

Health Insurance Portability and Accountability Act (HIPAA) Training

Using and Securing Protected Health Information (PHI)

Please use the “Back” and “Forward” navigation arrows to move through this program.



Overview of Training

This training will provide current information on the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** operating policies with an emphasis on using and releasing protected health information (PHI) in your job.

Please use the “Back” and “Forward” navigation arrows to move through this program.



Purpose & Basis of HIPAA

HIPAA, implemented in 2003, established a national standard for protecting the confidentiality and privacy of an individual's health information and prohibits unauthorized release of such information.

HIPAA extends the confidentiality and privacy protections to "Protected Health Information" or "PHI."



PHI Defined

Federal law defines PHI as individually identifiable health information maintained or transmitted by a covered entity that identifies the individual or includes information from which the individual could be identified.

Health information is information that relates to:

- ✓ Past, present, or future physical or mental health conditions of an individual
- ✓ Provision of health care to an individual; or
- ✓ Past, present, or future payment for provision of health care to an individual.



Using & Protecting PHI

HIPAA and agency policies require IT employees to:

- ✓ Be responsible for protecting the privacy and confidentiality of each person's PHI and records.
- ✓ Assure that an individual's PHI is only released to authorized individuals or agencies.
- ✓ Access and use an individual's health records only as required to perform their job duties and limited to the minimum necessary to complete their job duties.
- ✓ Receive HIPAA and HITECH training and ongoing training as directed.
- ✓ Sign a confidentiality agreement.



Using & Protecting PHI

HIPPA prohibits the unauthorized release of PHI and requires employees to:

- ✓ Not discuss confidential or personal health information in a manner or place where the discussion could easily be overheard.
- ✓ Remove from public view (e.g., place in desk or file) records and files containing PHI when an employee leaves his/her workstation.
- ✓ Secure against unauthorized access at any location, including an employee's home, all documents and equipment (laptops, smart phones, etc.) that may contain health information.
- ✓ Use PHI only as necessary in their jobs.

SECURE



TRUE OR FALSE

It is ok to leave information containing PHI on your desk when you leave for a break or lunch but you must secure the information overnight.



ANSWER

FALSE

You must remove any information containing PHI from public view when you leave your workstation.



Requirements for Data Security Protection

Network Security Access Controls

- Firewalls
- Access Control Lists
- User Authentication

System Access

- Follow prescribed procedures of Agency

Authentication

- Unique User ID
- Strong passwords changed at prescribed intervals
- Strong passwords required for administrative accounts



Requirements for Data Security Protection

Hardware (servers, workstations, etc.)

Must have current anti-malware installed and updated regularly

Backed up at agency prescribed intervals

Offsite backup

Backup tapes or electronic storage devices will not be left unattended when in transport

Failed hard drives cannot be returned to the hardware vendor



Requirements for Data Security Protection

Hardware (servers, workstations, etc.) cont.

Workstations cannot be reused until they have been cleansed using a DoD standard disk wiping software

Operating systems will be kept current with security patches



Requirements for Data Security Protection

Mobile Devices shall have:

- Encryption software installed
- Password/Passcode protection enforced

Software

- Non-Standard software will not be installed on any hardware without prior approval
- Workstations will be configured to not allow installation of non-standard software



Requirements for Data Security Protection

Email

PHI will be encrypted using the State's standard software



A Breach

A Breach is defined as “an unauthorized acquisition, access, use, or disclosure of unsecured PHI that compromises the privacy or security of such information.”

As of September 2009, the HITECH Act modified HIPAA to require that individuals be notified of any “breach” of their PHI.



A Breach – Unsecured PHI

The new definition of breach applies to both paper and electronic records, but the primary concern behind the law is for electronic records.

For instance, one of the more common breaches is when a laptop computer or other mobile storage device is lost or stolen. If the PHI on this device is not encrypted, then a breach is deemed to have occurred. If the PHI is encrypted, it is considered secure and not deemed to be a breach.



What happens when a Breach occurs?

Given the exceptions to the definition of a breach and the possibility of PHI being encrypted, if you have reason to be concerned that PHI has been breached, **notify your supervisor promptly.**

If you become aware of a possible breach of an agency's electronic security system, you are responsible for reporting the incident to your supervisor, creating an online help desk ticket, and then notifying the Chief Information Security Officer.

If necessary the CIO and CISO can implement an Incident Response plan.



TRUE OR FALSE

If a breach has occurred, the affected individual(s) must be notified of any breach of their PHI.



ANSWER

TRUE

If you have reason to believe that PHI may have been breached, you must notify your supervisor immediately to ensure appropriate action is taken.



Penalties

Serious penalties for the State of Missouri and its employees are possible if PHI is improperly disclosed or misused.

The **CIVIL PENALTIES** imposed on the State are based on each record disclosed. The penalties are:

Tier A Penalty

Imposed when the offender did not know, and by exercising reasonable diligence would not have known:

\$100 for each violation, up to a max of \$25,000.

Tier B Penalty

Imposed if the violation was due to reasonable cause and not willful neglect:

\$1,000 for each violation, up to a max of \$100,000.

For the most serious violations, the penalty is \$50,000 per violation up to \$1.5 million for each incidence.

Employees who fail to comply with HIPAA and the HITECH Act are subject to disciplinary action up to, and including, termination.



Criminal Penalties

Section 1177 of the HIPAA law established criminal penalties if a person knowingly violates the law. The possible penalties are as follows:

If a person knowingly obtains or misuses PHI in violation of the regulations, they could be fined up to \$50,000 and sentenced up to one year in jail.



If the misuse of PHI involves or is done under false pretense, the person could be fined up to \$100,000 and sentenced up to five years in jail.



If the misuse is for commercial or personal financial gain, or done for malicious harm, the person could be fined up to \$250,000 and sentenced up to ten years in jail.



Business Associates

Under HIPAA, business associates are any person or entity that performs certain functions on behalf of, or provides services to, a covered entity – and those functions **involve the use or disclosure of protected health information.**

ITSD is a business associate of all consolidated State of Missouri HIPAA covered agencies.

In 2009, the HITECH law extended HIPAA privacy and security requirements to the business associates of covered entities.



Summary

Federal law provides that PHI is confidential information and State employees **MUST** protect this information from unauthorized releases.

Employees are allowed to access the minimum necessary data in performing their jobs.

New federal law has defined a breach of PHI as “an unauthorized acquisition, access, use, or disclosure of their unsecured PHI that compromises the privacy or security of such information.”

All employees are required to promptly report suspected breaches.

Potential penalties for careless, negligent and intentional disclosures have been dramatically increased.



Health Insurance Portability and Accountability Act (HIPAA) Training

Using and Securing Protected Health Information (PHI)

Thank you for viewing this training program. Please remember that as a state employee it is your responsibility to adhere to the strategies and procedures outlined in this program.

Please discuss any questions or concerns you have about your ability to comply with this information with your supervisor.

This presentation was created by:



with technical assistance from:

Office of Administration
Information Technology Services Division

