



HIPAA, Confidentiality & Conflict of Interest Training

January Quality Topic



Section 1:

What is HIPAA?



HIPAA Overview

- HIPAA is the acronym of the **Health Insurance Portability and Accountability Act of 1996** and was enacted as part of a broad Congressional attempt at incremental healthcare reform.
- Signed into law on August 21, 1996 by the Clinton administration, HIPAA is considered to be the most significant body of health-care legislation to be enacted since Medicare.
- The main purpose of this federal statute was to help consumers maintain their insurance coverage, but it also includes a separate set of provisions called **Administrative Simplification**.



HIPAA Provisions

- HIPAA is made up of several provisions designed to protect the healthcare consumer in a number of ways
- At a high level, HIPAA legislation includes Titles I – V as follows:
 - ▶ **Title I**
Insurance portability: Helping workers and their families maintain insurance coverage when they change or lose a job
 - ▶ **Title II**
Administrative simplification: Providing legislation around privacy, security and electronic data
 - ▶ **Title III**
Tax-related provisions: Allowing employees to set up medical savings accounts.
 - ▶ **Title IV**
Enforcement of group health care requirements.
 - ▶ **Title V**
Revenue offsets: For company-based life insurance plans



Administrative Simplification (Title II)

It is HIPAA Title 2 legislation for Administrative Simplification that is of greatest importance to Medical Office Clients; especially, the legislation concerning electronic data.

Provisions for electronic data are divided as follows:

- ▶ **Transactions and Code Sets**
- ▶ **Privacy**
- ▶ **Security**
- ▶ **Identifiers**



Transactions and Code Sets

- The Standards for the Electronic Data Interchange (EDI) of healthcare information from one company to another for a specific purpose.
- Code Set standards are for any coded information within a transaction, i.e. diagnosis codes, procedure codes, inpatient services codes, and drug codes.



Privacy

- Standards designed to protect an individual's identifiable health information from unauthorized disclosure or use in any form, whether communicated or maintained electronically, on paper or orally.



Security

- Standards requiring that specific procedures and methods be implemented to protect individually identifiable health information from loss or inappropriate disclosure.
- These requirements are designed to be technologically neutral and scalable.



Identifiers

- Dep. of Health and Human Services (HHS) established Uniform Identifier Standards, which are national standards of identification for use on all claims and other data transmissions.
- Included are:
 - ▶ Employer Identifier Number (EIN)
 - ▶ National Health Plan Identifier (PlanID)
 - ▶ National Provider Identifier (NPI)
 - ▶ Unique Healthcare ID for Patients (UHID).



HITECH Act

- The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law on February 17, 2009.
- Promotes the adoption and meaningful use of health information technology, including:
 - ▶ **Subtitle A:** Promotion of Health Information Technology using Electronic Health Records (EHRs)
 - ▶ **Subtitle B:** Testing of Health Information Technology
 - ▶ **Subtitle C:** Grants and Loans Funding
 - ▶ **Subtitle D:** Improved Privacy and Security Provisions



HITECH Act

- **Subtitle A:**

Setting meaningful use of interoperable EHR adoption in the health care system as a critical national goal and incentivized adoption of certified EHRs.

Starting in 2015, hospitals and doctors will be subject to financial penalties under Medicare if they are not using electronic health records

- **Subtitle D:**

How privacy and security concerns associated with the electronic transmission of health information are addressed through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules, including:

- ▶ Four categories of violations that reflect increasing levels of culpability
- ▶ Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation
- ▶ A maximum penalty amount of \$1.5 million for all violations of an identical provision.
- ▶ Striking the previous bar on the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (such violations are now punishable under the lowest tier of penalties)
- ▶ Providing a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect



Security & Privacy Tips

SECURITY

- ▶ Always use a password to protect your computer and voicemail.
- ▶ If your login fails, contact IT immediately.
- ▶ **NEVER** share your passwords with others; not even IT or your Supervisor.
- ▶ If you leave your workstation, either activate your screensaver or turn off your monitor.

Shortcuts for activating your screensaver:

- Ctrl + Alt + Delete
- Press the Windows logo key + L



- ▶ If you see a person in a restricted area without a badge, stop them, find out who they are looking for, and escort them back to the front entrance to wait.



Security & Privacy Tips

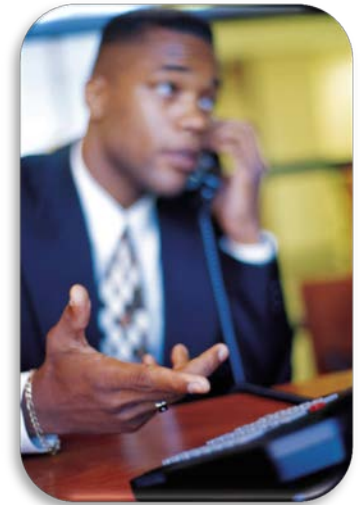
PRIVACY

- ▶ Empty your personal shred box at the end of each business day in the office shred bin.
- ▶ When you leave your workstation, turn all papers facedown or lock them in a file cabinet.
- ▶ Check fax machines and/or printers each hour to remove paperwork that may contain PHI.



Reporting S & P Violations

- If you suspect a violation in any security or privacy practices, **please notify your supervisor immediately.**
- You can also contact your compliance officer to report incidents or complaints involving HIPAA violations.
 - ▶ **Compliance Officer:** Melissa Nollkamper
214.574.2370
melissa.nollkamper@healthsmart.com
- All reported violations are monitored for adverse trends and are reported in our monthly quality meetings for tracking purposes.





Section 2:

Confidentiality & PHI



What is Confidentiality?

Confidentiality is defined as:

- Ensuring that information is accessible only to those authorized to have access
- One of the cornerstones of Personal Health Information (PHI) security



What is PHI?

- PHI is defined as any individually identifiable health information
- Examples of PHI include:
 - ▶ Name
 - ▶ Address
 - ▶ Phone Numbers
 - ▶ Email Addresses
 - ▶ Age and Gender
 - ▶ Social Security Numbers
 - ▶ Photographs
 - ▶ Medical Records
 - ▶ Biometric Information
 - ▶ Insurance or Health Plan Information



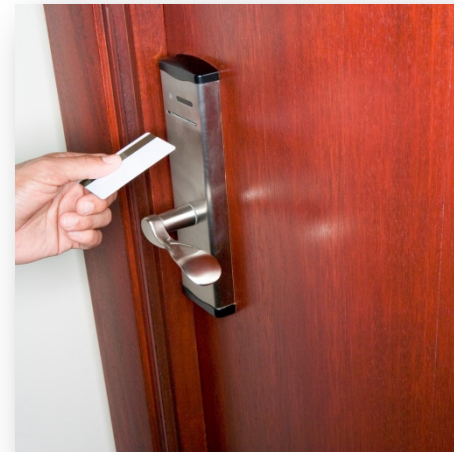
PHI Basics

- PHI comes in many formats, including paper records, oral communication and electronic files
- Confidentiality of PHI is maintained by not sharing it with **ANYONE**, including co-workers, other patients and family members
- Your use of PHI should be the “**minimum necessary**” or limited to what you need to do your job



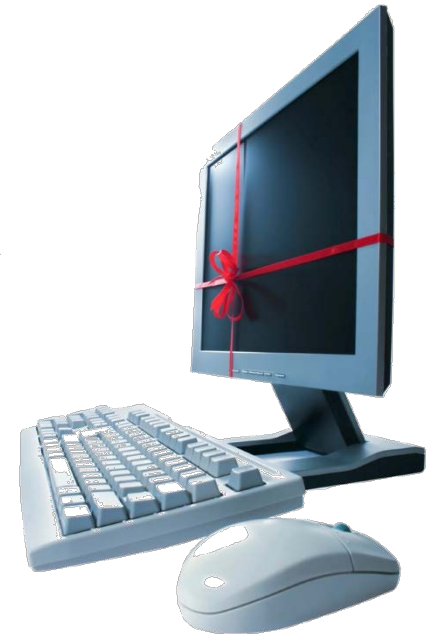
Tips on Protecting PHI

- File Cabinets containing patient information should be closed and locked when not in use
- Never leave information open on your desk – always turn face down if you leave your area, or lock up if overnight
- Office Keys/Badges or Key Codes should not be copied or shared without approval



More Tips on Protecting PHI

- Double check addresses and phone/fax numbers to ensure the correct person receives the information
- Verify that all patient information in JIVA is current and up to date prior to pre-cert
- Computer terminals should be password protected with screen savers
- **NEVER** share your password with others or leave it visible, and change your passwords frequently
- Limit work conversations to your work area to prevent others overhearing PHI
- Keep your voice volume to a normal level while on the phone to prevent others from over hearing your conversation that may contain PHI information



PHI Violations

Some examples of PHI violations include:

- ▶ Sending PHI to the wrong person via mail, fax, or email
- ▶ Leaving PHI on voicemails or with family members
- ▶ Incorrect PHI logged in JIVA system that results in future pre-cert errors
- ▶ Placing patient PHI in subject line of emails



What to do if a Violation Occurs?

Step 1: Notify your supervisor

Step 2: Take any corrective action needed to resolve the violation

Step 3: Request and fill out a “HIPAA Incident Form” from your Supervisor or HIPAA privacy officer (Melissa Nollkamper, VP of Clinical Economics)

Step 4: Once form is signed and returned, the incident will be logged for quality tracking and reporting



Your Responsibilities with PHI

- Be sensitive to other's PHI
- Respect Patient's Privacy Rights
- Keep updated on HealthSmart Security & Privacy Policies and Procedures
- Participate in Security and Privacy Training
- Each January re-sign your confidentiality and conflict of interest agreements
- Report any privacy concerns to your supervisor or privacy officer

Talk with your supervisor if you have any additional questions regarding PHI and confidentiality



Employee Confidentiality in the Workplace

As outlined in the HealthSmart Employee Handbook (p. 30), Ethical Conduct is integral to the success of this Company.

Basic reminders concerning Employee Confidentiality:

- ▶ Respect the privacy and dignity of the individual employee of the Company and any related affiliates
- ▶ Create a work environment free of any form of harassment
- ▶ Represent the Company in a manner in which is law abiding and sensitive to the needs and justifiable expectations of your fellow employees
- ▶ Exercise discretion while interacting with their fellow employees
- ▶ Personal disclosures should be made thoughtfully and any work-related information must not be shared at all or shared very carefully, if required
- ▶ Refrain from sharing information that the organization considers sensitive.
- ▶ All employees should maintain a professional attitude at all times.



Confidentiality Agreement

HealthSmart Care Management Solutions requires **ALL** staff to sign a written statement that acknowledges that all information related to HealthSmart CMS, and its operations is strictly confidential and that under no circumstances can there be any unauthorized disclosure of such information.

The HealthSmart Confidentiality Agreement must be reviewed and re-signed by all staff annually.

Your Confidentiality Agreement has been included with your January Quality Topic email.

Please print, sign and return your agreement to Karen Owens by **January 31st**.

Email: karen.owens@healthsmart.com Fax: 214.574.2355





Section 3:

Conflict of Interest



Definition

Conflict of Interest

Any situation in which an individual or corporation is in a position to exploit a professional or official capacity in some way for their personal or corporate benefit.



Types of Conflict of Interest

Self-dealing

- ▶ In which public and private interests collide.
For example: Issues involving privately held business interests

Outside employment

- ▶ In which interests of one job contradict another

Family interests

- ▶ In which a spouse, child, or other close relative is employed (or applies for employment) or where goods or services are purchased from such a relative or a firm controlled by a relative.

For this reason, many employment applications ask if one is related to a current employee.

Gifts

- ▶ From friends who also do business with the person receiving the gifts.
Such gifts may include non-tangible things of value such as transportation and lodging.



Handling Conflicts of Interest

Removal

The best way to handle conflicts of interest is to avoid them entirely. Short of avoiding conflicts of interest, the best way to deal with them is one or more of the following (mitigation) measures:

Disclosure

- Commonly, employees should disclose any potential conflict of interest with their employer.

Recusal

- Those with a conflict of interest are (ethically) expected to recuse themselves from (i.e., abstain from) decisions where such a conflict exists.

Third-party evaluations

- When a conflict of interest arises between 2 parties, an independent third party, well-qualified to evaluate such matters, is brought in to the discussion.



Conflict of Interest Acknowledgment

- Employees must attest on a written contract that no potential conflicts of interest exists with employees, contract employees, committee members, or companies that currently do business with **HealthSmart Care Management Solutions**
- **HealthSmart CMS** requires that all staff sign a new conflict of interest acknowledgment annually
- Your Conflict of Interest Acknowledgment has been included with your January Quality Topic email.

Please print, sign and return your agreement to Karen Owens by **January 31st**.

Email: karen.owens@healthsmart.com Fax: 214.574.2355





Take Your Completion Survey!

Please click on the link below to complete the annual HIPAA Test as your completion survey. The answers to the test questions can be found in the January Quality Topic presentations.

ALL Care Management staff is responsible for submitting their online completion survey by **January 31st**.

Completion Survey Link:

<https://www.surveymonkey.com/s/Jan2015QualityTopicSurvey>

Please contact Joslyn Crain if you have any questions.

Email: joslyn.crain@healthsmart.com | **Phone:** 214.574.2319