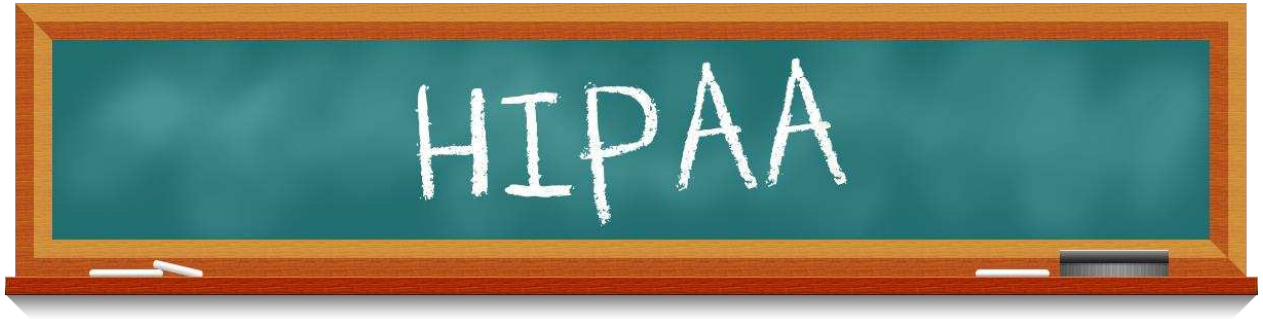
HIPAA PRIVACY TRAINING

Presented by **Oshaguard**

"Compliance Solutions for Healthcare"



HIPAA, or the Health Insurance Portability and Accountability Act, was signed into law into 1996. Health and Human Services (HHS) is the agency responsible for HIPAA regulations. The primary goal of the law is to protect the confidentiality and security of protected health information or PHI and help the healthcare industry control administrative costs.

HIPAA regulations apply to **Covered Entities** and **Business Associates**. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

Covered Entities are healthcare providers, health plans and healthcare clearinghouses that transmit medical information electronically. It requires them to protect the privacy of individually identifiable health information that they create, receive or maintain on their patients.

Covered entities include, but are not limited to:

- ☑ Medical and dental offices
- ☑ Hospitals
- ☑ Chiropractors
- ☑ Healthcare plans
- ☑ Clearinghouses
- ☑ Business associates and their subcontractors
- ☑ Pharmacies
- ☑ Labs
- ☑ Nursing homes

Business Associates are people or an entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Business Associates include, but are not limited to:

- ☑ Claims processing
- ☑ Data analysis
- ☑ Billing services and/or healthcare clearinghouses
- ☑ Practice management
- ☑ Accountants, auditors, consultants
- ☑ Technical support personnel from companies outside your workforce
- ☑ Shredding companies

Effective March 26, 2013, all subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information*.

You may disclose PHI to a Business Associate to carry out treatment, payment and healthcare operations only after a signed Business Associate Agreement is in place.

** Under The HITECH Act the U.S. Department of Health & Human Services can take enforcement action directly against a business associate that fails to comply with the Privacy or Security Rules.*

HIPAA Regulations Address

- ☑ Patient Privacy
- ☑ Security of Information
- ☑ Transactions and Code Sets

The HIPAA Privacy rule provides patients with certain rights and addresses the security of their protected health information.

Protecting the confidentiality, integrity and availability of electronic protected health information (ePHI) is addressed by the HIPAA Security Rule.

Code Sets for medical data are required in administrative and financial health care transactions for diagnosis, procedures and drugs. This standardization for electronic exchange of patient identifiable information better facilitates transactions and lowers administrative costs.

PHI is “individually identifiable” if it includes any of these 18 types of identifiers:

- ☑ Patient names
- ☑ Any geographic subdivision smaller than a state including street address, city, county, precinct, zip code and their equivalent geocodes
- ☑ All elements of the date, except the year related to an individual including birthdates, admission date, discharge date and date of death
- ☑ Telephone and fax numbers
- ☑ E-mail addresses
- ☑ Social Security numbers
- ☑ Medical records numbers

PHI is “individually identifiable” if it includes any of these 18 types of identifiers:

- ☑ Account numbers
- ☑ Certificate/License numbers
- ☑ Vehicle identifiers and serial numbers
- ☑ Biometric identifiers, including finger prints or voice prints
- ☑ Photographic images
- ☑ Web Universal Resource Locators (URLs)
- ☑ Internet Protocol (IP) address numbers
- ☑ And any other unique identifying numbers, characteristics, or codes that could identify an individual

Patients' Rights Under HIPAA

- ☑ Right to Privacy and the Uses / Disclosures of their PHI
- ☑ Right to Access and Accounting of Disclosures
- ☑ Right to Request Amendment of health information
- ☑ Right to Restrict Disclosure to Health Plan. *Only if they paid for the service in full out-of-pocket.*
- ☑ Right to Complain if they feel their information was disclosed inappropriately
- ☑ Right to be Notified in the event of a breach if PHI has been acquired, accessed, used or disclosed in an unauthorized manner

The Notice of Privacy Practices must be made available on the first treatment visit and they should sign an Acknowledgement of Receipt.

This facilities Privacy Policies and Procedures require you to:

- ☑ Collect, access, use and disclose protected health information (PHI) only for legitimate job function and are allowed by the law.
- ☑ Safeguard PHI in your possession, whether it's in paper of electronic format (ePHI).
- ☑ Properly dispose of documents containing PHI. Shred any media that has "individually identifiable" information.
- ☑ Use screensavers and/or logoff when the computer is not in use. Some programs have de-identification features that will hide names on computer patient schedules.

This facilities Privacy Policies and Procedures require you to:

- ☑ Position monitors so passers-by cannot view confidential information that might be visible.
- ☑ No information should be written on the outside jacket of charts.
- ☑ Charts should never be left opened on desks and/or in areas where unauthorized individuals have access.
- ☑ Never make reference to a patients' protected health information in an area where the comments could be overheard.

The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requires covered entities to implement reasonable safeguards that reflect their particular circumstances.

HIPAA Privacy rules recognize that oral communications often must occur freely and quickly in treatment settings. It permits certain incidental uses and disclosures of protected health information to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

Covered entities may use or disclose PHI for the purpose of treatment, payment and healthcare operations. With a few exceptions, you must obtain written authorization from your patients or their personal representative before you use or disclose their PHI for purposes other then treatment, payment or healthcare operations.

Signed Authorizations are not required for:

- ☑ Cases of any emergency involving your care, if incapacitated
- ☑ Disclosures required for reporting abuse, neglect or domestic violence
- ☑ Disclosures for public health activities
- ☑ Disclosures for health oversight agencies
- ☑ Disclosures in response to federal or state laws
- ☑ Disclosures to the military
- ☑ Disclosures to law enforcement officials
- ☑ Disclosures to federal officials for national security

Signed Authorizations are not required for:

- ☑ Disclosures in response to subpoenas, court orders and other judicial processes
- ☑ Disclosures in response to a Health and Human Services (HHS) request or compliance review
- ☑ Uses for marketing purposes that are limited to promotional gifts of a nominal value and/or face-to-face communications with a patient
- ☑ Effective March 26, 2013, immunization records for students may be released without an authorization
- ☑ If an individual is deceased you may disclose PHI to a family member or individual involved in care or payment prior to death

Employees that handle Social Security numbers (SSNs) need to take extra precautions. Misuse of SSNs can put individuals at risk for identity theft.

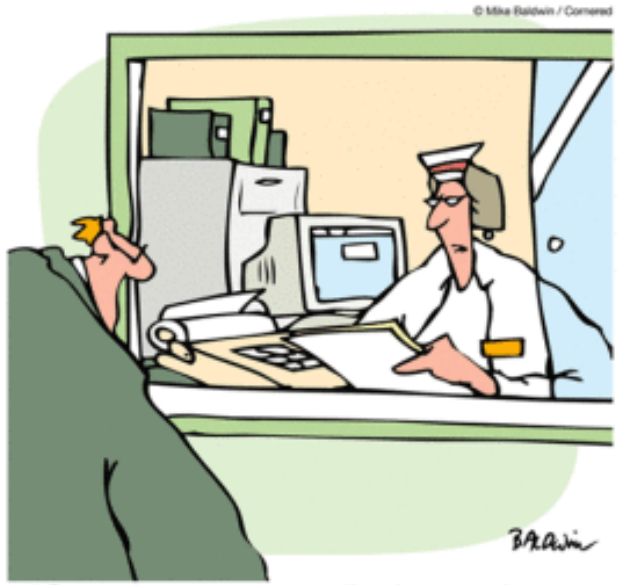
- ☑ Use the SSNs only when it is required. Truncate or mask the SSN in systems or on paper printouts whenever possible
- ☑ Disclose SSNs only to those that have a need to know and are authorized to receive the information. Documents containing SSNs should be put away so they are not left out when away from your desk.

Employees that handle Social Security numbers (SSNs) need to take extra precautions. Misuse of SSNs can put individuals at risk for identity theft.

- ☑ Identify and implement ways to eliminate the use of SSNs, when possible (e.g., removal from forms, assigning a randomly generated identifier.)
- ☑ Employees are required to report suspected privacy violations or incidents to your Privacy Officer immediately. Failure to report security incidents will result in disciplinary action as required under our sanction policy. Disciplinary action will depend on the nature and frequency of security incidents and will range from verbal reminders to termination.

Sending and receiving information by fax can violate the Privacy Rule if employees who are responsible for these tasks are careless.

- ☑ Fax machines should be located in areas that are restricted to staff only
- ☑ Use a fax transmittal sheet
- ☑ Verify the recipient's fax number prior to sending PHI
- ☑ Don't leave sensitive information in the tray
- ☑ Take your time and key fax numbers in correctly



"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

Tips for sending PHI by mail include:

- ☑ Information should be sent in an opaque or confidential envelope
- ☑ Follow-up to verify the package was received
- ☑ When possible, use a traceable delivery service

Breach Notification Rule

The rule defines “Unsecured Protected Health Information” to mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS guidance.

It’s presumed that any acquisition, access, use or disclosure of unsecured PHI is a breach unless you can demonstrate that there is a low probability that the PHI has been compromised based on a 4 factor risk assessment. The rule defines “Breach” to mean the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI.

If a breach has occurred, Notification to the Secretary of HHS of a Security Breach of Unsecured Protected Health Information is required. If more than 500 individuals are involved in the breach, then you will notify Health and Human Services concurrently with the individual notifications. For breaches involving fewer than 500 individuals, you will maintain an internal log or other documentation of such breaches and annually submit the log to HHS no later than 60 days after the end of each calendar year.

Violation Category	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
For violations in which it is established that the covered entity or business associate **did not know** and, by exercising reasonable diligence, would not have known that the covered entity violated a provision	$100-$50,000	$1,500,000
For a violation in which it is established that the violation was due to **reasonable cause** and not to willful neglect	$1,000-$50,000	$1,500,000
for a violation in which it is established that the violation was due to **willful neglect and was timely corrected**	$10,000-$50,000	$1,500,000
For a violation in which it is established that the violation was due to **willful neglect and was NOT timely corrected**	$50,000	$1,500,000

THE END.

Congratulations. You have completed your training on HIPAA Privacy. All employees should sign the training record and "Employee Confidentiality Statement" found at the back of your manual. If you have any questions about site specific information not covered on this training module, please talk to your HIPAA Privacy Officer.

DISCLAIMER This presentation you just viewed was intended to offer training guidelines based on HIPAA Privacy Standards affecting healthcare facilities. The information contained on this presentation was current at the time of production and Oshaguard believes the information to be accurate and disclaims any liability or damage which may result from the use of this presentation, furthermore should any of the information contained in these sections conflict with federal, state or local regulations, Oshaguard and the authors assume no responsibility or liability for any violation(s) which may result.