WEST
CANCER CENTER
& RESEARCH INSTITUTE

2023 Compliance & HIPAA Training

Module 1 – Compliance & HIPAA Training

West Cancer Center

West Cancer Center is committed to conducting business activities in compliance with:

- Federal, State, and Local Laws
- Applicable Regulations
- Company Policies
- Our Code of Conduct

WEST
CANCER CENTER
& RESEARCH INSTITUTE

What is Compliance Training?

Compliance training refers to the process of educating employees on pertinent:

- Laws
- Regulations
- Company Policies

Our Code of Conduct

- Compliance with applicable laws, rules, and regulations, including federal health care program requirements, as well as with West Cancer Center policies and procedures.
- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships.
- Prompt internal reporting of violations of the Code of Conduct, West Cancer Center policies and procedures, or any federal health care program requirements.
- The right of all individuals to report suspected violations to West Cancer Center without fear of retaliation.
- Full, fair, accurate, timely, and understandable disclosure in reports and documents with internal and external stakeholders, government agencies, and other public communications.
- Accountability for adherence to the Code of Conduct.

WCC Compliance Team

Chief Compliance Officer – James Cagle, CFO
Chief Medical Officer - Dr. Sylvia Richey
Compliance Advisor - Cheryl Prince, VP-Clinical Integration

WEST
CANCER CENTER
& RESEARCH INSTITUTE

COMPLIANCE HOTLINE

1-888-394-2306

Available 24 hours-a-day/7 days-a-week

Your confidentiality is ensured

Anonymity is possible

Note this number for future reference if needed

What are the benefits of a Compliance Program?

- Our Compliance program:
  - Encourages honest and ethical behavior
  - Fosters patient quality and safety
  - Promotes a culture of safety and quality for staff and providers
  - Reduces the risk of non-compliance with laws and regulations

WEST CANCER CENTER & RESEARCH INSTITUTE

What is Your Responsibility?

- To perform all duties honestly and truthfully
- Don’t be involved in any “cover-up” activities
- Always keep the patient and family members’ best interests in mind
- Report any activity that is not truthful and honest to your manager/supervisor, the Compliance Team, or the Compliance Hot Line
- Be accurate and factual in your communication

What are examples of reportable Compliance issues?

- Fraud
- False Claims
- Identify Theft
- Medical Identity Theft
- HIPAA Violations

WEST CANCER CENTER & RESEARCH INSTITUTE

Examples of Violations

- Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Breach
- Insurance Fraud/Abuse
- Identity Theft/Medical Identity Theft
- Medicare/Medicaid Regulations Breach
- Coding and Billing Irregularities
- Inappropriate Gifts or Entertainment
- Kickbacks and Bribes
- Auditing Issues
- Incorrect Provider Credentials
- Questionable Accounting

Coding and Billing

Coding and billing mishaps are one of the greatest risk areas for healthcare providers.

All entries must:

- Be complete and accurate
- Represent reasonable and necessary services

If in doubt… always ask!!!! Don't make it up!

A False Claims Violation imposes liability on any person who knowingly:

- Presents or causes to be submitted a false or fraudulent claim for payment
- Makes or uses a false record or statement material to a false or fraudulent claim or material to an obligation to pay
- Conceals or avoids or decreases an obligation to pay money to the government

Examples of False Claims Violations

- Submitting a false claim to the government to obtain payment
- Submitting a claim for medically unnecessary services
- Knowingly making false statements or providing false information to payers
- Falsifying records
- Double-billing for items or services
- Upcoding – Using a billing code, other than the intended code, to receive a greater payment
- Submitting bills for items or services never provided
- Filing a claim for payment in which the services were not rendered exactly as claimed
- Filing a claim for a physician’s service, when the service was provided by a non-physician

Tennessee Whistleblower Law:

- Imposes liability for conspiracy to violate the False Claims Act (FCA)
- Encourages and protects whistleblowers
  - *Qui tam* actions (lawsuits under the FCA)
  - Prohibits retaliation against whistleblowers

Identity Theft & Medical Identity Theft

Identity Theft: The fraudulent acquisition and use of a person's private identifying information, usually for financial gain

Example: Opening an account in another's name or using a credit card without permission

Medical Identity Theft: The illegal access and use of a patient's Protected Health Information (PHI) to obtain medical treatment, services, or goods

Example: Receiving medical care by use of another's insurance information

Medical Identity Theft Red Flags

- ID appears altered or forged
- ID photo does not match the person presenting the ID
- Presentation of a Social Security card or number that matches one that is already part of another patient's registration record
- Duplicate demographics, such as another patient has the same name or address on record
- Inconsistencies in the medical history, mismatched patient information, or procedures the physician was not aware the patient received documented in the patient's record
- Family or friends call the patient by a different name
- Individual presents medical background or information inconsistent with the existing medical record
- Individual is unaware of basic medical information within an existing medical record

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Legislative Purpose

- To allow people to keep their health insurance if they change jobs or move
- Administrative Simplification – Standardized transactions and code sets to facilitate the electronic exchange of:
  - Health Information
  - Insurance Eligibility Information
  - Claims Information
- Implementation of Electronic Billing
- Protection of Health Information
  - Access to and protection of medical records

Ask yourself… What information would you want to keep private?

- Name, Address, Phone/Fax Number
- Social Security Number
- Medical Record Number
- Diagnosis/Medical Information
- Date of Birth
- Admission and Discharge Dates
- Insurance or Payment Information
- Account Numbers
- Certificate/License Numbers
- E-Mail Address
- Biometric Identifiers – including Finger and Voice Prints
- Full Face Photographic Images and any Comparable Images

Protected Health Information (PHI)

Any individually-identifiable health information that is transmitted or maintained in any form or media including:

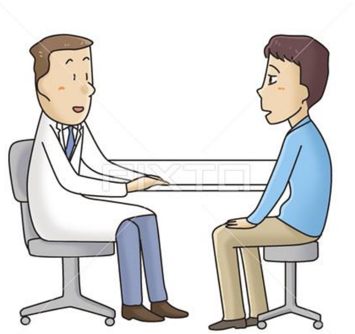
- Information, oral or recorded in any form
- Related to the physical or mental health of an individual
- Care provided to the individual
- Payment for healthcare provided to an individual

Summary: Any information about an individual's health or health plan coverage including the medical chart, billing information and other knowledge about the individual patient/client.

Protected Health Information (PHI)

There are three forms of PHI.

Printed



Verbal

Electronic

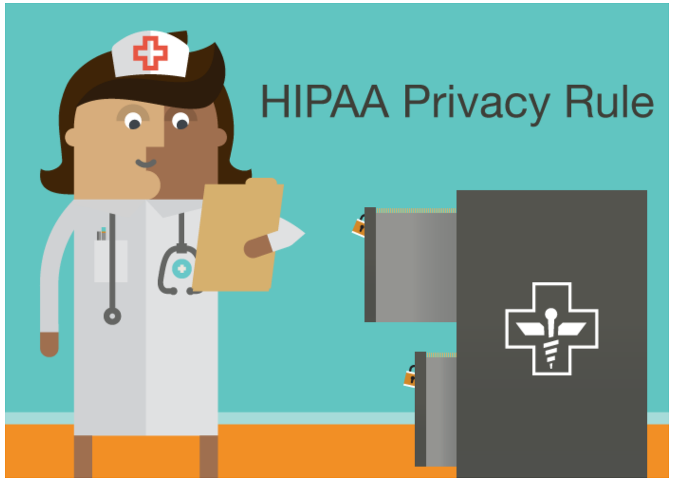
It is the responsibility of every employee to protect the privacy and security of PHI in ALL forms.

Covered Entities

- Providers – All healthcare providers that transmit health information in electronic form in connection with a covered transaction
- Health Plans – Health insurance plans, HMOs, PPOs, Medicare, Medicaid, etc.
- Clearinghouses – Individuals or entities who bill or handle health information on behalf of or for providers and health plans
- Business Associates – Contractors who provide services to help with internal operations that require use, access or disclosure of Protected Health Information (PHI)

HIPAA Privacy Rule

- Directs Covered Entities about when they “must” and when they “may” disclose PHI
- Defines patient rights
- Requires reasonable security measures
- Describes administrative responsibilities including what to do if there is a breach of privacy.



Minimum Necessary Rule

When using, disclosing or requesting PHI, only use, disclose, or request the **minimum necessary** to accomplish the task (need to know basis).

- Exception: When using accessing or disclosing PHI for treatment purposes.

Pre-Emption Rule

If other laws also protect patient privacy and don’t conflict with HIPAA:

- Follow the law that is most stringent in protecting privacy.
- Follow the law that provides the most generous patient rights.

When We **“Must”** Disclose PHI:

- To the Secretary of Department of Health and Human Services (DHHS), if asked (e.g., a HIPAA-related investigation)
- To the patient, if seeking access to own record (unless it will cause death or serious physical harm)

(For electronic records, information must be disclosed in a manner that does not constitute Information Blocking. This is discussed later.)

When We “**May**” Disclose:

- Without permission as specified*
  - Required by law
  - For public health activities
  - About victims of abuse, neglect or domestic violence
  - Health oversight activities
  - Law enforcement purposes
  - Decedents
  - Organ or tissue donation
  - Research
  - To avert threat to health or safety
  - Specialized government functions
  - Workers’ Compensation

- For treatment, payment or operations
- With written authorization
- With opportunity to verbally agree or object

Security Safeguards

Security Safeguards assure patients that we will protect their information from “bad guys” who would attempt to get their PHI for bad purposes. Covered Entities and Business Associates must have administrative, physical, and technical safeguards.

Examples of reasonable safeguards:

- Training for all staff
- Shred bins with patient information should be emptied daily
- Policies and procedures regarding use of personal devices
- Locked record rooms and locked file cabinets
- No charts on desks or left out overnight
- Passwords and encrypted email
- Screen-savers and policies regarding viruses, etc.
- Encryption of business laptops, smart phones, tablets, and other devices

Patients’ Rights

Privacy and Security Concerns:

- Vulnerability of Electronic Records
- Private information being given or sold to third parties
- Differences in state medical privacy laws

Privacy and Security Regulations Issued by Department of Health and Human Services (DHHS):

- HIPAA Privacy Regulations Effective April 17, 2003
- American Reinvestment and Recovery Act (ARRA) and Health Information Technology for Economic & Clinical Health Act (HITECH) Effective February 17, 2009
  - Interim Regulations HITECH Act – September 23, 2009
  - Final Regulations HITECH Act – September 23, 2013

Patients’ Rights (continued)

- Notice of Privacy Practices
- Requests for special privacy protection or communication of PHI
- Access to PHI
- Amendment of PHI
- Accounting of disclosures

Patients Rights & Responsibilities can be found on Page 1 of West Cancer Center’s “New Patient Handbook.” A digital version of this handbook can be found on our website - westcancercenter.org.

Patient’s Right to Access

West must respond timely to a patient’s or patient representative’s request for a copy of the patient’s records.

- Refer the patient to the appropriate **form for requesting access** to records in writing. However, the request must be honored if only verbal.
- The Practice **must provide access** except for certain limited circumstances.
- Access or a copy of records must be provided within a **specified time** period - 30 days or state law may be shorter.
- Only the **actual cost of reproducing and delivering** the record may be charged, unless to a third party or other person when the state fee cap would apply.
- For requests for electronic access to records maintained in the EMR, refer to the Information Blocking Policy included in this training

Patient Access FAQ

Q: Does a patient need to sign an Authorization to get a copy of the patient’s record?

A: No. A patient must only complete the Request for Access form or request a copy in writing.

Q: If the patient asks that the record be delivered to another healthcare provider or another person, does the patient need to sign an Authorization?

A: No. A patient may ask that you deliver the records to a third party.

Q: Can we charge the patient for the time to locate the records?

A: No. Only the actual cost of making a copy and delivery may be charged for providing the Patient with a copy. If a copy is going to a third party, additional fees may be billed.

Q: What is required if a patient’s parent, guardian or other legal representative requests the records?

A: The patient’s parent, guardian or other legal representative is treated the same as the patient. You may rely on the reasonable representation of the person’s relationship the patient. You may ask for documentation to support the relationship.

No Information Blocking Permitted

West may not block access to a patient’s electronic medical record.

- Applies to electronic records and electronic access requests
- Applies to requests by patients, patient representatives, other healthcare providers, or others permitted by HIPAA to access the records
- Patients must be provided prompt electronic access if available in the Patient Portal through the EMR and at no charge
- Specific exceptions may apply to restrict access including:
  - Access would violate HIPAA or other privacy laws
  - Access is not technically available or feasible
  - Access would result in a security breach based on West’s security policies

West’s Commitment to HIPAA Compliance

- It is the responsibility of West Cancer Center to protect the privacy and security of PHI in all forms.
- A HIPAA breach occurs when PHI is accessed, disclosed, shared, or used in any way that violates HIPAA regulations. Examples include:
  - Lost or stolen documents, laptops, iPads, cell phones, media devices, CDs, flash drives, etc.
  - Unauthorized electronic access using “malware” such as viruses, worms, spyware (hacking)
  - Email or faxes sent to the wrong address, person or number
  - Message left on the wrong voicemail
  - Information placed on the internet or a social media platform
  - Talking about a patient in a non-confidential manner.
- Prevention is the key to ensuring that HIPAA breaches do not happen.

Prevent HIPAA Breaches

- Check with your manager if you are unsure about your access to a patient’s medical record.
- Always log off a computer when you have completed your work and left the workstation.
- Keep your password confidential.
- Never snoop in a medical record out of curiosity – even for a friend or family.

WEST
CANCER CENTER
& RESEARCH INSTITUTE

Prevent Employee Breaches

Unless you are actively caring for or documenting records employees should not be in PHI of any form belonging to:

- Other employees
- Employee family members
- Family
- Friends

This is a federal law. Without permission as specified violations can result in immediate termination.

Prevent Breaches when Faxing

- Fax machines used to send or receive PHI or other confidential information must be in secure locations.
- All faxes must have a West Cancer Center fax cover sheet with the approved confidentiality statement.
- Verify the receiving fax number with the intended recipient and confirm that the fax was received.
- If notified that a fax has been received in error, either arrange for the fax to be returned to West Cancer Center or ask the caller to destroy the fax. Document the name of the caller, fax number, date/time, patient name, and type of information on the fax. Complete an Incident Report.

Prevent Breaches when Using Electronic Storage Devices

Electronic information must be disposed through PathForward IT Support. Always seek approval from your supervisor before using any portable electronic storage device.

To safeguard PHI:

- Use encryption and password protection for laptops, cell phones, and flash drives.

Prevent Breaches when Using the Internet

- Avoid downloading files that you don’t recognize as being from West Cancer Center.
- Avoid opening emails that may be spam (not from a recognized sender).
- Avoid responding to requests for information via email.
- Avoid using similar or easy-to-guess passwords for various devices.
- Change your passwords frequently.
- Don’t click on unrecognized links.

Email Phishing and Social Engineering

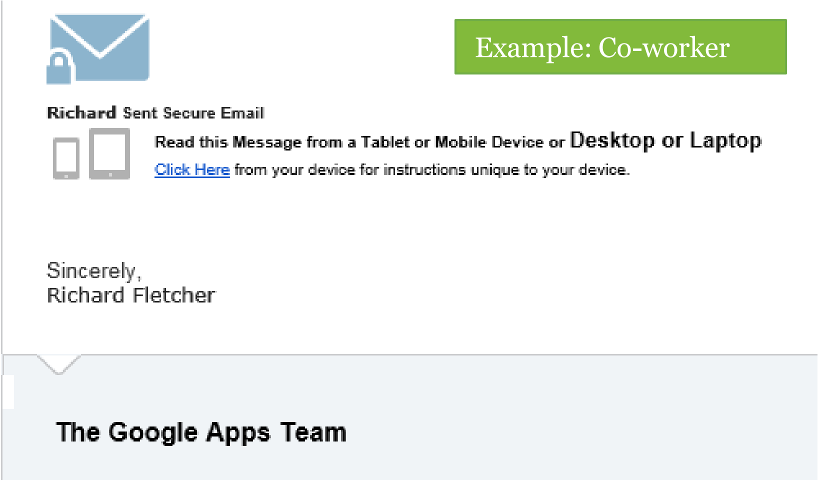
Beware of phishing communications and other forms of “fake” communications.

Why is this a problem?
Phishing emails and similar communications contain links or request information that may provide the bad actor with access to the West system.

- Emails, phone calls, text messages, and social media messages are used by hackers to gain access to computer networks
- The most common method is by email phishing.
- Emails may appear to come from a co-worker or trusted vendor.

WEST
CANCER CENTER
& RESEARCH INSTITUTE

Examples of phishing or other malicious communications



Example: Co-worker

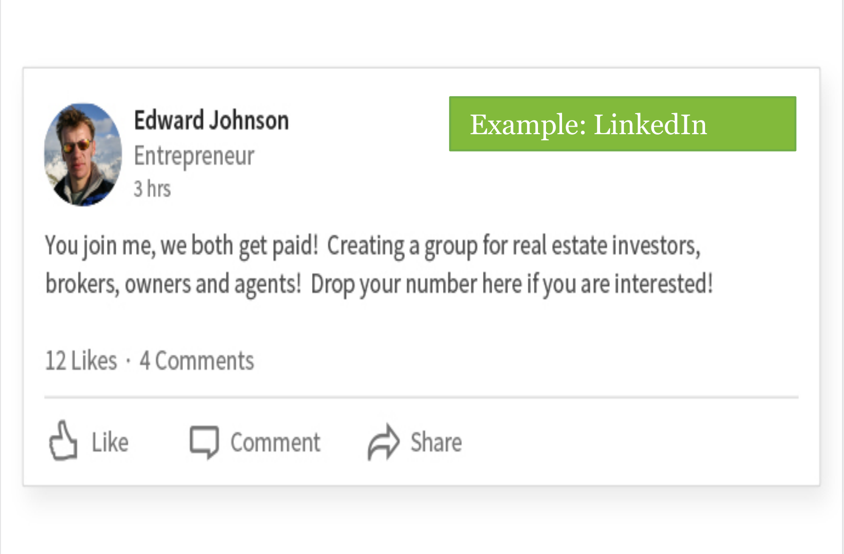
Richard Sent Secure Email

Read this Message from a Tablet or Mobile Device or Desktop or Laptop

Click Here from your device for instructions unique to your device.

Sincerely,
Richard Fletcher

The Google Apps Team



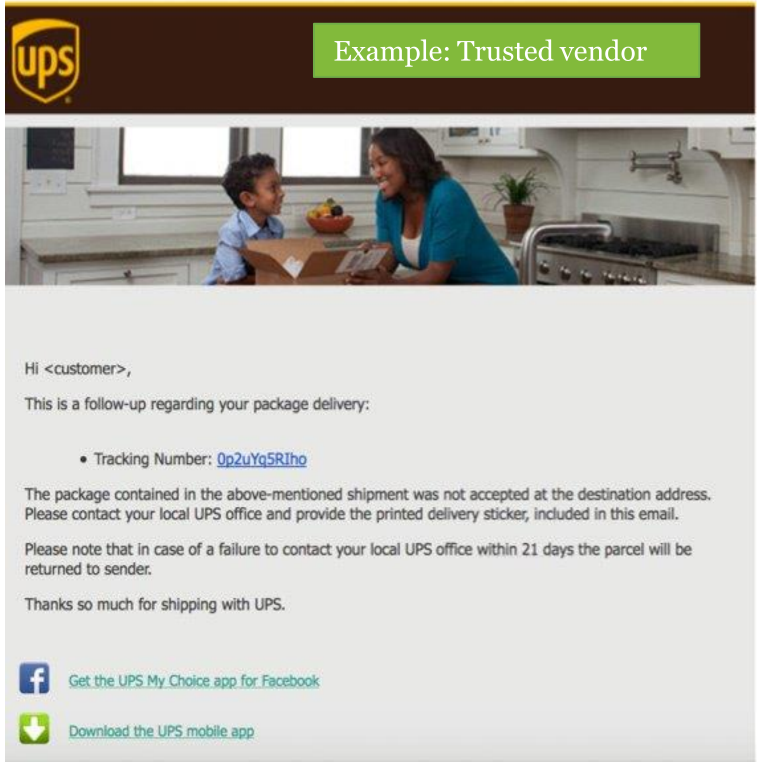
Example: LinkedIn

Edward Johnson
Entrepreneur
3 hrs

You join me, we both get paid! Creating a group for real estate investors, brokers, owners and agents! Drop your number here if you are interested!

12 Likes · 4 Comments

Malicious messages are not limited to email but may come in the form of text messages or other digital communications



Example: Trusted vendor

Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: 0p2uYq5RIho

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.

Get the UPS My Choice app for Facebook

Download the UPS mobile app

How can you detect a phishing email and what do you do?

To look for:

- Obvious grammar or spelling errors
- Unusual messages:
  - Urgent requests: “I really need your help this morning.”
  - Requests for personal information or West information
  - Requests to confirm or submit reports through an unusual link
  - Generic greeting/closing like “Your HR Team”

To Do:

Verify a suspicious message through a separate contact with the sender.

Hover over the email address or “Reply All” to see the “real” email.

Do NOT click on any links or provide information.

Contact IT immediately and report the communication.

Business Associates

Business Associates are individuals or companies hired to do work or to provide services for West Cancer Center.

When Business Associates have access to sensitive information, a written Business Associates Agreement is required of them to protect the information.

West Cancer Center is committed to the education of future generations of health care providers and requires an Affiliation agreement and Confidentiality Statement which is signed and kept on file.

Volunteers who provide support to our staff and patients are also required to maintain the privacy and security of patient information.

Prevent Breaches on Social Media

Always protect the privacy of our patients and their family members.

- Never discuss patient or patient care events on these sites, even if a name is not mentioned.
- Never discuss our patients' families or your coworkers – this violates the trust instilled in us as West Cancer Center associates.
- Do not post photographs of patients or other employees.
- Do not respond to "reviews" – negative or positive.
- Social Media Examples:
  - Facebook
  - Instagram
  - Twitter
  - LinkedIn

Prevent Breaches via Photography

At West Cancer Center, taking photographs or videos of patients with personal cell phones is prohibited.

- All photographs taken of patients become part of the medical record and the property of West Cancer Center.
- Never text message any patient information.

Doing What is Right

Making the right decision about compliance can be difficult or confusing. If you are unsure, ask yourself the following questions:

- Is this the right thing to do?
- Are my actions legal?
- Does it comply with our standards, policies, and laws?
- Is this in the best interest of West Cancer Center and our patients?
- Am I being fair, honest, and truthful?
- Could my action harm patients, employees, physicians, or others?
- Would I be proud to see it on the news?

If you are ever in doubt or have questions, contact your supervisor or Human Resources.

Reporting a HIPAA Breach or Violation

Each West Cancer Center team member is responsible for HIPAA Compliance:

- Perform all duties honestly and truthfully.
- Don’t be involved in any “cover-up” activities.
- Always keep the patient and family members’ best interests in mind.
- Be accurate and factual in your communication.
- **Promptly Report** any breach or violation to your manager/supervisor, the compliance team or the compliance hot line and complete an Incident Report.

COMPLIANCE HOTLINE: 1-888-394-2306

Compliance & HIPAA Training - Conclusion

This concludes Module 1 – 2023 Compliance & HIPAA Training.

This course includes four modules:

- Module 1 – 2023 Compliance & HIPAA Training
- Module 2 – 2023 Infection Prevention Training
- Module 3 – 2023 Safety Training
- Module 4 – 2023 Sexual Harassment Prevention

After completing all four modules, each employee is required to pass the annual test with a score of 90% or higher. You have three attempts to pass the test. You may refer these modules during the test if needed.

Thank you!