WEST
CANCER CENTER
& RESEARCH INSTITUTE

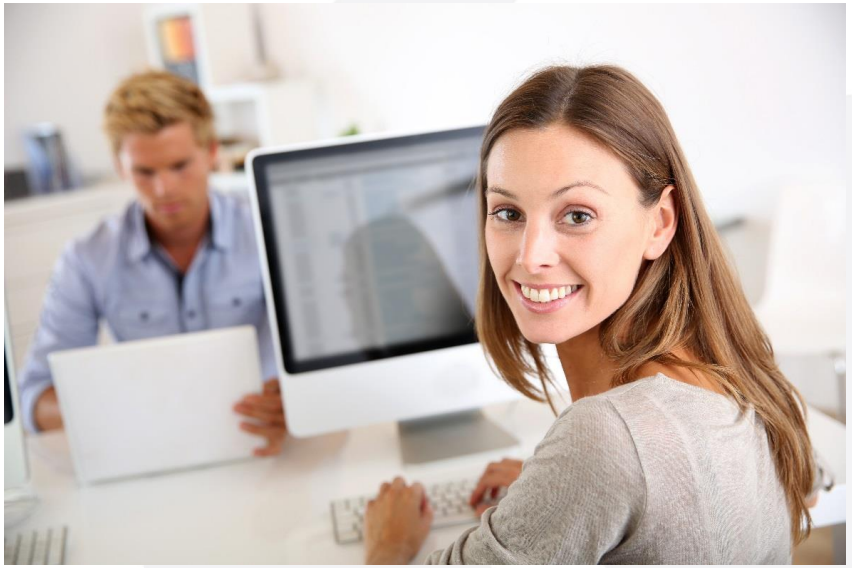
partner of OneOncology

Corporate Compliance Training

What is Compliance Training?

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

- Laws
- Regulations
- Company Policies



The Way We Do Business as West Cancer Center

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 Ethics

Our Code of Ethics states that at West Cancer Center…

- All activities are in compliance with applicable laws and regulations.
- We provide quality care in an ethical and professional manner.
- We maintain the confidentiality of patient records, including financial and other confidential or sensitive information.
- We value our Associates and Physicians and are committed to their professional success.

What are the Benefits of an Effective 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

What is My 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 supervisor or use the compliance hot line
- Be accurate and factual in your communication

We have a Compliance Team at WCC

Our Compliance Team

- Chief Compliance Officer – Mitch Graves, CEO
- Chief Medical Officer - Dr. Kurt Tauer
- Compliance Advisor - Cheryl Prince, VP-Clinical Integration

We also have a Compliance Hotline:

1-844-473-5115

- 24 hours-a-day/ 7 days-a-week
- Confidentiality ensured
- Anonymity possible

What are some examples of reportable Compliance issues?

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

Fraud

Examples of Violations to Report:

- HIPAA Privacy and Security (HIPAA 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 can be HUGE problems for Compliance.

Coding and Billing - It's Complicated!

- One of the greatest risk areas for healthcare providers' compliance problems
- Must be complete and accurate
- Must represent reasonable and necessary services
- If in doubt… always ask!!!! Don't make it up!

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 actually provided by a non-physician

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 patient files
- 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

- Designed to protect sensitive information known as Protected Health Information (PHI)
- Gives patients greater access to and protection of their medical records and more control over how they are used
- Assures that an individual's health information is protected while allowing the flow of health information needed to provide high quality health care

West Cancer Center HIPAA Privacy Rule

- Patients are given a copy of the West Cancer Center Privacy Notice the first day that healthcare is delivered.
- Attempts are made to get an acknowledgment of receipt.
- The notice informs patients how West Clinic will use or disclose their PHI.
- Privacy Notice posters are located in the reception room and on the website.
- We **must** make reasonable efforts to identify patient representatives and disclose information accordingly.

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
- Electronic Mail Addresses
- Biometric Identifiers – including Finger and Voice Prints
- Full Face Photographic Images and Any Comparable Images

At West Cancer Center there are several forms of Sensitive Information

Printed

Verbal

Electronic

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

What is a HIPAA Breach?

A *HIPAA Breach* occurs when PHI is accessed, disclosed, shared or used in a way that violates the HIPAA Regulations.

How can a HIPAA Breach occur?

- Lost/stolen paper documents, laptops, iPads, cell phones, media devices, CDs, flash drives, memory drives
- Hacking – unauthorized electronic access using “malware” such as viruses, worms, spyware
- Email or faxes sent to the wrong address, person, or number
- Message left on the wrong voicemail
- Information placed on internet or social media such as Facebook
- Verbal Communication – employees talking about a patient in a non-confidential manor. Example: employees discussing a patient in a crowded room with a loud tone of voice.

If a HIPAA Breach is Suspected:

Report all possible breaches immediately to:

- Your Director, Manager, or Supervisor
- Compliance Officer – Mitch Graves, CEO
- The Compliance Hotline: 1-844-473-5115

Prevention is the Key to Ensuring that HIPAA Breaches Don’t Happen

Breaches can occur with the **Electronic Medical Record (EMR)**

How to avoid problems:

- Ask your supervisor if you are unsure if your access of a patient's medical record is part of your job responsibility.
- Always log off a computer when you have completed your work and left the workstation to prevent others from accessing medical records under your log in and password.
- Keep your password confidential. This may prevent others from using your password to access medical records inappropriately.
- Never snoop in a medical record out of curiosity. You should only be looking at the EMR to meet your job requirements.

Breaches Can Occur During **Faxing**

- Fax machines used to send or receive PHI or other confidential information must be in secure locations.
- All faxes should have a West Cancer Center fax cover sheet with 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.

Breaches Can Occur with Electronic Storage Devices

- Electronic information should be disposed of 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.

Breaches Can Occur With **Internet Security**

Protect Your Electronic Systems by Following These Guidelines:

- 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.

Breaches Can Occur with Business Associates and Students

- 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 students to sign an affiliation agreement and confidentiality statement which is signed and kept on file.

Breaches can occur with 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.

Cell Phones, Photographs, and Videos

- 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

Sometimes making the right decision for compliance can be difficult or confusing. If you are unsure, ask yourself these simple 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, associates, 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.