?
	Jane – As always, OMH employees need to be vigilant in protecting patient information. The security framework is simply a means to organize the overall approach to accomplishing this.

VIDEO	**AUDIO**
	Kilene – Will individual OMH facilities and units have to develop an entirely new set of security procedures?
	Jane – No! OMH's Information Security Office has developed an Information Security Policy that applies to all of OMH including its facilities. Here's an overview.

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
	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.
	
	Maintaining security is a balance between ensuring reasonable and appropriate protection while enabling information to be shared among caregivers and others.
	
	The OMH Information Security Policy encompasses all information regardless of format or type of system on which the information resides. This includes spoken communication, written documentation, computer databases, tapes, diskettes, voice mail messages and faxes.

VIDEO	AUDIO
	Kilene – Okay, so protecting a person's Protected Health Information, or PHI, is everyone's responsibility and every employee, even those who do not use computers or think of themselves as involved with "security" must be mindful of all the PHI he or she comes into contact with everyday.
	Jane – That's right.
	Kilene – There are countless pieces of PHI transmitted in one way or another everyday in an OMH facility. What do we need to do?
Protecting Protected Health Information (PHI)	Jane – Let's take a look at telephones, e-mail and faxes.
When sharing PHI via telephone, verify who the other party is.	Kilene – We use phones, e-mail and faxes a lot.
	Jane – When sharing PHI over the phone, we need to know, or authenticate, who the other person is. For example, if we know we are sharing PHI with an appropriate person, like a caregiver or billing person, it's okay to share the PHI. However, if a person calls us and requests PHI, we shouldn't share any PHI until we can take reasonable and appropriate efforts to authenticate who the person is and whether or not they have a sound purpose for the information.
PHI should not be left on voice mail or answering machines.	Kilene – What about voice mail or answering machines?
	Jane – Good question. Since we have no way of knowing who will ultimately access the voice mail, PHI should not be left on voice mail or on answering machines.
	Kilene – Okay, but what about e-mail. Is that secure?

VIDEO	**AUDIO**
	Jane –
Not necessarily. PHI can be sent over a secure system, such as OMH's internal network where GroupWise is used. It should not be sent over public networks unless those networks are protected by an approved encryption package.
Use only internal e-mail system, which has been secured, when sharing PHI	
	Kilene –
Encryption?
	Jane –
There are some very technical ways of describing this term, but encryption can be thought of as a way of 'scrambling' data so if you are not allowed to read it, all you can see is 'garbled' incomprehensible, text.   It's particularly useful when transmitting information across insecure networks, such as the Internet, or to protect data stored on devices that can be easily lost or stolen, such as laptop PCs.
	Kilene –
And, how would we know if an approved encryption package is being used?
	Jane –
Individual facilities, centers or sites will be informed of technical issues like that. Bottom line, use only internal e-mail systems whenever sharing PHI. If conditions dictate that a public network be used, staff should check with an OMH Information Security Officer before sending it.
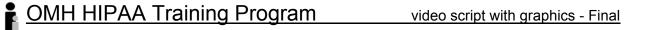| | Kilene –
You've mentioned the 'OMH Information Security Officer' before.   I'm still a little unclear.   Who or what is the OMH Information Security Officer? |
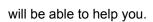| **OMH Information Security Structure**

• Central OMH Information Security Officer and team.
• Facility Information Security Liaisons.
• If questions, ask your supervisor or facility Information Center Coordinator (FICC). | Jane –
We use the term to describe the Information Security function that OMH has established.   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 your Information Security Officer is, either your supervisor or your Facility Information Center Coordinator, or FICC, |

will be able to help you.

VIDEO	**AUDIO**
	Kilene – Thanks.
	Jane – Now, getting back to email, there's one more thing I wanted to mention.
	Kilene – What's that?
Never include PHI in e-mail subject lines, headers, or the first few lines of the message.	Jane – Never include any patient details in the subject line or header. Likewise don't include any PHI in the first lines of the e-mail message.
	Kilene – Why?
	Jane – E-mail preferences and settings vary from user to user. Subject lines, headers and similar identifiers can appear on screens that might be viewed by someone other than the intended recipient. It's good practice and policy not to include PHI in subject lines. Kilene, you use e-mail, right?
	Kilene – Sure.
	Jane – How often do you change your password?

VIDEO	AUDIO
	Kilene – Umm…. I don't. I've been using the same password for ages.
Change passwords regularly and keep them private.	Jane – Bad idea. Not only email but also computer workstation passwords should be changed regularly. And there are tips for making sure that your password is kept private. These extra layers of security are important. Change that password Kilene. And, don't change it to anything that would be easy for anyone else to guess or figure out.
Use only OMH-trusted fax machines when sending PHI.	Kilene – I will! Right away. You mentioned fax machines. Can we fax PHI?
	Jane – Sending PHI via fax machines is permissible, as long as it is sent to an OMH-trusted machine. Even then, care should be taken because it is easy to send a fax to a wrong number. Sending PHI to a "non-trusted" location is permissible only if it is immediately needed for patient care.
	Kilene – What is "trusted?"
	Jane – "Trusted" means that we've taken reasonable and appropriate steps to ensure that we know where the information is going and who is going to receive it. Examples would be where we have "pre-programmed" the fax number into the fax machine, where we call to verify that it has been received, and where we know that the fax machine is located in a secure area.

VIDEO	AUDIO
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** • 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. • 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 printer is in a secure OMH area.	Kilene – So, PHI can be shared over the phone as long as we can authenticate the other person, and we don't leave PHI on voice-mail. With respect to emails, only internal e-mail should be used for sharing PHI. If a public network needs to be used, check with an OMH Information Security Officer or Facility Security Liaison or the Facility Information Center Coordinator to be sure there is proper encryption. Faxing PHI to and from OMH-trusted fax machines is permissible. All of these practices certainly seem reasonable to me. Jane – I agree. Now, let's cover procedures to follow when printing PHI, how to label documents, and how to discard PHI appropriately. Kilene – You said printing. Jane – Right. When printing PHI, the person should be physically present at the printer when the document is being printed. However, if the printer is located in a secure OMH area, physical presence is not required.

VIDEO	**AUDIO**

<table>
<tr><td></td><td>

Kilene –
A "secure OMH area?"

Jane –
Right, that would be any area where unauthorized individuals do not have access. And this is a good time to remind people that when they create a new document that contains PHI, it should clearly indicate on the bottom of the page "OMH PHI." An easy way to do this is to put that wording either in the header or footer of the document.

</td></tr>
</table>

Clearly label all Protected Health Information as "OMH PHI"

Kilene –
Sending PHI through the mail. What precautions are necessary?

Jane –
When sending PHI through internal mail, the envelope must be sealed and clearly marked: "Protected Health Information – To be opened by addressee only." This includes their designee.

Mailing PHI
For Internal Mail: Use a sealed envelope clearly labeled "Protected Health Information – To be opened by addressee only."
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.

Kilene –
But what about using U.S. Mail or overnight couriers for external mail?

Jane –
All external mail containing PHI that is not intended for "treatment, payment or healthcare operation" should be sent via certified mail or equivalent or a bonded courier. The receipt should be logged as evidence of the disclosure. For external mail that is intended for treatment, payment, or healthcare operations, you don't need to use certified mail – but you need to take reasonable precautions to ensure PHI is not inappropriately disclosed. For example, instead of mailing a bill in an OMH envelope to patient "John Doe," use an envelope that only has a Post Office Box number as the return address. Mark the envelope confidential, as well.

VIDEO	AUDIO
	Kilene – The last item you mentioned was disposing of PHI.
Disposing of PHI Paper - Use a shredder. Electronic - Physically destroy the disk or cd.	Jane – Right. Reports with PHI should be appropriately disposed of -- this means shredding if the information is in a paper format. If the information is on a computer diskette or CD, the disk or CD should be physically destroyed.
	Kilene – So you don't just throw anything away with PHI on it. To ensure security, we need to safeguard that the document or media is physically destroyed.
	Jane – Good summary. Now let's cover storing PHI and transporting PHI off OMH sites.
Storing or Transporting PHI	Kilene – Okay.
Use a secured enclosure, (e.g., store in a locked cabinet/desk, transport in a carrying case).	Jane – Whenever PHI is stored, it must be in a secured enclosure such as a locked cabinet or desk. When carrying PHI off-site, use a carrying case.
	Kilene – And when the PHI is in electronic form, what must be done?
When in digital format, data must be encrypted.	Jane – Well for one thing, PHI should never be stored on an employee's desktop PC's hard drive. Storing PHI on a hard drive, be it a memo, e-mail message or similar file, places that PHI at risk. Hard drives have limited security. The requirement is that where data is held on laptops or portable disks, it must be encrypted.

VIDEO	**AUDIO**
	Kilene – Another question Jane. Every OMH facility or location has unique operations. How can OMH employees ensure that these procedures will work or be enough to assure security at their specific locations?
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). • 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.	Jane – Three ways. First, whenever in doubt regarding protecting PHI, OMH employees should ask for guidance from their supervisor, OMH Information Security Officer, Facility Information Security Liaison or Facility Information Center Coordinator or FICC for short. Secondly, employees are encouraged to treat all PHI as if it belonged to them or a family member. If a document or database contained your personal health information, or that of a family member, what steps would you take to safeguard its security? Kilene – That's a good point. Treat all PHI with respect. Jane – And the third way to keep up to date and make sure that proper attention is given to these issues is to dialogue with your co-workers and supervisors.
PLEASE STOP THE PROGRAM AND COMPLETE LEARNING ACTIVITY FIVE.	

VIDEO	AUDIO
	Jane – Hello again. At this point, you've had the chance to review some of your responsibilities in safeguarding Protected Health Information, or PHI, in your workplace. From phone calls and memos to properly storing records, keeping PHI secure is everyone's responsibility. Kilene – The new HIPAA security measures share a fundamental purpose – protecting patient information, but the way and manner in which OMH employees will carry out those measures is really determined by their specific responsibilities and work-site specific factors such as differences in equipment, physical layout, etc. Jane – Thanks for that reminder Kilene. Now, we're going to cover three more areas that apply to all OMH employees and in particular those employees working at computer workstations. Kilene – What's next? Jane – OMH has developed an Information Security policy and a number of security standards to ensure that computer files and other digital information remain secure. These address security concerns such as: • Malicious software; • E-mail; and, • Information Security Event Response, or ISER.

VIDEO	AUDIO
	Kilene – How does using a computer translate into HIPAA Security?
	Jane – Because there are any number of malicious software programs that can breach information security. You've probably heard of computer viruses, worms or Trojan Horses. These and similarly destructive programs can wreak havoc on a computer system and put a great deal of confidential data at risk.
	Kilene – What do we need to know?
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.	Jane – Let's talk about malicious software first. Under no circumstance should software other than that provided by OMH Information Services be installed on machines. That prohibition includes but certainly isn't limited to new commercial software, downloaded software, programs from vendors and personal, "home grown" software.
	Kilene – But there are certain OMH offices or sites that test new software, new applications. What can they do?
PHI AND SOFTWARE SECURITY 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.	Jane – They'll need to contact their Information Security Officer, Liaison or their Facility Information Center Coordinator for approval prior to installing any outside software. Even the best, most-trusted sources can have viruses hidden in them.
	Kilene – Better safe than sorry, then?
	Jane – That's right. Your FICC, OMH Information Security Officer or Liaison can also provide support when installing new approved software.
	Kilene – Earlier, we covered the dos and don'ts of e-mail use. There are other security measures, right?

VIDEO	AUDIO
PHI AND E-MAIL SECURITY • Use only OMH-approved e-mail product (GroupWise) when e-mailing PHI.	Jane – Yes. When using e-mail, remember to use only OMH-approved e-mail products. Currently, the only approved e-mail package is GroupWise. Kilene – What about sending e-mail to outside agencies, particularly when sending PHI?
• Do NOT send PHI via e-mail to non-OMH recipients	Jane – OMH encrypts its e-mail to protect it. Since few outside organizations practice similar security safeguards, do not send any PHI to non-OMH recipients via e-mail, unless authorized to do so.

VIDEO	AUDIO
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.	Jane – This is a good time for a reminder that OMH employees are not allowed to store patient PHI on their desktop PC's hard drive. They should store it on a centralized server which provides security safeguards to ensure that PHI remains protected and private. And…if your PC crashes, there will be a back-up. Kilene – Okay Jane. But mishaps happen. Files can get deleted, computers can crash or breakdown, or viruses can spread through a network. Suppose someone suspects a piece of PHI has been released inappropriately. How should OMH staff respond? Jane – To address those incidents, the OMH Information Security Office has established the Information Security Event Response or ISER. ISER is a procedure to follow whenever someone suspects PHI or other sensitive information has been put at risk.

VIDEO

Kilene –
What are some examples of things that would cause an ISER?

INFORMATION SECURITY EVENT RESPONSE (ISER)
Trigger 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").
- Inappropriate use of e-mail to send "spam" messages.
- An intrusion into OMH files, either digital or hard copy, by an unauthorized individual.

Jane –
Information Security Event Responses or ISERs can be triggered by:
- Damage to equipment, facilities or utilities.
- Losing or misplacing computer diskettes, files or other media containing PHI.
- Losing or misplacing portable devices like laptops or Personal Digital Assistants.
- Inappropriate use of the computer system such as sending "spam" mail.
- And an ISER would be if you think an unauthorized person has been accessing your PC or files.

Kilene –
If I understand this correctly, an Information Security Event Response isn't limited to inappropriate access to computer files. If the wrong person has access to OMH paperwork with PHI on it, that would be an event that would trigger an ISER.

Jane –
Right. An ISER could be triggered by things like:
- Someone misrepresenting him or herself (Be sure to ask for ID, or look for an ID badge).
- A patient's file that is accessed by someone you don't know or who does not ordinarily view patient records.
- A question about someone picking up patient records (Was there an appointment made to do this?)

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 at risk.

Kilene –
If any of those incidents, occur, OMH staff should contact their supervisor immediately?

Jane –
Yes – their supervisor or other appropriate Security official as soon as possible. Obviously, circumstances involving patient care or protecting yourself or others must be addressed before any notification.

VIDEO

AUDIO

Kilene –
Let's review the three areas we just discussed. We covered malicious software.

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.

ISER REVIEW

- Information Security Event Response
  - 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.

Jane –
Right. Under no circumstances should non OMH-approved software be installed on an OMH computer.

Kilene –
We reviewed the OMH E-mail policy. Only GroupWise should be used for sending internal e-mail. Forwarding or sending PHI over outside networks should only occur when cleared by an OMH Information Security Officer.

Jane –
Finally we discussed the Information Security Event Response, or ISER. An ISER is any event or security breach that places OMH information, including PHI at risk. Examples include damage to equipment, losing or misplacing computer diskettes or paperwork, losing or misplacing removable or temporary storage devices and any inappropriate use of the computer system.

Kilene –
And an ISER could be unauthorized access to OMH files, either digital or hard copy.

PLEASE STOP THE PROGRAM AND COMPLETE LEARNING ACTIVITY SIX.

VIDEO

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.

- 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.

- 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.
- HIPAA's Security Regulations tell you how to protect PHI.
- OMH's Information Security Policy and Standards provide additional guidance.

Jane –
This learning program has provided OMH employees and our partners with an overview of HIPAA.

Kevin –
Among HIPAA's overall purpose is to ensure patient confidentiality and safeguard patients' protected health information.

Kevin –
The portion of HIPAA of greatest concern to OMH employees is called Administrative Simplification. Included in this are requirements relating to Privacy, Security and Electronic Data Interchange, or EDI. EDI relates to the electronic interchange or transfer of health information and as such is largely transparent to most OMH employees. Therefore, of these three areas, understanding and complying with HIPAA's Privacy and Security provisions is most important to our workforce.

OMH is a Covered Entity under HIPAA, which means that OMH must comply with all HIPAA regulations. Business Associates are those individuals or organizations that work for or on behalf of OMH and must have access to Protected Health Information in order to do their job. Like Covered Entities, Business Associates must comply with HIPAA, and OMH must establish Business Associate Agreements to ensure this.

Jane –
HIPAA's Privacy regulations set standards for what kind of patient health information is protected. This is called Protected Health Information, or PHI.
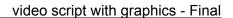
Protected health information, or its abbreviation "PHI," is any type of health information that contains something that could identify the individual.

As a general rule unless the patient has provided his or her specific written permission, protected health information can be used or disclosed only for treatment, payment or healthcare operations.

Kevin -
Under normal circumstances, patients have the right to access their PHI. They can supplement their records and they can file complaints.

Additionally, a patient can ask for an accounting of disclosures of their PHI - but NOT when the use or disclosure of PHI is for treatment, payment, or healthcare

operations or where the patient authorized such disclosure.

VIDEO	**AUDIO**
OMH's Privacy Policy provides additional guidance.	Jane – And HIPAA's security regulations set standards for how PHI is protected. Jane – OMH Information Security Policy and Standards set forth those procedures that OMH employees need to follow in order to protect a patient's Protected Health Information.
HIPAA compliance is everyone's responsibility.	Kilene – HIPAA security is everyone's responsibility. We've covered procedures for transmitting, printing, storing and transporting a patient's Protected Health Information. Jane – Safeguarding a patient's Protected Health Information is critical to providing care, enacting solid public policy and is core to the mission of the Office of Mental Health.
Questions about HIPAA? Talk to your • Supervisor • Privacy liaison or officer • Information Security Liaison or Officer	Kilene – This concludes the video portion of the HIPAA learning program. One more learning activity remains. Jane – Before stopping the program, remember - HIPAA compliance is **_everyone's_** responsibility. It is up to all of us to keep HIPAA on our minds as we continue our important work at OMH. For those who are supervisors and managers – you should find ways to emphasize and remind your staff about the importance of protecting the confidentiality and security of PHI.
THIS CONCLUDES THE VIDEO PORTION OF THE HIPAA TRAINING PROGRAM. ***PLEASE STOP THE PROGRAM AND COMPLETE LEARNING ACTIVITY SEVEN.***	It is you and your fellow employees who know your own workplace best – only through your and their efforts will the intention behind these policies and standards be fully realized. You're sure to have questions regarding HIPAA compliance. Talk to your supervisor, manager, privacy and information security officer or liaison if you have questions about any of the information you've been provided or about any new procedures you may have to follow. Managers and supervisors can contact those staff in their facility working on HIPAA coordination and compliance, or contact OMH Central Office for more information regarding HIPAA's administrative issues and the policies we've discussed. Jane – Thanks for being part of our program.