



HIPPA Policy & Training

Mandatory Training Requirements for all employees, contractors, and associates:

- 1) Complete OSHAacademy, HIPPA Privacy Training module #625. Printed copies of you Transcript of Completion and Certificate MUST be on file prior to ANY interaction with any client, associate, or vendor of Hearthstone House. Please find included below a link to and an overview of the required basic training.**
- 2) Review/study the Hearthstone House HIPPA Policy, be prepared to illustrate your full understanding of said policy.**
- 3) Be prepared to illustrate how the HIPPA Policy applies to the handling of (paper, digital or verbal) related operational guidelines, not limited to but including; Pre Entry Screening, Agreements, Contracts, Assessments, House Rules, Grievance Policy, Good Neighbor Policy, and implementation of Signature Recovery Plan.**
- 4) It is YOUR responsibility to ensure the Hearthstone HIPPA Policy which often exceeds the base Federal HIPPA guidelines are met at all times.**
- 5) It is your responsibility to proactively report any concerns or issues that may interfere with the intent and purpose of the Hearthstone House HIPPA Policy to the HIPPA Security Officer.**
- 6) Complete both HIPPA Privacy Security Training and secure file/data password and procedures orientation.**

Protecting client privacy, trust, security and confidentiality are the pillars of Hearthstone House and the Signature Plan of Care.



HIPAA stands for "Health Insurance Portability and Accountability Act" (HIPAA). President Bill Clinton signed the bill into law on August 21, 1996. It is said to be the most significant act of Federal legislation to affect the health care industry since Medicare and Medicaid were rolled out in 1965. The law officially became effective on July 1, 1997. HIPAA required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations to protect the privacy and security of certain health information. Healthcare providers and employees should take this important course to receive a summary of key elements of the HIPAA rules.

Training Module #625 [HIPAA Privacy Training](#)

Modules: 3 Hours: 3 Sectors: Healthcare

OSHAcademy Honor Code Pledge

Introduction

By registering as an OSHAcademy student, you are joining a worldwide community of learners. The aspiration of OSHAcademy is to provide anyone in the world who has the motivation and ability to engage in coursework to attain the best educational experience possible. You are part of the community who will help OSHAcademy achieve this goal.

OSHAcademy depends upon your motivation to learn the material and to do so with honesty. In order to participate in OSHAcademy training, you must agree to the following OSHAcademy Honor Code:

OSHAcademy Honor Code

By registering as an OSHAcademy student, I confirm I will:

- personally complete all course exams without the assistance or help of another person
- not complete or submit an exam on behalf of another person
- maintain only one user account and not let anyone else use my username and/or password
- not engage in any activity that would dishonestly improve my results, or improve or hurt the results of others
- not post or distribute answers to exam questions used to assess student performance
- not engage in any fraudulent or illegal activity associated with my OSHAcademy account

OSHAcademy students are encouraged to:

- Read all course material, view course videos, and complete course quizzes prior to taking the final exams.
- Ask questions when an instructional concept is unclear or not understood.

Changing the Honor Code

Please note that we review and may make changes to this Honor Code from time to time. Any changes to this Honor Code will be effective immediately upon posting with an updated effective date. By accessing the Site after any changes have been made, you signify your agreement on a prospective basis to the modified Honor Code and any changes contained therein.

Last Updated: April 27th, 2018

HIPAA Overview

Key Topics

- HIPAA Law Components
- Privacy and Security Rule
- Protecting Patients' Privacy
- Covered Entities
- Personal Rights
- Good Privacy Practices
- Protected Information
- Sharing Health Information
- Protected Healthcare Identifier
- Electronic Protected Health Information
- Non-Compliance Enforcement
- Training Requirements
- Filing Complaints
- Civil Money and Criminal Penalties
- Administrative, Physical, and Technical Safeguards
- Employers and Health Information in the Workplace

Target Audience

- Employee/Contractor/Associate

Privacy Rule

The Privacy Rule establishes national standards for the protection of certain health information. It applies to all forms of individuals' protected health information, whether electronic, written, or oral. The major goal of the Privacy Rule is to make sure an individuals' health information is properly protected while allowing the flow of health information needed to provide high quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of those who need care.

The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf.

For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Notify patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Secure patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

Protected Information

The following information is always protected for each individual:

- information your doctors, nurses, and other health care providers put in your medical record
- conversations your doctor has about your care or treatment with nurses and others
- information about you in your health insurer's computer system
- billing information about you at your clinic
- most other health information about you held by those who must follow these laws

Covered entities must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly. They must also have procedures in place to limit who can view and access your health information, as well as implement training programs for employees about how to protect your health information.

Does the HIPAA Privacy Rule permit hospitals and other health care facilities to inform visitors or callers about a patient's location in the facility and general condition?

Answer:

Yes. Covered hospitals and other covered health care providers can use a facility directory to inform visitors or callers about a patient's location in the facility and general condition. The Privacy Rule permits a covered hospital or other covered health care provider to maintain in a directory certain information about patients – patient name, location in the facility, health condition expressed in general terms that does not communicate specific medical information about the individual, and religious affiliation. The patient must be informed about the information to be included in the directory, and to whom the information may be released, and must have the opportunity to restrict the information or to whom it is disclosed, or opt out of being included in the directory. The patient may be informed, and make his or her preferences known, orally or in writing. The facility may provide the appropriate directory information – except for religious affiliation – to anyone who asks for the patient by name. Religious affiliation may be disclosed to members of the clergy, who are given additional access to directory information under the Rule. (See other FAQs at this site by searching on the term “clergy”.)

Even when, due to emergency treatment circumstances or incapacity, the patient has not been provided an opportunity to express his or her preference about how, or if, the information may be disclosed, directory information about the patient may still be made available if doing so is in the individual's best interest as determined in the professional judgment of the provider, and would not be inconsistent with any known preference previously expressed by the individual. In these cases, as soon as practicable, the covered health care provider must inform the patient about the directory and provide the patient an opportunity to express his or her preference about how, or if, the information may be disclosed. See 45 CFR 164.510(a).

When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?

Answer:

The Privacy Rule is balanced to protect an individual's privacy while allowing important law enforcement functions to continue. The Rule permits [covered entities](#) to disclose protected health information (PHI) to law enforcement officials, without the individual's written authorization, under specific circumstances summarized below. For a complete understanding of the conditions and requirements for these disclosures, please review the exact regulatory text at the citations provided. Disclosures for law enforcement purposes are permitted as follows:

- **To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.** The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information ([45 CFR 164.512\(f\)\(1\)\(ii\)\(A\)-\(B\)](#)).
- **To respond to an administrative request**, such as an administrative subpoena or investigative demand or other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used ([45 CFR 164.512\(f\)\(1\)\(ii\)\(C\)](#)).
- **To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but the covered entity must limit disclosures** of PHI to name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request ([45 CFR 164.512\(f\)\(2\)](#)).

This same limited information may be reported to law enforcement:

- **About a suspected perpetrator of a crime when the report is made by the victim who is a member of the covered entity's workforce** ([45 CFR 164.502\(j\)\(2\)](#));
- **To identify or apprehend an individual who has admitted participation in a violent crime** that the covered entity reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual's request for therapy, counseling, or treatment related to the propensity to commit this type of violent act ([45 CFR 164.512\(j\)\(1\)\(ii\)\(A\), \(j\)\(2\)-\(3\)](#)).
- **To respond to a request for PHI about a victim of a crime, and the victim agrees.** If, because of an emergency or the person's incapacity, the individual cannot agree, the covered entity may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person

broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree, and the covered entity believes in its professional judgment that doing so is in the best interests of the individual whose information is requested (45 CFR 164.512(f)(3)).

Where child abuse victims or adult victims of abuse, neglect or domestic violence are concerned, other provisions of the Rule apply:

- **Child abuse or neglect may be reported** to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required (45 CFR 164.512(b)(1)(ii)).
- **Adult abuse, neglect, or domestic violence may be reported** to a law enforcement official authorized by law to receive such reports (45 CFR 164.512(c)):
 - If the individual agrees;
 - If the report is required by law; or
 - If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations (see 45 CFR 164.512(c)(1)(iii)(B)).
 - Notice to the individual of the report may be required (see 45 CFR 164.512(c)(2)).
- **To report PHI to law enforcement when required by law** to do so (45 CFR 164.512(f)(1)(i)). For example, state laws commonly require health care providers to report incidents of gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws.
- **To alert law enforcement to the death of the individual**, when there is a suspicion that death resulted from criminal conduct (45 CFR 164.512(f)(4)).
 - Information about a decedent may also be shared with **medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties**(45 CFR 164.512(g)(1)).
- **To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the covered entity's premises** (45 CFR 164.512(f)(5)).
- **When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity**, specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime (45 CFR 164.512(f)(6)). This provision does not apply if the covered health care provider believes that the individual in need of the emergency medical care is the victim of abuse, neglect or domestic violence; see above Adult abuse, neglect, or domestic violence for when reports to law enforcement are allowed under 45 CFR 164.512(c).
- When consistent with applicable law and ethical standards:
 - To a law enforcement official reasonably able to **prevent or lessen a serious and imminent threat to the health or safety of an individual or the public** (45 CFR 164.512(j)(1)(i)); or
 - **To identify or apprehend an individual who appears to have escaped from lawful custody** (45 CFR 164.512(j)(1)(ii)(B)).

- **For certain other specialized governmental law enforcement purposes**, such as:
 - **To federal officials authorized to conduct** intelligence, counter-intelligence, and other national security activities under the National Security Act (45 CFR 164.512(k)(2)) or to provide protective services to the President and others and conduct related investigations (45 CFR 164.512(k)(3));
 - **To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody** of an inmate or others if they represent such PHI is needed to provide health care to the individual; for the health and safety of the individual, other inmates, officers or employees of or others at a correctional institution or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility (45 CFR 164.512(k)(5)).

Except when required by law, the disclosures to law enforcement summarized above are subject to a minimum necessary determination by the covered entity (45 CFR 164.502(b), 164.514(d)). When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose (45 CFR 164.514(d)(3)(iii)(A)). Moreover, if the law enforcement official making the request for information is not known to the covered entity, the covered entity must verify the identity and authority of such person prior to disclosing the information (45 CFR 164.514(h)).

Created 7/23/04

Content created by Office for Civil Rights (OCR)
Content last reviewed on July 26, 2013

Risk Analysis and Management

HIPAA requires health care providers to conduct risk analysis.

The Administrative Safeguards provisions in the HIPAA Security Rule require covered entities to perform a risk analysis as part of their security management processes.

A **risk analysis** process includes, but is not limited to, the following activities:

- Evaluating the likelihood and impact of potential risks to e-PHI.
- Implementing appropriate administrative, physical, and technical security measures to address the risks identified in the risk analysis.
- Documenting the chosen security measures and, where required, the rationale for adopting those measures.
- Maintaining continuous, reasonable, and appropriate security protections.

Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI.

Ensure unauthorized access to e-PHI with transmission security.

Technical Safeguards. Here are examples of technical safeguards that can be implemented to protect e-PHI:

- **Access Controls:** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).
- **Audit Controls:** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- **Integrity Controls:** A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
- **Transmission Security:** A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

Organizational Requirements

If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.

Policies, Procedures, and Documentation Requirements

Covered entities must develop, adopt, and maintain HIPAA Security Rule policies and procedures.

HIPAA provisions require covered entities to develop and maintain policies, procedures, and documentation to comply with the Security Rule. A covered entity must:

- adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule.
- maintain written security policies and procedures and written records of required actions, activities or assessments.
- maintain written security policies, procedures, and records of required actions, activities or assessments for six years after the date of creation or last effective date, whichever is later.
- periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI).

The federal government can impose fines and penalties for non-compliance.

In general, state laws contrary to the HIPAA regulations are pre-empted by the federal requirements, which means the federal requirements will apply. "Contrary" means it would be impossible for a covered entity to comply with both the state and federal requirements, or the provision of state law is an obstacle to accomplishing the full purposes and objectives of the HIPAA provisions.

Enforcement and Penalties for Non-Compliance

If a covered entity's employees and/or volunteers do NOT follow the rules set out by HIPAA, the federal government has the right to do the following:

- conduct an investigation
- impose fines and/or jail sentences, if found guilty

Civil Penalties

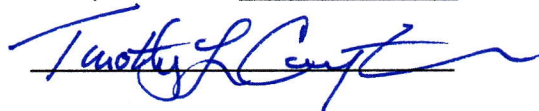
Unintentional HIPAA violations could result in monetary penalties. Health and Human Services may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

Criminal Penalties

Knowingly making unauthorized disclosure of PHI, intentionally selling information, and offenses that include false pretenses may result in substantial fines (\$50,000 - \$250,000) and/or imprisonment. The U.S. Department of Justice will enforce the criminal sanctions.

Sign 
HIPPA Security Officer TIMOTHY L CARPENTER
Address PO BOX 1965
City CYPRESS, TX 77410
Cell : 832-298-1970

Completion Date 7-8-18



Approval Date 7-8-18



This is to certify that

Timothy L Carpenter

*Has successfully completed all assignments and final exam requirements for the following
OSHAcademy Occupational Safety & Health Course:*

HIPAA Privacy Training

Topics covered in this training include: HIPAA Law Components; Training Requirements; Privacy and Security Rule; Protecting Patients' Privacy; Protected Healthcare Identifier; Good Privacy Practices; Personal Rights; Protected Information; Employers and Health Information in the Workplace; Sharing Health Information; Filing Complaints; Covered Entities; Health Plan, Health Care Clearinghouse, and Providers; Electronic Protected Health Information; Administrative, Physical, and Technical Safeguards; Non-Compliance Enforcement; Civil Money and Criminal Penalties.

Steven J. Geigle, MA, CET, CSHM
Director, Instructor
OSHAcademy Safety and Health Training

This training conforms to OSHA CBT Training Standards and ANSI Z490.1, Criteria for Accepted Practices in Safety, Health and Environmental Training. OSHAcademy training is endorsed by the National Safety Management Society and is recognized by the Institute for Safety and Health Management.

625

Recognized by



Original certificates are embossed with the official OSHAcademy raised stamp. Certificates can be validated through the OSHAcademy website.

449541	07.08.2018	3
Student #	Issue Date	Hours

OSHAcademy is a division of
Geigle Safety Group, Inc.
15220 NW Greenbrier Pkwy, Ste 230
Beaverton, OR, USA, 97006
Tel: +1.971.217.8721
Website: www.oshatrain.org



Validate Certificate

Unique QR Code