

Privacy and Security Safeguards for the OMH Workforce

- Follow the “minimum necessary rule” ... except for treatment purposes, use and disclosure of PHI is limited to that amount that is necessary to perform job functions.
- Use file covers, locked filing cabinets and locked record rooms to protect PHI.
- Avoid conversations identifying patients in public places.
- Avoid posting PHI where it can be seen by unauthorized individuals.
- Don't leave the worksite with unsecured PHI.
- Don't share or document computer passwords.
- Follow computer security policies for desktops, laptops, disks and other media; **DO NOT** email confidential clinical information or PHI over the internet (unless an ISO approved encryption method is used).
- Keep track of paper files and secure electronic devices which contain PHI.
- Before faxing or phoning PHI, be sure to verify the receiving party and the contact numbers.
- Be mindful of disposing of PHI: shred, don't toss, and use secure waste receptacles systems, not regular trash bins.
- When storing electronic PHI, choose the most secure, accessible and authorized location – e.g., encrypted portable devices and appropriate OMH system drives.
- Don't store PHI on personally owned devices or home computers.
- Remove PHI from electronic files and storage devices when no longer needed while following the requirements of the OMH Records Retention policy.
- When changing job functions or leaving OMH, discuss with your supervisor the disposition of PHI under your control.
- Report suspected violations of HIPAA privacy or security requirements to your supervisor or your facility's privacy liaison.
- Immediately report any suspected instance of lost or stolen paper or electronic files containing PHI to your supervisor or your facility's privacy liaison.

To obtain more detailed information about HIPAA and the HITECH Act, please visit the US Department of Health and Human Resources website at www.hhs.gov/ocr/privacy or contact your OMH Information Security Liaison and/or Privacy Liaison.

Remember...

**Information Privacy and Security
is everyone's responsibility.**

New York State
David A. Paterson, Governor

Office of Mental Health
Michael F. Hogan, PhD, Commissioner



Prepared by the
OMH Bureau of Education and
Workforce Development (BEWD),
OMH Information Security Unit
and the OMH Counsel's Office

May 2010

2010

Information Security Training Update
including related Privacy updates for
NYS Office of Mental Health (OMH)
Workforce Members

From HIPAA

(Health Insurance Portability and Accountability Act)

to HITECH

(Health Information Technology for Economic and Clinical Health)

Privacy and Security Basics

Please Note:

Every member of the New York State Office of Mental Health (OMH) workforce, regardless of job title or function, is mandated to read this brochure and document receipt as instructed by their education and training office. If you have questions, please direct them to your education and training department.

The HITECH Act



HIPAA mandated comprehensive information security and privacy programs to ensure the confidentiality, integrity, and availability of Protected Health Information (PHI).

In February 2009, the American Recovery and Reinvestment Act (ARRA), 'stimulus bill', was signed into law. It includes provisions for heightened enforcement of HIPAA and stiffer penalties for privacy and security violations.



The new privacy and security provisions are found in Title XIII, Health Information Technology, which includes the HITECH Act.

From HIPAA to HITECH

Covered Entities are Health Plans, Healthcare Providers and Healthcare Clearinghouses. OMH is a 'Covered Entity' and is required to comply with the requirements of the HIPAA Privacy and Security Rules.

- HITECH expands HIPAA privacy and security rules to directly cover 'Business Associates' of covered entities. 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.
- **OMH clinical information is covered by both Mental Hygiene Law and HIPAA.** Clinical information is PHI, if it includes information that tends to identify a patient and relates to his/her care and treatment.
- **Mandatory Audits.** HITECH mandates audits to ensure compliance.
- HITECH affords a private right of action for HIPAA violations, with prosecuting authority to State Attorneys General.
- **OMH continues to follow Mental Hygiene Law confidentiality rules.** In general, the HIPAA Privacy Rule or Mental Hygiene Law requirement providing the greater confidentiality protections, or the broader rights of records access to the individual, will apply.
- **PHI/Clinical Information is confidential.** Within OMH, no consent is required for uses and disclosures of PHI for treatment, payment and health care operations.
- **With some exceptions, a person will need to give written permission to share his/her clinical information.** OMH provides standard HIPAA authorization forms.
- **Mental Hygiene Law has a "need to know" standard; HIPAA has a similar "minimum necessary standard" for access and disclosure of PHI.**



- There are new patient rights regarding **Electronic Health Records (EHRs)**. For example, patients can request an accounting of disclosures that includes disclosures made for treatment, payment, healthcare operations, and those authorized by the patient, of EHRs. Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. The requested accounting can go back as far as three years.
- **Individuals may file privacy complaints.** Complaints can be forwarded to designated OMH contact persons, the Facility Director, and the federal Department of Health and Human Services (HHS), Office of Civil Rights (OCR).
- **HITECH requires OMH to notify individuals when there is a "breach" of their unsecured PHI/clinical information.** Previously, covered entities (and their business associates) were not bound by HIPAA to inform individuals when a breach occurred. Now they must notify each person whose unsecured PHI is disclosed in a breach. If the breach involves more than 500 residents in a state or jurisdiction, prominent media outlets must be notified.
- HITECH *significantly* increases civil and criminal penalties for violating HIPAA requirements. Civil penalties are tiered and can range from \$100 a violation to \$1.5 million per year. Criminal fines up to \$50,000 and/or imprisonment can result.