WELCOME TO THE HIPAA: PRIVACY AND SECURITY TRAINING MODULE

Provided with permission from the

University of North Carolina,

which contributed to its content

Course Competencies

This training addresses the essential elements of maintaining the privacy and security of Sensitive Information and protected health information (PHI) within MIEMSS

During this course you will learn:

- about the Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules;
- about the HIPAA identifiers which create protected health information ("PHI");
- about Maryland law concerning information from health care records;
- how to recognize situations in which confidential and protected health information can be mishandled;
- about practical ways to protect the privacy and security of Sensitive Information, including PHI; and
- that employees will be held responsible if they mishandle confidential or protected health information.

Forms of Sensitive Information

Sensitive Information exists in various forms...

printed

spoken

electronic

It is the responsibility of every employee to protect the privacy and security of Sensitive Information in ALL forms.

Examples of Sensitive Information

- Social Security numbers
- credit card numbers
- driver's license numbers
- personnel information
- research data
- computer passwords
- individually identifiable health information

The improper disclosure of Sensitive Information presents the risk of identity theft, invasion of privacy, and can cause harm and embarrassment to patients, EMS Providers, and MIEMSS employees. Breaches of information privacy can also result in criminal and civil penalties for MIEMSS and for those individuals who improperly access or disclose Sensitive Information, as well as disciplinary action for MIEMSS employees that are responsible for such violations.

Every MIEMSS employee must protect the privacy and security of Sensitive Information.

HIPAA Privacy and Security Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect a subset of Sensitive Information known as protected health information (PHI).

In 2009, HIPAA was expanded and strengthened when the American Recovery and Reinvestment Act was passed. This law is referred to as the Health Information Technology for Economic and Clinical Health (HITECH) Act.

This training focuses on two primary HIPAA rules, as amended by HITECH:

Section I: The HIPAA Privacy Rule

Section 2: The HIPAA Security Rule

Note: *There is also a Transaction Rule that is not covered in this course. Healthcare providers need to be aware that under this rule, treatment must be accurately billed using the prescribed code set for their profession.*

Maryland Confidentiality of Medical Records Act

The Maryland Confidentiality of Medical Records Act protects patient medical records in much the same way and with the same sorts of penalties as HIPAA. Its prohibition on disclosure is very broad and extends beyond health care providers. The Maryland Act has one interesting limitation (below in bold)…

(i) Medical record. --

(1) "Medical record" means any oral, written, or other transmission in any form or medium of information that:

(i) **Is entered in the record of a patient or recipient;**

(ii) Identifies or can readily be associated with the identity of a patient or recipient; and

(iii) Relates to the health care of the patient or recipient.

Md. HEALTH-GENERAL Code Ann. § 4-301

Section 1.A.

HIPAA Privacy Rule

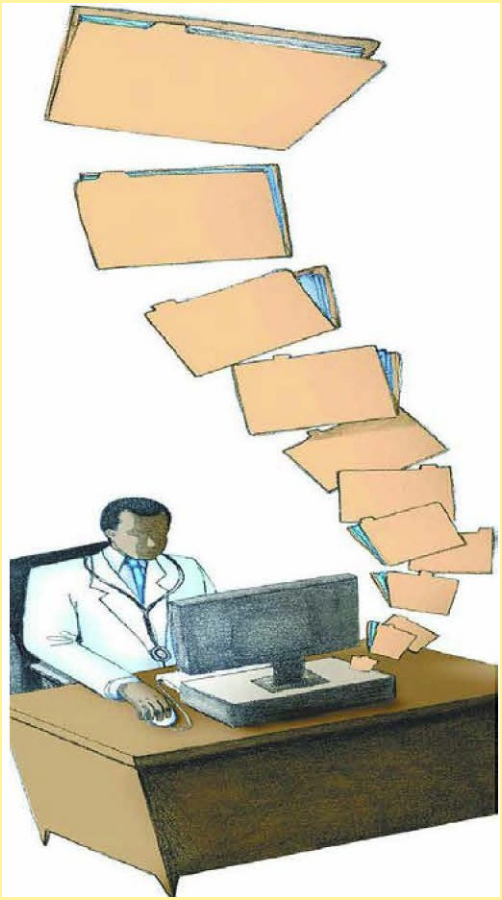
Overview

Covered Entities and Business Associates Have a Duty to Protect PHI Under HIPAA

A "covered entity" is any person or organization that furnishes, bills, or is paid for health care services in the normal course of business (electronic transaction required).

Pursuant to HIPAA, individually identifiable health information collected or created in a covered entity is considered "protected health information," or PHI.

MIEMSS is not a covered entity, but it is a business associate of covered entities because it provides billing data for and maintains data for covered entities. As a business associate, MIEMSS has the same duty to safeguard PHI as a covered entity.



PHI Defined

PHI is generally defined as:

Any information that can be used to identify a patient—whether living or deceased—and which relates to the patient's past, present, or future physical or mental health or condition, including health care services provided and the payment for those services.

Employees may access PHI

only when necessary to perform their job-related duties.

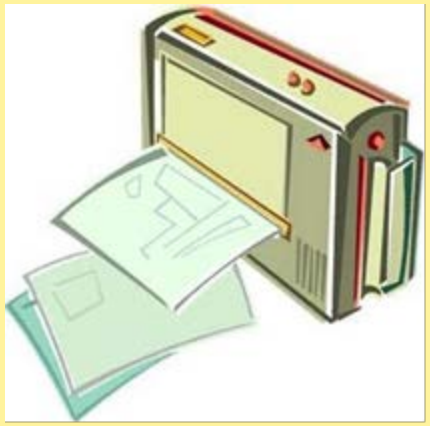
Any of the following are considered identifiers under HIPAA

- Patient names
- Geographic subdivisions (smaller than state)
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Health plan beneficiary numbers
- Dates (except year)
- Names of relatives or characteristics that can be linked to an individual
- Full face photographs or images
- Healthcare record numbers
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- E-mail addresses
- Certificate/license numbers
- Web URLs and IP addresses
- Any other unique number or code

Reality Check:

In general, HIPAA violations are enforced by the Department of Health and Human Services. However, the more recently enacted Health Information Technology for Economic and Clinical Health (HITECH) Act now permits state Attorneys General to bring civil actions AND to sue for monetary awards to be shared with harmed individuals.

The Tufts Medical Center and an employee were sued by a patient who alleged the Center sent documents containing her protected health information to a shared office fax machine in her place of business without her consent, causing her great embarrassment. Although the PHI was related to the employee's disability claim, it was sent to the wrong fax machine located in a common area of her office.



Confirm authorization instructions and verify telephone numbers before faxing AND use pre-programmed telephone numbers whenever possible.

Reality Check:

- **Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach**

- Lifespan Health System Affiliated Covered Entity (Lifespan ACE), a non-profit health system based in Rhode Island, has agreed to pay $1,040,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to implement a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules related to the theft of an unencrypted laptop.
- On April 21, 2017, Lifespan Corporation,, filed a breach report with OCR concerning the theft of an affiliated hospital employee's laptop containing electronic protected health information (ePHI) including: patients' names, medical record numbers, demographic information, and medication information. The breach affected 20,431 individuals.
- OCR's investigation determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt ePHI on laptops after Lifespan ACE determined it was reasonable and appropriate to do so. OCR also uncovered a lack of device and media controls, and a failure to have a business associate agreement in place with the Lifespan Corporation.
- "Laptops, cellphones, and other mobile devices are stolen every day, that's the hard reality. Covered entities can best protect their patients' data by encrypting mobile devices to thwart identity thieves," said Roger Severino, OCR Director

Access Must be Authorized:

An employee may only access or disclose a patient's PHI when this access is part of the employee's job duties.

If an employee accesses or discloses PHI without a patient's written authorization or without a job-related reason for doing so, the employee violates MIEMSS policy and HIPAA.

Access Must be Authorized:

University of California Los Angeles Health System was fined $865,000 in 2010 for failing to restrict access to medical records. The healthcare provider was investigated following the discovery that a physician had accessed the medical records of celebrities and other patients without authorization. Dr. Huping Zhou accessed the records of patients without authorization 323 times after learning that he would soon be dismissed. Dr. Zhou became the first healthcare employee to be jailed for a HIPAA violation and was sentenced to four months in federal prison.

Unauthorized Access:

It is never acceptable for an employee to look at PHI "just out of curiosity," even if no harm is intended.

It also makes no difference if the information relates to a "high profile" person or a close friend or family member—ALL information is entitled to the same protection and must be kept private.

These rules apply to all employees, including health care professionals.

Be aware that accessing PHI of someone involved in a divorce, separation, break-up, or custody dispute may be an indication of intent to use information for personal advantage, unless the access is required for the individual to do his or her job. Such improper behavior will be considered by MIEMSS when determining disciplinary action against violators.

Breaches:

A breach occurs when information that, by law, must be protected is:

- lost, stolen, or improperly disposed of (e.g., paper or device upon which the information is recorded cannot be accounted for);
- "hacked" into by people or mechanized programs that are not authorized to have access (e.g., the system in which the information is located is compromised through a "worm"), or
- communicated or sent to others who have no official need to receive it (e.g., gossip about information learned from a medical record).

Reality Check:

Colorado hospital failed to terminate former employee's access to electronic protected health information

Pagosa Springs Medical Center (PSMC) has agreed to pay $111,400 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services and to adopt a substantial corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. PSMC is a critical access hospital, that at the time of OCR's investigation, provided more than 17,000 hospital and clinic visits annually and employs more than 175 individuals.

The settlement resolves a complaint alleging that a former PSMC employee continued to have remote access to PSMC's web-based scheduling calendar, which contained patients' electronic protected health information (ePHI), after separation of employment. OCR's investigation revealed that PSMC impermissibly disclosed the ePHI of 557 individuals to its former employee and to the web-based scheduling calendar vendor without a HIPAA required business associate agreement in place.

Size doesn't matter:

In July 2013, for the first time, a federal investigation of a health information breach that affected fewer than 500 individuals resulted in a penalty for HIPAA violations.

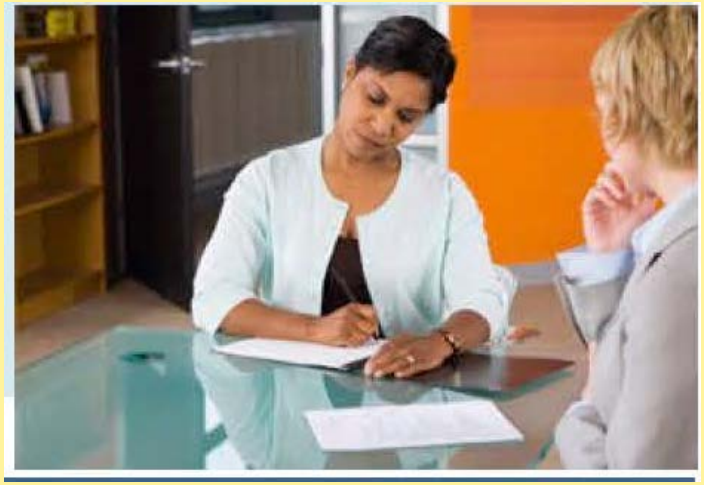
The case illustrates that no matter what the size of a breach, the Department of Health and Human Services' Office for Civil Rights (OCR) may impose penalties if its investigation reveals HIPAA non-compliance issues.

The $50,000 settlement in the case, which involved the theft of an unencrypted laptop computer from the non-profit Hospice of North Idaho, demonstrates OCR is ramping up HIPAA enforcement, says Leon Rodriguez, director of the office.

"This action sends a strong message to the healthcare industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information," Rodriguez says in a statement.

Employees must report breaches:

Part of your responsibility as a MIEMSS employee is to report privacy or security breaches involving PHI to your supervisor AND the MIEMSS Information Security Officer (Nick Seaman) or the Office of the Attorney General.



Employees, volunteers, students, or contractors of MIEMSS may not threaten or take any retaliatory action against an individual for exercising his or her rights under HIPAA or for filing a HIPAA report or complaint, including notifying of a privacy or security breach.

Employees must report breaches:

- On November 27, 2019, Sentara Hospitals (Sentara), a health system with sites of care in Virginia and North Carolina, settled with OCR for $2.175 million for failing to properly notify OCR and affected individuals of a breach of unsecured PHI. Specifically, Sentara mailed out 577 patient billing statements to the incorrect addresses. The billing statements included patient names, account numbers, and dates of services. At the time of the incident, Sentara conducted a risk assessment and determined Sentara only needed to notify eight individuals of the breach because the other disclosures did not contain a patient diagnosis, treatment information, or other medical information. That is, Sentara determined the other disclosures created only a “low risk of compromise” to the PHI and thus, notification was not required.
- Sentara also did not notify OCR at the time, since Sentara treated the breach as one affecting less than 500 individuals (i.e., only eight individuals were notified). Breaches affecting 500 or more individuals must be reported to OCR within 60 days of discovery of the breach; breaches affecting less than 500 individuals must be reported to OCR within 60 days of the end of the calendar year in which the breach was discovered.

Penalties for breaches:

Breaches of the HIPAA Privacy and Security Rules, as well as Maryland law, have serious ramifications for all involved. In addition to sanctions imposed by MIEMSS, such breaches may result in civil and criminal penalties.

Statutory and regulatory penalties for breaches may include:

- Civil: $50,000 per incident, up to $1.5 million per calendar year for violations that are not corrected

- Criminal: $50,000 to $250,000 in fines and up to 10 years in prison

In addition, institutions that fail to correct a HIPAA violation may be fined up to $50,000 per violation.

Quick Review:

- Sensitive Information exists in many forms: printed, spoken, and electronic.
- Sensitive Information includes Social Security numbers, credit card numbers, driver's license numbers, personnel information, computer passwords, and PHI.
- There are a number of laws that impose privacy and security requirements, including the Maryland Confidentiality of Medical Records Act and the federal HITECH Act.
- Two primary HIPAA regulations are the Privacy Rule and the Security Rule.
- When used to identify a patient and when combined with health information, HIPAA identifiers create PHI.
- An employee must have a patient's written authorization or a job-related reason for accessing or disclosing patient information.
- Breaches of information privacy and security may result in both civil and criminal penalties, as well as MIEMSS sanctions. Employees must report such breaches

Section 1.B.

HIPAA Privacy Rule

Program Components

5 HIPAA Program Components:

MIEMSS follows these five **HIPAA** program components

1. Individual (Patient) Rights
2. "Minimum Necessary" Information Standard
3. Procedures for Data Use in Research
4. Limits for Marketing and Fundraising Uses
5. Business Associates

1. Patient Rights:

The first component sets forth the following individual rights for patients.

- To receive a copy of the Notice of Privacy Practices (*Note: this does not apply to MIEMSS*)
- To request restrictions and confidential communications of their PHI
- To inspect and copy their healthcare records
- To request corrections of their health care records
- To obtain an accounting of disclosures (i.e., a list showing when and to whom their information has been shared)
- To file a complaint with a healthcare provider or insurer and the U.S. Government if the patient believes his or her rights have been denied or that PHI is not being protected

2. Minimum Necessary:

Under the HIPAA Privacy Rule, when the use or disclosure of PHI is permitted, only the minimum necessary information may be used or disclosed. However, this does not restrict the ability of doctors, nurses, and other healthcare providers to share information needed to treat patients, process payments, or to report public health concerns.

Otherwise, patients must sign an authorization form before their PHI may be released by MIEMSS to outside parties.

Disclosures of PHI:

HIPAA regulations **permit** use or disclosure of PHI for:

- providing medical treatment
- processing healthcare payments
- conducting healthcare business operations
- public health purposes as required by law (applies to MIEMSS)

Employees **may not** otherwise access or disclose PHI unless:

- the patient has given written permission
- it is within the scope of an employee's job duties
- proper procedures are followed for using data in research
- required or permitted by law (applies to MIEMSS)

Reality Check:

Imagine that through your work, you become aware of a family under substantial financial hardship. You believe that kindhearted members of the community would provide help “if they only knew" of these circumstances. In order to tell this story you must get specific written authorization from the patients or their legal representatives that identifies whom you will tell. In addition, you may communicate only the minimum amount of information necessary to describe the need.

Note: This type of "outreach" should be approved in advance by departmental managers and supervisors and must be consistent with institutional policy.

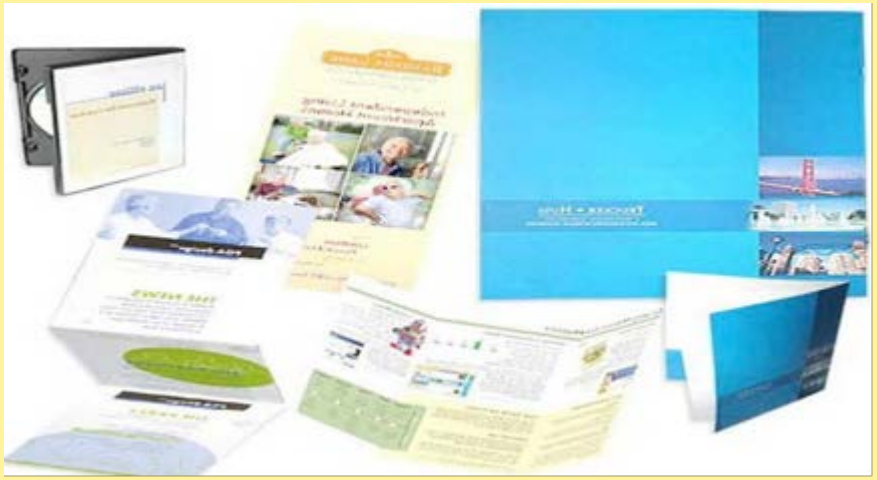
3. Research Data:

HIPAA regulates how PHI may be obtained and used for research. This is true whether the PHI is completely identifiable or partially "de-identified" in a limited data set.

A researcher or healthcare provider is not entitled to use PHI in research without the appropriate HIPAA documentation, including an authorization or an institutionally approved waiver.

Approval of a waiver of the requirement for a written authorization by the patient is required from a federally registered Institutional Review Board.

4. Marketing and Fund Raising:



Without an authorization, MIEMSS may not use information about the medical treatment of an individual for targeted fundraising or marketing.

5. Business Associates:

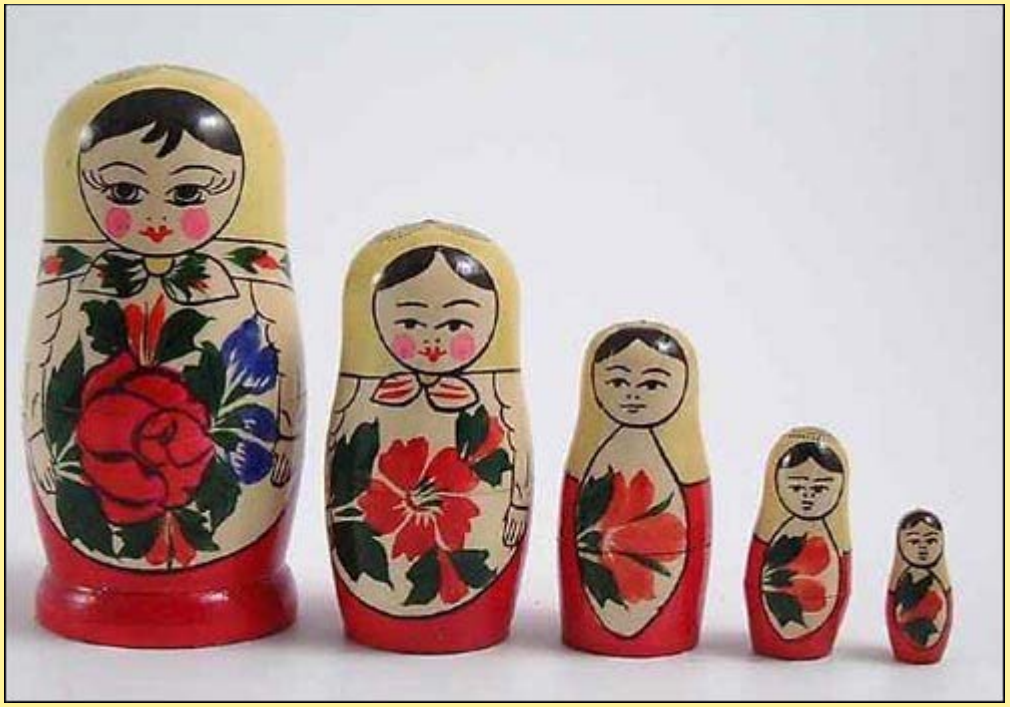
An outside company or individual is a HIPAA Business Associate of MIEMSS when providing services involving PHI maintained by MIEMSS.

Under HIPAA, a Business Associate must:

- Enter into a Business Associate Agreement (sometimes called a BAA) with the covered entity or with another business associate;
- Use appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by a contract with the covered entity;
- Notify the covered entity of any individual instances of a breach for which the Business Associate was responsible where PHI has been improperly accessed, used, or disclosed;
- Ensure that their employees and/or subcontractors receive HIPAA training; AND
- Protect PHI to the same degree as a covered entity.

6. Business Associates:

Business associates need to have business associate agreements with other business associates:



Quick Review:

Under HIPAA, patients have the right to:

- Receive a copy of the covered entities Notice of Privacy Practices
- Inspect and copy their healthcare records
- Ask for corrections of their health care records
- Receive accounting of when and with whom their PHI has been shared
- Restrict how their PHI is used and shared
- Authorize confidential communications of their PHI to others
- File a HIPAA complaint

Quick Review:

MIEMSS may use or share only the minimum necessary information to perform its duties.

- Patients must sign an authorization form before a covered entity or business associate can release their PHI to a third-party not involved in providing health care or other activities provided by law.
- A researcher or healthcare provider is not entitled to use PHI in research without the appropriate HIPAA documentation.
- A Covered Entity must obtain an individual's specific authorization before using his or her PHI for marketing or fundraising.
- A contractor providing services involving PHI is called a Business Associate.
- A covered entity and business associate must enter into a Business Associate Agreement (BAA).

Quick Review:

- The Business Associate must enter a Business Associate Agreement with all of its Business Associates (which must be repeated on down the line) and its employees must receive HIPAA training.

- Business Associates must ensure that their employees or subcontractors sign a Business Associate Agreement and receive HIPAA training.

- HIPAA protections apply to a person's protected health information even after they have died.

Section 2:

HIPAA Security Rule

HIPAA Security Rule:

The HIPAA Security Rule concentrates on safeguarding PHI by focusing on the confidentiality, integrity, and availability of PHI.

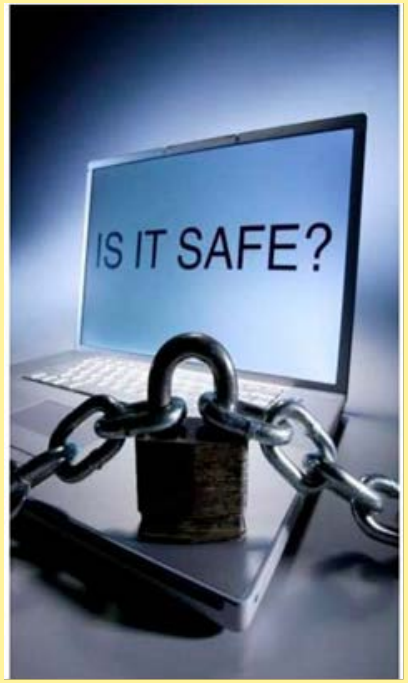
- Confidentiality means that data or information is not made available or disclosed to unauthorized persons or processes.
- Integrity means that data or information has not been altered or destroyed in an unauthorized manner.
- Availability means that data or information is accessible and useable upon demand only by an authorized person.

HIPAA Security Rule:

MIEMSS is required to have administrative, technical, and physical safeguards to protect the privacy of PHI.

Safeguards must:

- Protect PHI from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites such as Facebook, Twitter, and others) and work areas;
- Limit accidental disclosures (such as discussions in waiting rooms and hallways); and
- Include practices such as document shredding, locking doors and file storage areas, and use of passwords and codes for access.



Employee Responsibilities:

- Access information only as necessary for your authorized job responsibilities.
- Keep your passwords confidential.
- Report promptly to your supervisor and the MIEMSS Information Security Officer the loss or misuse of MIEMSS information
- Initiate appropriate actions when problems are identified.
- Comply with MIEMSS Information Security and Privacy policies.
- Avoid storing Sensitive Information on mobile devices and portable media, and if you must, make sure the device is encrypted.
- Always keep portable devices physically secure to prevent theft and unauthorized access.

Reality Check:

Be careful when disposing of desks, file cabinets and other office furniture that may hold documents in them. Please check them carefully and confirm that all documents have been removed and properly disposed of before sending furniture to the DGS Surplus department.

Physical Security:

Breaches of MIEMSS policies or an individual's confidentiality **must be reported** to the employee's supervisor **AND** one of the following persons:

- MIEMSS Information Security Officer
- MIEMSS AAG

MIEMSS is required to take reasonable steps to lessen harmful effects of any breach. This may include notifying the individual whose information has been breached and the entity whose data has been breached. The HITECH Act requires that covered entities report breaches of PHI to the Secretary of Health and Human Services at least once a year.

Disciplinary Actions:

Individuals who violate MIEMSS Information Security Policy will be subject to appropriate disciplinary action as outlined in accordance with Maryland State employee laws and regulations, as well as possible criminal or civil penalties.

Best Practice Reminders:

- **DO** keep computer sign-on codes and passwords secret and **DO NOT** allow unauthorized persons access to your computer. Also, use locked screensavers for added privacy.

- **DO** keep notes, files, memory sticks, and computers in a secure place, and be careful to **NOT** leave them in open areas outside your workplace, such as a library, cafeteria, or airport.

- **DO NOT** place PHI on a mobile device without required approval. **DO** encrypt mobile devices that contain PHI.

- **DO** hold discussions of PHI in private areas and for job-related reasons only. Also, be aware of places where others might overhear conversations, such as in reception areas.

Best Practice Reminders:

Throughout the year MIEMSS provides security training through the knowb4 fore program which includes a variety of updates on current security issues.

MIEMSS employees need to remain uptodate in this training both for general security training and as part of the MIEMSS annual HIPAA training.

HIPAA: PRIVACY AND SECURITY TRAINING MODULE

Questions?

Contact the Office of the Assistant Attorney General

or MIEMSS Security Officer