

WAUKESHA COUNTY DEPARTMENT OF HEALTH AND HUMAN SERVICES

2013 ANNUAL HIPAA TRAINING FOR
STAFF, CONTRACTED STAFF, INTERNS



PROPERTY OF WCDHHS

**THIS POWERPOINT SUPPLEMENTS THE
HIPAA PRIVACY AND SECURITY DVDS
THAT YOU WATCHED TO HELP YOU
COMPLETE THE 2013 ANNUAL HIPAA
TRAINING**



WHY IS HIPAA PRIVACY AND SECURITY TRAINING IMPORTANT?

- It is everyone's responsibility to take the confidentiality of patient information seriously
- Anytime you come in contact with patient information or any PHI that is written, spoken or electronically stored, **YOU** become involved with some facet of the privacy and security regulations
- Training is required by law



WHY SHOULD OUR ORGANIZATION COMPLY WITH HIPAA?

- **It's the Right Thing to Do:**
 - Protect patient records
 - Protect business data
 - Reduce the risk of litigation to organization
- There are significant penalties associated with non-compliance to organizations and employees of those organizations

HIPAA TERMS AND DEFINITIONS REFRESHER



WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

PHI is defined as:

Individually Identifiable Health Information that connects the patient to the information

- Health/condition of an individual
- Payment for health care of an individual
- Reasonably identifies the individual
 - Patient identifiers
 - Demographics

Patient Identifier Examples

- Names
- Address
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification numbers
- Vehicle Identifiers/Serial numbers/License plate numbers
- Internet protocol addresses
- Health plan numbers
- Full face photographic images and any comparable images
- Web universal resource locaters (URLs)
- Any dates related to any individual
 - Date of birth
 - Admit/Discharge dates
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code

USE/DISCLOSE

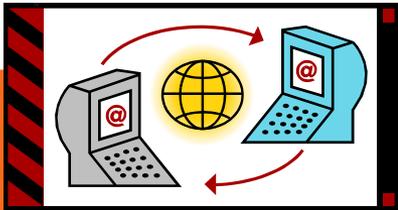
- **Use:** When we review or use PHI internally
 - Audits
 - Training
 - Customer service
 - Quality improvement
- **Disclose:** When we release or provide PHI to someone
 - Patients
 - Attorneys
 - Faxing records to another provider, etc.



MINIMUM NECESSARY RULE

- To use/disclose/release only the minimum necessary to accomplish the intended purposes of the use, disclosure or request
- Requests from employees at WCDHHS:
 - Identify each workforce member who needs to access PHI
 - Limit the PHI provided on a “need-to-know” basis
- Requests from individuals not employed at WCDHHS:
 - Limit the PHI provided to what is needed to accomplish the purpose for which the request was made

HIPAA Regulations Require That we Protect our Patients' PHI in all Media



PROTECT PHI IN ALL MEDIA TYPES

- **Verbal discussions**
 - In person
 - On the phone
- **Written on paper**
 - Chart
 - Progress note
 - Encounter form
 - Prescription
 - Lab order
 - Referral form
 - Explanation of benefits (EOB)
 - Scratch paper-including Post-It Notes
- **Computer Applications/Systems**
 - Avatar
 - PeopleLink
 - eWiSACWIS
 - Microsoft Outlook
 - Microsoft Office Products
- **Computer hardware/equipment**
 - PC's
 - Laptops
 - PDA's
 - Pagers
 - Fax machines/Printers/Copiers
 - Cell/Multifunctional phones
 - Patient care devices
 - Servers

NOTICE OF PRIVACY PRACTICES

- **What is the purpose of the Notice?**
 - Summarizes how WCDHHS uses and discloses a patient's PHI
 - Details patient's rights in respect to their PHI

NOTICE OF PRIVACY PRACTICES (NPP)

- **Client/Patient review and signature is required when:**
 - The client/patient begins treatment at WCDHHS
 - The client/patient transfers to a different program within WCDHHS
 - When the minor client/patient turns 18
 - When the information in the NPP changes
 - Client/patient signs the Acknowledgment of Receipt to confirm that they have been offered and/or received the Notice of their rights
 - A client/patient can refuse to sign and in that case, document that information

PATIENT RIGHTS UNDER HIPAA

- HIPAA focuses on the rights of the patient and confidentiality of their information
- Under HIPAA, patients have the right to several key issues:
 - Right to *Request Amendment* of their medical record
 - Right to *Request to Inspect and Copy* their record
 - Right to *Restrict* what information and to whom it can be released
 - Right to *Receive Confidential Communication*
 - Right to an *Accounting of Disclosures*
 - Right to receive a *Notice of Privacy Practices*
 - Right to *Complain* about a disclosure of their PHI

HIPAA SECURITY RULE



HIPAA SECURITY RULE

- **Security means controlling:**
 - The **confidentiality, integrity and availability** of electronic protected health information (ePHI) in the following ways:
 - Created
 - Received
 - Maintained
 - Transmitted
 - Used
 - Stored
 - Accessed
- **Having safeguards in place:**
 - Administrative
 - Technical
 - Physical

ADMINISTRATIVE SAFEGUARDS

- Organizational policies and procedures are **REQUIRED**
 - Define what needs to be done to maintain security

Examples include:

- Use of the internet
- Use of email
- Proper use personal smartphones/mobile devices
- How to fax properly
- Proper use of identifying clients
- Workforce security and security incident procedure
- Security awareness and training

ADMINISTRATIVE SAFEGUARDS

Email

- Do not send PHI via email unless it is encrypted by Zixmail
- Do not put client information in the subject line
 - This applies to all emails being sent outside of our system
- They are caught in the Zixmail filter
- Forwarded to your supervisor/department manager
 - Do not forward “joke emails” since they usually contain viruses and take up a lot of space on our servers
 - Do not use profanities in your emails
 - They are caught in the Zixmail filter
 - Forwarded to your supervisor and department manager

ADMINISTRATIVE SAFEGUARDS

Faxing

Fax with caution!

- Confirm fax number when on phone with requestor
- Obtain their phone number in case question(s) arises
- Dial number carefully
- Verify the number on fax display is correct before sending fax
- Frequently monitor fax machine to remove faxes containing sensitive information
- USE a **FAX COVERSHEET** on all faxes, especially those with PHI
 - They give instructions to the receiver in case a problem occurs or if they receive the documents in error

ADMINISTRATIVE SAFEGUARDS

Proper use of Personal Smartphones/Mobile Devices

- Work-related use should be kept to a minimum
- The following precautions MUST be followed:
 - Only use Waukesha County's account for work-related email/calendar/tasks/contacts on phone
 - Do not use the mobile device's calendar/personal email for work-related activity
 - Only use minimal information regarding clients (ex: initials)
 - Do not include client's full name, DOB, PL# or any other identifying information
 - Taking photos of clients is highly discouraged
 - If using your personal mobile device for work, you must secure your mobile device with a lock screen feature
 - Pin
 - Password
 - Swipe

TECHNICAL SAFEGUARDS

- Many technical devices are needed to maintain security.

Examples include:

- Different levels of computer passwords
 - Screen savers
 - Devices to scan ID badges
 - Data backups
 - Safe disposal of media
 - Encryption
 - Audit trails
-
- Computer and system processes are set up to protect, control and monitor information access

USERNAMES/PASSWORDS

- Used to control access to electronic protected health information (ePHI) in our computer systems/applications
 - Require all users to utilize individually unique Usernames and Passwords
 - Usernames/Passwords control what users are able to access and help us identify what information users accessed in our applications
- You may not share your username and password with anyone else, including your supervisor!
- When leaving your computer, no matter for how short of time, **ALWAYS:**
 - Lock the computer screen (Ctrl-Alt-Del and select lock) **OR**
 - Click on the lock icon on the bottom of your screen **OR**
 - Log off

This prevents other users from using the applications in your name!

PHYSICAL SAFEGUARDS

- Many physical barriers devices are needed to maintain security

Examples include:

- Installing locks on doors
- Securing buildings and rooms
- Identifying visitors
- Locking file cabinets to protect the organization's property and client information



PHYSICAL SAFEGUARDS

To protect our facilities:

- Always wear your ID badge
- Only let employees enter with you, direct others to use the main entrance
- Patients, vendors, former employees, etc need to sign-in
- If you see someone without an ID badge,
 - Ask “May I help you?” or “Who are you here to see”
 - Escort the individual to proper location

Keep PHI out of view of public

- Close records when not in use
- Flip records over to hide client information
- Cover clipboards
- Never leave paper with PHI unattended
- Retrieve faxes promptly
- Lock office doors and file cabinets

PHYSICAL SAFEGUARDS

Clean Desk Policy

- HSC-All client files or PHI must be kept in a file drawer or cabinet when leaving for the day
- IP Hospital-All patient files are to be kept at nurse's station or in medical records once patient is discharged
- Clinic Area-All client files must be returned at the end of the work day to the Records Area
- Public Health-At the end of the day files should be in the designated file cabinets, or placed in desk drawer
- If files are left out, then they need to be turned over to conceal the client's name from others

HIPAA BREACHES



DEFINITION OF A BREACH

The unauthorized acquisition, access, use or disclosure of unsecured PHI under the Privacy Rule which compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

DEFINITION OF A BREACH-3 EXCEPTIONS

- Unintentional acquisition, access, or use of protected health information (PHI) by a workforce member acting under the authority of a covered entity or business associate
- Inadvertent disclosure of protected health information (PHI) within covered entity
 - In both above cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule
- Unauthorized recipient reasonably could not retain information

EXAMPLES OF BREACHES

- Disclosing data to someone who did not have the right to receive it
- Releasing information to a requestor without a valid authorization in the client's chart
- Accessing information that you do not have a "need to know" for your job because of personal curiosity or as a favor to someone else
- Discussing PHI or confidential information in a public area
- Sending a fax to the wrong number
- Sending information to the wrong address
- Sending an email to the wrong person

EXAMPLES OF BREACHES

- Loss of a paper or electronic file containing confidential information
- Losing a laptop that is not encrypted
- Improper use of passwords-sharing, posting or distributing personal password or account access
- Allowing a co-worker to log-on with your password because it provides access to more or different security levels your co-worker doesn't have
- Attempting to learn or use another person's access information
- Selling health or personal information or inappropriately providing it to the news media

HITECH BREACH NOTIFICATION

- All suspected and actual incidents MUST BE reported to Michelle Magedanz, Privacy & Security Coordinator, IMMEDIATELY!
- An investigation will be conducted with the involved individuals
- Affected clients have to be notified without reasonable delay but no later than 60 days of discovery

HITECH BREACH NOTIFICATION

For breaches involving less than 500 individuals, the organization must log the breaches and report them annually to the OCR (Office of Civil Rights)

For breaches involving more than 500 individuals, the organization must report this to the OCR at the same time they notify the individual

- Media outlets must also be notified
- HHS will also post this information on their public website

PENALTIES FOR PATIENT CONFIDENTIALITY BREACHES



PENALTIES FOR PATIENT CONFIDENTIALITY BREACHES

- **State penalties**
- **Federal penalties**
 - Civil penalties
 - Criminal penalties
- **Both State and Federal penalties include:**
 - Monetary penalties
 - Imprisonment
 - Termination of employment at Waukesha County

PENALTIES FOR BREACH OF PATIENT CONFIDENTIALITY - WI

WI Stat 51.30

- Knowing and willful disclosure
 - Up to \$25, 000 plus actual damages and attorney fees
- Negligent disclosure
 - \$1,000 plus actual damages and attorney fees per violation
- Requests/obtains information under false pretenses
 - \$25,000 or imprisonment for up to 9 months or both
- Discloses information knowing that the disclosure is unlawful and not necessary to protect another from harm
 - \$25,000 or imprisonment for up to 9 months or both
- Falsification, obstruction, investigation, intentional destruction or damages records
 - \$25,000 or imprisonment for up to 9 months or both
- Intentional disclosure, knowing the information is confidential and discloses for monetary gain
 - \$100,000 or imprisoned 3.5 years or both
- Employee may be suspended or discharged without pay

PENALTIES FOR BREACH OF PATIENT CONFIDENTIALITY - HIPAA SANCTIONS

Civil Penalties:

Violation	Penalty	Maximum Penalty
Individual did not know they violated HIPAA	\$100 per violation, with an annual max. of \$25,000 for repeat violations	\$50,000 per violation, with an annual max. of \$1.5 million
Due to reasonable cause/not willful neglect	\$1,000 per violation, with an annual max. of \$100,000 for repeat violations	\$50,000 per violation, with an annual max. of \$1.5 million

PENALTIES FOR BREACH OF PATIENT CONFIDENTIALITY - HIPAA SANCTIONS

Civil Penalties Continued:

Violation	Penalty	Maximum Penalty
Due to willful neglect but violation is corrected within required time period	\$10,000 per violation, with an annual max. of \$250,000 for repeat violations	\$50,000 per violation, with an annual max. of \$1.5 million
Due to willful neglect but not corrected	\$50,000 per violation, with an annual max. of \$1.5 million	\$50,000 per violation, with an annual max. of \$1.5 million

PENALTIES FOR BREACH OF PATIENT CONFIDENTIALITY - HIPAA SANCTIONS

Criminal Penalties – Improperly obtaining or disclosure of PHI or improperly use unique health identifiers are subject to the following penalties:

Penalty	Fine	Prison time
Knowingly	\$50,000	Up to 1 year
Under false pretenses	\$100,000	Not more than 5 yrs
For profit, gain or harm	\$250,000	Not more than 10 yrs

HIPAA VIOLATIONS

- There are three types of violations:
 - Incidental
 - Accidental
 - Intentional
- The goal is to prevent all three from happening

INCIDENTAL VIOLATIONS

Incidental disclosures are going to happen...even in the best of circumstances and we **DO** want to take measures to prevent these from happening

Examples:

- A file was left away from public view but part of the name label was able to still be read
- You selected the wrong patient name in any computer system and had to go back to select the right name – an honest error
- You have left your office unlocked and another employee walked in your office and saw a name on one of your file folders

ACCIDENTAL VIOLATIONS



OOPS!

Mistakes happen. If you mistakenly disclose PHI or provide confidential information to an unauthorized person or if you breach the security of confidential data:

- Acknowledge the mistake and notify your supervisor and the Privacy & Security Coordinator **immediately**
- Learn from the error and review the policy
- Assist in correcting the error only if you are instructed
- ***Do not cover up the situation or try to make “right” by yourself***
 - Procedures may need to be revised to prevent this from happening again
 - Accidental disclosures are Privacy Incidents and must be reported to the Privacy & Security Coordinator immediately!
 - This is an accountable disclosure that needs to be reported to the OCR

INTENTIONAL VIOLATIONS

- If you ignore the rules and carelessly or deliberately use or disclose protected health or confidential information, you can expect:
 - Disciplinary action
 - Civil and/or criminal charges
- **Examples include:**
 - Accessing PHI for purposes other than assigned job responsibilities
 - Looking up a person that you read about in the newspapers or another employee's records just because you were interested
 - Attempting to learn or use another person's access information
 - Deliberately using/disclosing client information in which you know should not be released

If you're not sure about a use or disclosure, check with your supervisor or the Privacy & Security Coordinator

**THE FOLLOWING SLIDES
PROVIDE EXAMPLES OF PRIVACY &
SECURITY VIOLATIONS TO HELP YOU
BETTER UNDERSTAND HOW THEY
OCCUR SO THAT YOU MAY HELP
PREVENT THEM**



ACCESS VIOLATION – ACCESS TO INFORMATION

Scenario:

A co-worker calls one of the social workers to see the paper file on their brother's child who they know has been the subject of child neglect

The social worker allows the co-worker to view the paper file in their office during an “impromptu meeting”

- Is this against WCDHHS policies?

ACCESS VIOLATION?

YES.

Both workers violated WCDHHS policy.

It is WCDHHS policy that you may not have access to paper files that you have no authority in your position to be looking at.

A fellow employee who has proper access to the paper files should not let a co-worker view the file even though the co-worker is related to the client.

COMPUTER VIOLATION

Scenario:

When leaving to go to lunch, an employee didn't log off of his computer

Another employee then utilized his computer to look up a PeopleLink number to do her job

Is this against WCDHHS policies?



COMPUTER VIOLATION?



YES.

Both employees did not follow our policies which require:

- Logging off/password protecting the screen, securing all applications when unattended
- Not using another person's login

Don't let this happen to you!

SECURITY VIOLATION



- An employee uses a personal flash drive on his computer to take work home for the weekend.
- Is this against WCDHHS policies?

SECURITY VIOLATION?



- **YES** – We may not use personal flash drives on Waukesha County computers
- We need to use Waukesha County issued flash drives
- The flash drive needs to be encrypted
- Viruses can be introduced to the Waukesha County network that may be on a personal flash drive

HOW AND WHOM DO YOU REPORT A POTENTIAL VIOLATION OR CONCERN?

- It is your duty to report any concerns you have about privacy and security **IMMEDIATELY!**
- Tell your supervisor right away and contact the WCDHHS Privacy and Security Coordinator–Michelle Magedanz @ ext. 7679 or via email: mmagedanz@waukeshacounty.gov
- The County Security Officer is Allen Mundt, amundt@waukeshacounty.gov
- The County Privacy Officer is Tom Farley, tfarley@waukeshacounty.gov

2013 HIPAA BREACHES



HOSPICE OF NORTH IDAHO

January 2013

HHS announces first HIPAA breach settlement involving less than 500 patients

Hospice of North Idaho settles HIPAA security case for \$50,000

- The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services' (HHS) \$50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.
- The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of their field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule.

INTERNAL REVENUE SERVICE

- March 2013
- The IRS is facing a lawsuit over HIPAA violations considered to be a data breach of ten million records with unauthorized seizure. The class action lawsuit does not name the individual company and called it “the John Doe Company” who filed the case. The IRS is being accused of not being helpful regarding supplying information and the lawsuit is looking for \$25,000 per individual compensation.
- The covered entity, called John Doe Company, states that the IRS agents stole more than 60,000,000 medical records of more than 10,000,000 Americans, including at least 1,000,000 Californians.
- The agents for the IRS allegedly conducted the unlawful search and seizure in 2011 in Southern California.

ERICKSON LIVING'S RIDERWOOD PHYSICAL THERAPY

April 2013:

- Erickson Living's Riderwood physical therapy of Silver Spring, MD reported this week that there were five laptops stolen back in November from Riderwood's physical therapy offices.
- Though the number of affected patients is unknown, a key element of the breach was that not all files on the laptops were encrypted.
- The information included Erickson health plan member names, addresses, policy numbers, dates of birth and certain insurance information were potentially compromised as a result of the breach.

UNIVERSITY OF ROCHESTER MEDICAL CENTER (URMC)

May 2013:

PHIPrivacy.net reports that the University of Rochester Medical Center (URMC) informed 537 former orthopedic patients that their (PHI) had been compromised in a recent data breach.

It was a familiar storyline, as a resident physician lost an unencrypted USB computer flash drive that was used to evaluate surgical results at a URMC outpatient orthopedic facility. The flash drive belonged to the resident and the copied PHI included patient names, gender, age, date of birth, weight, telephone number, medical record number (a number internal to URMC), orthopedic physician's name, date of service, diagnosis, diagnostic study, procedure and any complications. There were no Social Security numbers on the drive, however, which is a good thing for patients who may have identity theft concerns.

HIM DEPARTMENT LOSES PAPER RECORDS

- May 2013
- Jackson Health System in Miami has notified 1,407 patients that their paper medical records have been lost.
- The records, missing since January from the health information management department, were in transit to be electronically scanned or were being returned when they disappeared, according to a Jackson Health notice.
- The public health system said there was no breach of Social Security numbers or financial information, but affected patients are being offered paid credit and identity protection services. “We hold ourselves accountable anytime a patient’s information is illegally or inappropriately accessed, which is why we are offering this free credit and identity protection as a precaution,” a spokesperson tells *Health Data Management*.

IN CLOSING...

Protecting PHI
is everyone's
JOB;

PHI is NOT
everyone's
business.



TO RECEIVE CREDIT FOR THIS TRAINING, COMPLETE THE FOLLOWING REQUIREMENTS

- The Online HIPAA assessment (Test automatically goes to Michelle for grading)
- The Confidentiality/Non-Disclosure Statement is now part of the online HIPAA assessment-no documents to turn in!
- Any questions, please contact Michelle Magedanz, Centralized Records Supervisor/DHHS Privacy & Security Coordinator at ext. 7679 or via email at mmagedanz@waukeshacounty.gov