

HIPAA Compliance

May 2, 2019

Dannae Delano
Partner - The Wagner Law Group
ddelano@wagnerlawgroup.com
(314) 236-0065

THE WAGNER LAW GROUP
A PROFESSIONAL CORPORATION

Course Overview

▶ During this course you will learn:

- ▶ Background
- ▶ Health Insurance Portability and Accountability ("HIPAA") Privacy Rule
- ▶ Individual Rights
- ▶ HIPAA Security Rule
- ▶ Protecting Privacy & Security: Best Practices
- ▶ Business Associates
- ▶ Security Breach Notification
- ▶ Complaints

Part 1: Background

What is HIPAA?

- ▶ HIPAA is a federal law designed to protect a subset of Sensitive Information known as Protected Health Information ("PHI") and Electronic Protected Health Information ("EPHI")
- ▶ In 2009, HIPAA was expanded and strengthened by the HITECH Act
- ▶ In January 2013, HHS issued a Final Rule implementing HITECH's statutory amendments to HIPAA
- ▶ This training focuses on two primary HIPAA rules, as amended by HITECH:
 - ▶ HIPAA Privacy Rule
 - ▶ HIPAA Security Rule

What Does HIPAA Do?

- ▶ Establishes standards to protect the privacy of individually identifiable health information (aka PHI)
- ▶ Provides rights and protections for employees and their dependents
- ▶ Defines the authorized and required uses and disclosures of PHI
- ▶ Creates Administrative and Security Requirements for Employers

*Biggest challenge is changing attitudes and behavior regarding the importance of safeguarding the confidentiality of PHI

Who Must Comply With HIPAA?

- ▶ Health plans
- ▶ Health care clearinghouses
- ▶ Health care providers
- ▶ Business Associates of health plans, clearinghouses and providers

HIPAA Privacy Rule: The Basic Idea

▶ Information contained in an individual's health record must be:

- ▶ Handled securely
- ▶ Not accessed
- ▶ Not shared
- ▶ UNLESS it is for...

HEALTH CARE
OPERATIONS:

- Auditing
- Monitoring
- Quality Assurance



Privacy: Standards for Protected Health Information

- ▶ Applies to health information in all forms:



Spoken



Written



Electronic

What is “PHI” and “EPI”?

- ▶ Any individually identifiable health information (oral, written, or electronic) that relates to the health care of an individual

- ▶ To be PHI or EPHI, the information must come from the plan or from a provider
- ▶ The regulations identify 18 factors that are individually identifiable
- ▶ Any one of these factors is enough to make information PHI

What is “PHI” and “EPI”?

Identifiers:

- ▶ Name
- ▶ Telephone number
- ▶ Medical record number
- ▶ Address
- ▶ Age
- ▶ Dates (*i.e.*, birthdate)
- ▶ Fax number
- ▶ E-mail address
- ▶ Social Security Number
- ▶ Device Identifiers
- ▶ Beneficiary number
- ▶ Web addresses
- ▶ Vehicle identifier number
- ▶ Certificate/license number (*i.e.*, driver’s license)
- ▶ Finger print or voice print
- ▶ Genetic Information
- ▶ Medical record number
- ▶ Account number
- ▶ Photographs

What is NOT “PHI” and “E PHI”?

To be PHI, information must come from a plan or provider

- ▶ Information from an individual to the employer IS NOT PHI
 - ▶ Employee to supervisor - generally not PHI
- ▶ Information from an individual to “plan employee” IS PHI
 - ▶ A “plan employee”:
 - ▶ Works directly for a health plan and the information is given while working for the health plan OR
 - ▶ May qualify as an “Authorized” or “Responsible” Employee
 - ▶ Employee to Authorized Employee - PHI
- ▶ Summary health information IS NOT PHI
 - ▶ Summarizes claims history, claims expenses, or types of claims
 - ▶ Contains no identifying information other than zip codes

What is NOT “PHI” and “E PHI”?

- ▶ Health information collected pursuant to other laws, such as FMLA, ADA, OSHA, or Worker’s Compensation, is not PHI
- ▶ *NOTE:* This information may be protected under other federal and state laws
 - ▶ Authorized drug and alcohol testing, fitness for work assessments, etc., that are a condition of employment
 - ▶ Provider information received pursuant to authorization for FMLA
 - ▶ Provider information received pursuant to authorization for disability
 - ▶ Provider information or Plan information received pursuant to authorization for ADA
 - ▶ Provider information required by OSHA
 - ▶ Worker’s Comp - employer, carrier, and administrator can receive PHI if authorized by employee or as required by law

What is NOT “PHI” and “E PHI”?

- ▶ HIPAA does not apply to administration of:
 - ▶ Dependent Care Flexible Spending Account (DCFSA)
 - ▶ Life Insurance and AD&D
 - ▶ Long and Short-Term Disability
 - ▶ Workers’ Compensation
 - ▶ Family and Medical Leave Act
 - ▶ 401(k)
 - ▶ Profit Sharing
 - ▶ Drug Testing
 - ▶ Resource and Referral Program

REALITY CHECK

- ▶ A court ordered Walgreens to pay \$1.44 million to a customer whose PHI was impermissibly accessed and disclosed by a pharmacy employee. The employee suspected her husband's ex-girlfriend gave him an STD, looked up the ex-girlfriend's medical records to confirm her suspicion, and shared the information with her husband. He then texted his ex-girlfriend and informed her that he knew about her STD.

How Does This Affect YOU?

Do you have self-funded group health plans or are you a medical care provider?

- ▶ **medical**
- ▶ **Dental**
- ▶ **Health FSA**

***Any PHI related to these plans is covered by HIPAA

How Does This Affect YOU?

- ▶ HIPAA does NOT apply to employers
 - ▶ A health plan is a separate entity from the employer with a separate workforce
 - ▶ You wear two hats: employer and plan
 - ▶ ***Importance of specifying limitations on Dissemination of PHI
 - ▶ Information in Plan files are covered by HIPAA
 - ▶ Information in Personnel files and HRIS system are not PHI and not covered by HIPAA

How Does This Affect My job?

- ▶ Two types of employees:
 - ▶ Authorized Employees - Have access to PHI or EPHI directly during the normal course of the plan administration
 - ▶ Responsible Employees - May have access to PHI or EPHI by virtue of their job duties but are not involved in plan administration
 - ▶ Accounting
 - ▶ Finance
 - ▶ Payroll
 - ▶ Information Technology

How Does This Affect My job?

- ▶ What is the process if an employee wants help and PHI is involved?
 - ▶ Refer employee to applicable business associate or insurer
 - ▶ If employee still needs help, refer to an Authorized Employee who handles Plan administration

Why Does This Affect My Job?

Enforcement:

- ▶ The Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") will enforce HIPAA
 - ▶ Accepts and investigates complaints
 - ▶ Conducts compliance reviews
- ▶ State Attorney Generals
 - ▶ Pursuant to HITECH, state attorney generals are also permitted to bring civil actions and recover monetary awards that may be shared with harmed individuals.
- ▶ Individual Litigation

Penalties

- ▶ HIPAA Penalties
 - ▶ Civil Penalties
 - ▶ Up to \$100-\$50,000 per violation, not to exceed \$1.5 million per calendar year
 - ▶ Criminal Penalties
 - ▶ If you knowingly obtain or disclose individually identifiable health information in violation of the privacy rules
 - ▶ Up to \$250,000 and/or up to ten years in jail
- ▶ Company Corrective and Disciplinary Actions
 - ▶ Up to and including loss of privileges and termination of employment

Use or Disclosure of PHI

- ▶ In order to use or disclose PHI:
 - ▶ The health plans must give each individual a Notice of Privacy Practices (NPP) that:
 - ▶ Describes how the plans may use & disclose the person's PHI
 - ▶ Advises the person of his/her privacy rights
 - ▶ Describes the Plan's and Employer's duties
 - ▶ Provides description of the Plan's Complaint procedures
 - ▶ Must get acknowledgement of receipt from individual
 - ▶ NPP allows PHI to be used and disclosed for purposes of Treatment(T), Payment(P), Operations(O) ("TPO")

Treatment, Payment, or Health Care Operations

- ▶ Treatment: Provision, coordination, or management of health care
- ▶ Payment: Eligibility and coverage determinations, risk adjusting, billing, claims management, collection activities, obtaining payment under a reinsurance contract, review for medical necessity, coverage, utilization review, limited disclosures to consumer reporting agencies relating to collection of premiums or reimbursement, subrogation services
- ▶ Operations: Coordination of benefits, legal services, appeals, auditing, business planning, management, and general administration

Part 2: Privacy

When Can You Access & Use PHI?

- ▶ Plan administrative functions
 - Quality assurance - Monitoring
 - Claims processing - Insurance underwriting
 - Auditing
- ▶ Information can only go to Authorized Employees for administrative functions - no one else
 - ▶ Pursuant to a valid authorization of the covered individual or his designated representative
 - ▶ PHI cannot be used for any employment-related purpose without the individual's authorization

Privacy - When Can You Access and Use PHI?

- ▶ Disclose directly to the Individual
- ▶ Disclose to Spouses, other Family Members, and Friends
 - ▶ Can disclose PHI to family members and close personal friends if:
 - ▶ The individual agrees to such disclosure either orally or in writing
 - ▶ You reasonably infer from the circumstances (for example, an emergency or incapacity) that the individual does not object AND it would be in the best interest of the individual to disclose such PHI

Privacy - When Can You Access and Use PHI?

- ▶ Disclosure to personal representatives
 - ▶ You can disclose PHI to a personal representative if the plan receives:
 - ▶ A notarized power of attorney for health care purposes
 - ▶ A court order appointing the person as conservator or guardian
- ▶ Disclosure to parent of minor child (18 years old)
 - ▶ State law governs
- ▶ Public Policy
 - ▶ Required by law
 - ▶ Government-sponsored health oversight activities
 - ▶ Subpoena
 - ▶ Public health activities

Privacy - When Can You Access and Use PHI?

- ▶ Minimum necessary disclosure
 - ▶ Cannot use, disclose, or request more than the minimum amount of PHI necessary to accomplish the intended purpose, taking into account practical and technological limitations
- ▶ The minimum necessary standard does not apply to:
 - ▶ Uses or disclosures to the individual or representative
 - ▶ Disclosures to or requests by a health care provider for treatment
 - ▶ Uses or disclosures made pursuant to a valid authorization
 - ▶ Disclosures made to the HHS
 - ▶ Uses or disclosures required by law
 - ▶ Uses or disclosures required to comply with HIPAA
- ▶ All disclosures other than the minimum necessary should be reviewed with the Privacy Officer

Except for Treatment - Minimum Necessary Standard Applies

- ▶ For individual care and treatment, HIPAA does not impose restrictions on use and disclosure of PHI by health care providers
 - ▶ Exceptions: psychotherapy information, HIV test results, and substance abuse information
- ▶ For anything else, HIPAA requires users to access the minimum amount of information necessary to perform their duties
 - ▶ Example: In order to determine whether a submitted claim is an "allowable expense," an Authorized Employee only needs to know what the medical condition is—nothing more. (expense for foot inserts—only need to know foot related condition)

Confidentiality of Individual Information

- ▶ All personnel are obligated to protect confidential information about individuals
- ▶ Job-related purpose or HIPAA-compliant individual authorization is required for access, use, or disclosure
- ▶ Direct government requests to HR
- ▶ In the event of a search warrant, do not obstruct search, notify your supervisor

Time Out For Practice

- ▶ Julia receives a phone call from a health care provider regarding treatment that her co-worker, Whitney, is obtaining. Whitney and Julia are members of the same church. Julia knows that Whitney's family could use some help with meals, transportation, and babysitting. Julia knows that members of the church would be happy to help, but the problem is that nobody from the church knows that Whitney is sick. Julia can get Whitney's family the help it needs by making a quick call to the church.
- ▶ To remain in compliance with HIPAA, Julia should:

<input type="checkbox"/>	Call her pastor, explain the situation, and arrange to have healthy meals taken to Whitney's home for the next five days
<input type="checkbox"/>	Do nothing unless Whitney gives her the authorization to call the church and get help for her family

Time Out For Practice

- ▶ Julia receives a phone call from a health care provider regarding treatment that her co-worker, Whitney, is obtaining. Whitney and Julia are members of the same church. Julia knows that Whitney's family could use some help with meals, transportation, and babysitting. Julia knows that members of the church would be happy to help, but the problem is that nobody from the church knows that Whitney is sick. Julia can get Whitney's family the help it needs by making a quick call to the church.
- ▶ To remain in compliance with HIPAA, Julia should:

	Call her pastor, explain the situation, and arrange to have healthy meals taken to Whitney's home for the next five days
	Do nothing unless Whitney gives her the authorization to call the church and get help for her family

Remember - It's Common Sense

- ▶ Use information *only when necessary* to perform your job duties
 - ▶ Only information you **NEED TO KNOW** for your job
- ▶ Use only the *minimum necessary* to perform your job duties
- ▶ Follow the employer's policies and procedures for information confidentiality and security

Unauthorized Access

- ▶ It is NEVER acceptable to look at PHI “out of curiosity,” even if no harm is intended (*i.e.*, retrieving an address to send a “get well” card).
- ▶ It also makes no difference whether the information relates to a “high profile” person, a close friend or a family member - ALL information is entitled to the same protection and MUST be kept private
- ▶ These rules apply to all employees

Part 3: Individual Rights

- ▶ Individual may make a request to restrict disclosure
 - ▶ Each individual has the right to request that the Plan not use or disclose his or her PHI for any reason
 - ▶ The Privacy Officer will decide whether to grant any such request
 - ▶ If the request is granted, the Plan will not use the PHI except in an emergency, for treatment, payment or operations, or for public policy reasons
- ▶ Each individual has the right to inspect and obtain a copy of his or her PHI
 - ▶ The individual must complete a form prescribed by the Privacy Officer
 - ▶ The requested information will be provided within 30 days (regardless of whether the information is maintained off-site). It may be able to obtain an additional 30 days if unable to respond.
 - ▶ If the request is denied, the individual will be given a written denial and the right to appeal

Part 3: Individual Rights

- ▶ Right to amend PHI
 - ▶ Each individual has the right to correct his or her PHI
 - ▶ Each request should be directed in writing to the Privacy Officer
- ▶ Right to receive communication by alternate means or at alternate locations
- ▶ No retaliation for exercising rights under HIPAA
- ▶ Right to request an accounting
 - ▶ An individual may request an accounting of all disclosures during the past six years except:
 - ▶ Disclosures to carry out treatment, payment, and health care operations
 - ▶ Disclosures to the individual about himself or herself pursuant to a valid authorization
 - ▶ Disclosures for public policy reasons

Part 3: Individual Rights
Accounting for PHI Disclosures

- ▶ Authorized Employees are responsible for maintaining a record of all disclosures other than disclosures for:
 - ▶ Treatment, payment, or health care operations
 - ▶ Pursuant to a valid authorization
 - ▶ To the individual
 - ▶ Otherwise permitted under regulations
- ▶ The Privacy Officer should compile and maintain a master list of disclosures
 - ▶ Disclosures should be maintained for 6 years

Part 3: Individual Rights
HIPAA Privacy & Security Manual & Procedures

- ▶ Communication Procedures
- ▶ Individual Rights and Requests
 - ▶ Forms for Requests and Denial
- ▶ Tracking Disclosures
- ▶ Standard Confidentiality Agreements
- ▶ Breach Notification Rules
- ▶ Notice of Privacy Practices
- ▶ Privacy and Security Officer Roles and Job Descriptions

Part 4:
HIPAA Security Rule

- ▶ Security Rule concentrates on safeguarding PHI by focusing on the confidentiality, integrity, and availability of PHI.
 - ▶ Confidentiality means that data or information is not made available or disclosed to unauthorized persons or processes.
 - ▶ Integrity means that data or information has not been altered or destroyed in an unauthorized manner.
 - ▶ Availability means that data or information is accessible and useable upon demand only by an authorized person.

Security Standards/Safeguards

- ▶ **Safeguards must:**
 - ▶ Protect PHI from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites such as Facebook, Twitter and others) and work areas;
 - ▶ Limit accidental disclosures (such as discussions in lobby and hallways); and
 - ▶ Include practices such as encryption, document shredding, locking doors and file storage areas, and use of passwords and codes for access.

Security - How to Protect PHI

- ▶ **Malicious Software = viruses, worms, spyware & spam (a/k/a “malware”)**
 - ▶ Employees should utilize anti-virus and anti-spyware software & update it regularly
 - ▶ Safe Internet browsing habits can reduce likelihood of an infection;
 - ▶ do not open email or click on embedded links from an unknown or untrusted site.
 - ▶ If the computer or mobile device you are using stores work-related sensitive information, personal use of the web is not recommended.

Part 5: Protecting Privacy & Security Best Practices

- ▶ This section explains:
 - ▶ Verbal exchanges
 - ▶ Knowing where you left your paperwork
 - ▶ Taking PHI off-site
 - ▶ Disposal of paper documents
 - ▶ Training and hard copy storage
 - ▶ E-mail Protection
 - ▶ Ways to protect electronic data
 - ▶ Password control
 - ▶ Safe computing, Facsimile, Mobile Devices, and Social Media
 - ▶ Privacy breach from lost, stolen, or misdirected information

Best Practices: Verbal Exchanges

- ▶ Be aware of your surroundings when talking about PHI
 - ▶ Close doors when discussing an individual's PHI
 - ▶ Move away from any conversation about a specific individual's care
- ▶ Do not leave PHI on answering machines

Ask yourself, "What if it was my information being discussed like this?"

Best Practices: Know Where You Left Your Paperwork

- ▶ Double check! When mailing or handling documents containing PHI, verify that each document belongs to the correct individual
- ▶ Check printers, faxes, copier machines when you are done using them
- ▶ Limit the number of photocopies made of PHI
- ▶ Clean Desk Practice
 - ▶ PHI must be put away when away from desk
 - ▶ PHI must be in closed and locked file cabinet when out of the office

Best Practices: Taking PHI Off-Site Involves Risk

- ▶ Risks:
 - ▶ If your car is burglarized and the thief takes off with the PHI (this happens more often than you think!)
 - ▶ Mislacing PHI in a coffee shop, restaurant, etc.
- ▶ If your job requires you to work from home or transport PHI between sites, follow best practices:
 - ▶ Access PHI remotely via Virtual Private Network (VPN) instead of transporting PHI
 - ▶ Securely fax or E-Mail the PHI to yourself and securely access it from the off-site location to avoid carrying PHI
 - ▶ Never leave PHI unattended in your bag, briefcase, or your car (even if it is locked in the trunk!)
- ▶ This applies to all types of PHI—paper, films, photos and EPHI stored on laptops!
- ▶ REMEMBER: you are responsible for securing the PHI and keeping it in your possession at all times

Best Practices: Disposal of Paper Documents

- ▶ Shred or destroy PHI before throwing it away
- ▶ Dispose of paper and other records with PHI in secured shredding bins - recycling and trash bins are NOT secure
- ▶ Shredding bins work best when papers are put inside the bins. When papers are left outside the bin, they are not secured from:
 - ▶ Daily gossip
 - ▶ Daily trash
 - ▶ The public

Best Practices: Training & Hard Copy Storage

- ▶ Training for all Authorized and Responsible Employees
 - ▶ Within 60 days of hire
- ▶ Hard copies of PHI kept in locked file cabinets labeled as PHI and confidential - kept separate from other personnel and benefits files

Best Practices: E-mail Protection

- ▶ All E-mail should limit PHI to Limited Data Sets or the minimum necessary to accomplish purpose
 - ▶ Limited Data Set
 - ▶ Limited data set is PHI that excludes ALL of the following direct identifiers: Names, postal street address, telephone or fax numbers, e-mail addresses, SSNs, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers (like license plate numbers), device identifiers, Web URLs, IP addresses, biometric identifiers, and photographic images

Best Practices: E-Mail Protection

- ▶ Avoid use of E-Mail when communicating with individuals (where reasonably practicable)
- ▶ If using E-Mail to communicate within the Company and E-mail will leave secured network, it must be encrypted or saved to password-protected file
 - ▶ Deliver password to recipient by other means (phone or separate email)
- ▶ Use Confidentiality Statement in E-Mail:
 - ▶ “This email and any attached files are intended solely for the use of the individual or entity to whom they are addressed, and may contain confidential information. If you have received this email in error, please notify me immediately by responding to this email. If you are not the intended addressee please do not forward, or otherwise distribute or copy this e-mail.”

Best Practices: E-Mail Protection

- ▶ **Receiving Emails**
 - ▶ **No forwarding - prepare a new message**
 - ▶ Do not save E-mail in Outlook
 - ▶ Print, file a hard copy and delete the electronic copy or save it on a disc
 - ▶ Save it to the Y: Drive
 - ▶ **Do not respond to “spam”** - simply discard or delete it, even if it has an “unsubscribe” feature.
 - ▶ **Do not open email attachments** if the message looks the least bit suspicious, even if you recognize the sender. “When in doubt, throw it out.”

Best Practices: Safe Browsing Habits

- ▶ Safeguard sensitive information
 - ▶ Look for signs of security when providing sensitive information (*i.e.*, address starts with “https” or a padlock icon is displayed in the status bar).
- ▶ Keep browser updated and use security settings
 - ▶ Update browser and application updates frequently
 - ▶ Enable browsing security settings to alert threats to your computer like popups, spyware, and malicious cookies.
- ▶ Safe downloading & streaming
 - ▶ When in doubt just don’t do it!
 - ▶ Downloaded files like software or other media can contain hidden malware.
- ▶ Use security software

Best Practices: Ways to Protect Electronic Data

- ▶ If have access to EPHI:
 - ▶ Use screen savers to block information displayed on unattended computer monitors.
 - ▶ Point computer monitors in such a way that people walking by cannot view the on-screen information.
 - ▶ Always log off when leaving a workstation.
 - ▶ If you need to discard data or information that is kept electronically, always check with your supervisor about the proper procedure.

Best Practices: Password Control

- ▶ Use strong passwords where possible (at least 8 characters, containing a combination of letters, numbers & special characters)
- ▶ Change your passwords frequently (45-90 days) to prevent hackers from using automated tools to guess your password
- ▶ It is a violation of Company Policy to share your password with anyone. Electronic audit records track information based on activity associated with user IDs

Best Practices: Safe Computing

- ▶ **Company policy requires that written approval** be granted by Privacy Officer or Security Officer **before storing PHI or EPHI on mobile devices**
- ▶ **Encryption is required** when an employee sends or receives PHI or EPHI to a destination address outside the Company network
- ▶ When **traveling, working from home, or using a mobile device**, an employee whose work involves the transmission of PHI or EPHI **must encrypt** the data **UNLESS** the employee uses a VPN connection **AND** transmits data only to a destination within the Company network

Best Practices: Facsimile

- ▶ Only fax PHI if urgent information
- ▶ All faxed PHI must contain confidentiality statement and warning about releasing data:

"This message is intended only for the use of the individual of entity to which it is addressed. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this message is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone."

OR

"The documents accompanying this transmission may contain confidential health information that is legally protected. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless permitted by law or regulation."

Best Practices: Mobile Devices

- ▶ Employees must utilize the following security controls when storing and transmitting sensitive information:
 - ▶ strong power-on passwords
 - ▶ automatic log-off
 - ▶ display screen lock at regular intervals while the device is inactive
 - ▶ **Encryption - the best defense!**
- ▶ Never leave mobile computing devices unattended in unsecured areas. Immediately report the loss or theft of any mobile computing device to your supervisor and the Information Security Office.

Best Practices: Use of Social Media

- ▶ Do not share on social media any individual information acquired from your work, even if the information is public
- ▶ Posting individual information without authorization is a violation of the individual's right to privacy and confidentiality
- ▶ Even if you think you've de-identified the information, it still might be identifiable to others
- ▶ NOTE: De-identification of PHI requires removal of all 18 PHI identifiers, which includes "any other unique identifying number, code, or characteristic."

Best Practices: Destruction vs. Storing

- ▶ Destruction of EPHI
 - ▶ Ensure EPHI stored on the system is overwritten when no longer needed
 - ▶ Only Security Officer should receive discs & CDs containing EPHI
 - ▶ CD ROM disks must be rendered unreadable by shredding, defacing the recording surface, or breaking.
 - ▶ Magnetic media such as diskettes, tapes, or hard drives must be physically destroyed or "wiped" using approved software & procedures.
- ▶ Storing EPHI
 - ▶ Must take reasonable steps to store in secure, encrypted, password-protected folders
 - ▶ Should be labeled highly sensitive if system allows labeling documents

Best Practices: Procedures

- ▶ Procedures in place for:
 - ▶ Authorizing and terminating access to computer systems and software where EPHI is maintained
 - ▶ Include reset of any third party vendor website access
 - ▶ Reuse of equipment, devices and termination of employment
 - ▶ Security Officer must remove all PHI prior to reuse
 - ▶ Maintenance to doors and windows in offices where PHI and EPHI are accessed

Best Practices: Sanctions

- ▶ Sanctions in place for violations
 - ▶ First not willful violation - immediate supervisor addresses issue unless very large exposure potential
 - ▶ Second not willful violation - supervisor initiates disciplinary process
 - ▶ First willful violation - Privacy Officer notified and disciplinary process initiated
 - ▶ Disciplinary process is up to and including termination of employment
 - ▶ Very large exposure potential = immediate report to Privacy Officer
 - ▶ All sanctions must be documented

Breach from Lost, Stolen, or Misdirected Information

- ▶ A privacy breach can occur when information is:
 - ▶ Physically lost or stolen
 - ▶ Paper copies, films, tapes, electronic devices
 - ▶ Anytime, anywhere - even while on public transportation, crossing the street, in the building, in your office
 - ▶ Misdirected to others outside the Company
 - ▶ Verbal messages sent to or left on the wrong voicemail or sent to or left for the wrong person
 - ▶ Mislabeled mail, misdirected mail
 - ▶ Wrong fax number, wrong phone number
 - ▶ Placed on internet, websites, Facebook, Twitter, etc.

Part 6: Business Associates

- ▶ BA (Business Associate) creates, receives, maintains, or transmits PHI on behalf of Covered Entity (CE)
 - ▶ Plan sponsor is not a BA, but has obligations if it performs plan administration functions that require PHI
 - ▶ Handles PHI
 - ▶ Each third-party vendor will be required to enter into a Business Associate Contract
 - ▶ Includes TPAs, utilization review managers, attorneys, auditors, software vendors

Business Associate Agreements

- ▶ Business Associate Agreements must provide:
 - ▶ BA will comply with security rule's standards and implementation specifications
 - ▶ BA will enter into BA contracts with BA subcontractors
 - ▶ BA will report breaches of unsecured PHI
 - ▶ BA subcontractors will apply same restrictions and conditions that apply to the BA with respect to PHI
 - ▶ For delegated tasks, BA will comply with privacy rules as if the BA were a CE

Business Associates

- ▶ PHI cannot be disclosed to any vendor in the absence of a Business Associate Contract
- ▶ HIPAA does not require you to police the activities of business associates
- ▶ HIPAA does require you to take action when contract violations become known
 - ▶ Report any suspected or known violations to the Privacy Officer
 - ▶ Terminate the business associate, if necessary, and report violations to the Health and Human Services Department

Part 7: Security Breach Notification

- ▶ Applies to CEs and BAs
- ▶ Requires a notification following a breach of unsecured PHI
 - ▶ Unsecured PHI can be in any form or medium
 - ▶ Must notify: Individuals, HHS, and media
- ▶ Breaches affecting 500+ individuals (large) will have notifications posted on HHS' OCR website

Security Breach Notification: What is a Breach?

- ▶ Meaning
 - ▶ Acquisition, access, use, or disclosure of PHI
 - ▶ In a manner not permitted by the privacy rule
 - ▶ Compromises the security or privacy of the PHI
- ▶ Excludes:
 - ▶ Unintentional, good faith use/disclosure by workforce member within the scope of authority without further use/disclosure
 - ▶ Inadvertent disclosure to an authorized person at same CE or BA without further use/disclosure
 - ▶ Good faith belief that unauthorized recipient not reasonably able to retain PHI

Security Breach Notification: What is a Breach?

- ▶ A breach occurs when information that, by law, must be protected is:
 - ▶ lost, stolen or improperly disposed of (*i.e.* paper or device upon which the information is recorded cannot be accounted for);
 - ▶ “hacked” into by people or mechanized programs that are not authorized to have access (*e.g.* the system in which the information is located is compromised through a “worm”), or
 - ▶ communicated or sent to others who have no official need to receive it (*e.g.* gossip about information learned from a medical record).

Security Breach Notification: Meaning

- ▶ Presumption of breach
 - ▶ CE or BA must perform four factor risk assessment
 - ▶ Breach notification is required unless the risk assessment demonstrates a low probability that the PHI has been compromised
 - ▶ Burden is on CE or BA to prove that all required notifications were given - or were not required because PHI was not compromised
 - ▶ No “*de minimis*” standard, although the type of PHI is a risk assessment factor

Security Breach Notification: Risk Assessment

- ▶ Must consider all four factors and may consider others if appropriate:
 - ▶ Nature and extent of PHI involved (including types of identifiers and likelihood of re-identification)
 - ▶ Identity of the unauthorized user or recipient (Duty to protect? Capability of re-identifying?)
 - ▶ Whether the PHI was actually acquired or viewed
 - ▶ Extent to which the risk to PHI has been mitigated

Employees Must Report Breaches

- ▶ Part of your responsibility as an employee is to report privacy and security breaches involving PHI to your supervisor AND one of the following persons:
 - ▶ HIPAA Privacy Officer
 - ▶ HIPAA Security Officer
- ▶ No one can threaten or take any retaliatory action against an individual for exercising his or her rights under HIPAA or for filing a HIPAA report or complaint, including notifying of a privacy or security breach



- ▶ Real world scenario: Affinity Health Plan, Inc. discovered and reported to HHS that it had returned leased photocopiers to the leasing agents without first erasing the data contained on the copier hard drives that included PHI. The breach was estimated to have affected over 344,000 individuals. Following an investigation, Affinity entered a settlement agreement with HHS providing for a \$1.2 million dollar payment and a corrective action plan.
 - ▶ Copiers: erase all data from hard drives
 - ▶ Faxes: confirm authorization instructions, verify telephone numbers before faxing; when possible, use pre-programmed numbers
 - ▶ Devices: encrypt, enable, and use password protection

Mitigation of Security Breaches

- ▶ Privacy Officer will investigate reported breaches
- ▶ Privacy Officer will determine if breach notice is necessary and send notices if needed
- ▶ The Privacy Officer will maintain and complete the Breach Incident
 - ▶ Disclosures should be maintained for six years

Part 8: Complaints

- ▶ Complaints should be filed by e-mailing or telephoning the Privacy Officer to submit a written complaint
- ▶ The Privacy Officer will resolve disputes and take corrective action
 - ▶ If an individual wants to know the status of a complaint, he or she should directly contact the Privacy Officer
- ▶ The Privacy Officer will maintain a log of complaints and resolutions for a period of six years

QUESTIONS?

Dannae Delano
ddelano@wagnerlawgroup.com
(314) 236-0065
(314) 397-2429 (mobile)

The Wagner Law Group
25 W. Moody Ave
St. Louis, Missouri 63119
www.wagnerlawgroup.com
