WEST
CANCER CENTER
& RESEARCH INSTITUTE

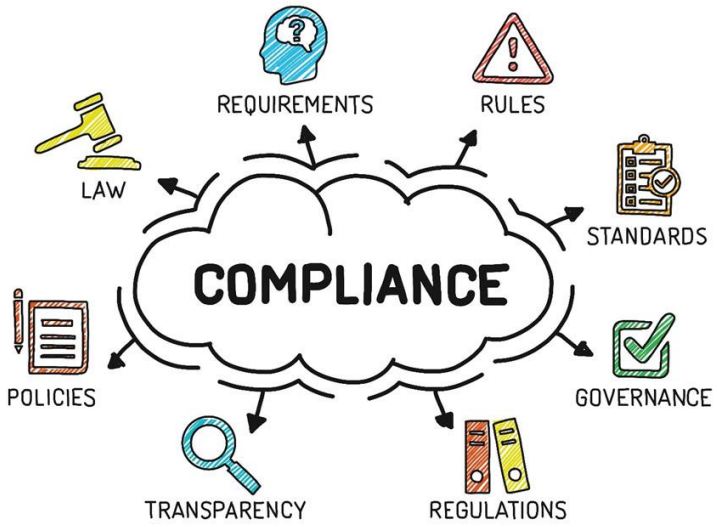
Module 2 – HIPAA Compliance

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

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

What are examples of reportable Compliance issues?

- Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Breach
- Insurance Fraud/Abuse
- False Claims
- 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

WEST CANCER CENTER & RESEARCH INSTITUTE

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

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 (printed, verbal, or electronic)
- Related to the physical or mental health of an individual
- Care provided to the individual
- Payment for healthcare provided to an individual

WEST CANCER CENTER & RESEARCH INSTITUTE

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

PHI - Security Safeguards

Security Safeguards assure patients that we will protect their information. Covered Entities and Business Associates must have administrative, physical, and technical safeguards.

- Examples of reasonable safeguards:
- Training for all staff
- Company Shred bins will remain locked and be emptied on schedule.
- 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

HIPAA Privacy Rule

The Privacy Rule standards address the use and disclosure of individuals' health information (known as *protected health information* or *PHI*) by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities."

The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used. A major goal of the Privacy Rule is to make sure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality healthcare, and to protect the public's health and well-being. The Privacy Rule permits important uses of information while protecting the privacy of people who seek care and healing.

- Directs Covered Entities on 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.

WEST CANCER CENTER & RESEARCH INSTITUTE

Audit Logging and Monitoring
Proper Disposal of PHI

West Cancer Clinic reviews and analyzes audit records for evidence of suspicious, unusual, and inappropriate activities, as necessary.

All paper documents containing PHI must be shredded regardless of work location. Place paper in designated shred bins only.

- Do not use waste baskets or boxes to hold documents to be shredded.
- Hard drives that need to be replaced will be removed and arranged for proper scrubbing of data prior to disposal.

WEST CANCER CENTER & RESEARCH INSTITUTE

Patients' Rights to Access

Patients have a right to inspect, and or request a copy of their medical records.

Patients may request records in a specific format and West Cancer Clinic must comply with the request if the data is readily producible. If not readily producible in the patient's specified format, West Cancer Clinic will work with the patient in an agreed upon format.

If West cannot reach a decision, then a hard copy of the record will be provided.

Records of Minor Patients

As the minor's personal representative, parents can have access to their child's medical record when such access is consistent with state or other laws. **There are three situations when the parent would not be the minor's personal representative under the HIPAA Privacy Rule.**

- When the minor is the one who consents to the care and the consent of the parent is not required under state or other applicable law.
- When the minor obtains care at the direction of a court of law or a person appointed by the court.
- When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

WEST CANCER CENTER & RESEARCH INSTITUTE

Patients' Rights to Access

Patients can request an Accounting of Disclosure (AOD).

HIPAA allows patients to learn to whom West Cancer Clinic has disclosed their protected health information (PHI) for 6 years prior to the date of the request.

Disclosures of PHI that are not for treatment, payment or health care operational purposes must be documented.

Examples of disclosures that are tracked, but not limited to:

- Those related to a subpoena or court order
- Disease reporting to the Department of Health
- Provided information to registries
- Any breach of PHI

WEST CANCER CENTER & RESEARCH INSTITUTE

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 frame –
  - 30 -60 for offsite records
  - 10 days or less for onsite
- 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

Information Blocking

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 CANCER CENTER & RESEARCH INSTITUTE

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.

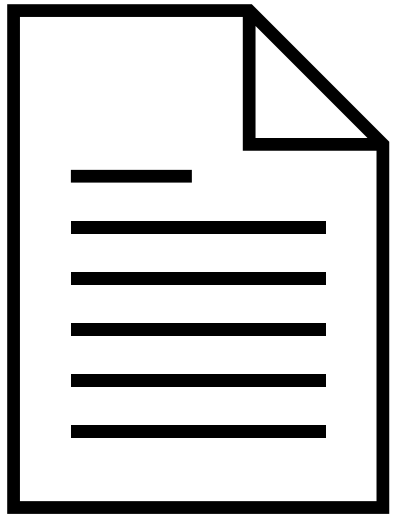
Pre-Emption Rule

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)



WEST CANCER CENTER & RESEARCH INSTITUTE

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

HIPAA Breaches

A HIPAA breach occurs when PHI is accessed, disclosed, shared, or used in any way that violates HIPAA regulations.

Examples include:

- 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.

Prevent Breaches when Using Electronic Storage Devices

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

Creating Strong Passwords - A compromised password can impact patient care!

- A strong password consists of at least 8 characters long and include a combination of:
- Lowercase and uppercase letters
- At least one Number
- At least one special character (i.e.. !,@, #, $,%)

To help keep your password safe and secure:

- Do not include your password in an email, text message, or other electronic communications.
- Do not share your password with others.
- Do not leave your password written down at your desk.
- Do not use your name or social security number as part of your password

If you think your password has been compromised, report the issue immediately to IT support.

WEST CANCER CENTER & RESEARCH INSTITUTE

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.

WEST CANCER CENTER & RESEARCH INSTITUTE

Billing and Coding

Billing and coding represent the greatest risk areas for healthcare providers.

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

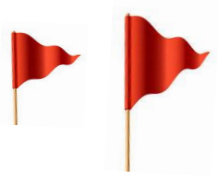
- Presents or causes to be submitted a false or fraudulent claim for payment
- Makes or uses a false record or statement material to a false or fraudulent claim or material to an obligation to pay
- Conceals or avoids or decreases an obligation to pay money to the government

Billing and Coding

- Submitting a false claim to the government to obtain payment
- Submitting a claim **for medically unnecessary services**
- Knowingly providing false information to payers
- **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**

Medical Identity Theft

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



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 number that matches one that is already part of another patient's registration 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

WEST CANCER CENTER & RESEARCH INSTITUTE

Prevent Breaches when Using the Internet

- Avoid downloading files that you don’t recognize as being from West Cancer Center.
- Avoid using similar or easy-to-guess passwords for various devices.
- Change your passwords frequently.
- Don’t click on unrecognized links.

WEST CANCER CENTER & RESEARCH INSTITUTE

Prevent Breaches on Social Media

Social media networking sites shall not be used by West Cancer Clinic personnel that would risk, cause, or suggest:

- The compromise or disclosure of Protected Health Information (PHI) or other protected personal, financial information of any patient or patient family member, including photographs of employees engaged in patient care.
- The disclosure of any business-related, technological, or academic information related to the activities and operations of The West Cancer Clinic.
- The use of social networking sites, such as Facebook, Twitter, Instagram, YouTube, etc. can all result in HIPAA violations even if you never identify a patient's name.

WEST CANCER CENTER & RESEARCH INSTITUTE

Prevent Breaches on Social Media

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

Examples of HIPAA violations include:

- Never discuss our patients' families or your coworkers – this violates the trust instilled in us as West Cancer Center associates.
- Posting a status on Facebook detailing the care of a patient even if a name is not mentioned.
- Posting a picture of a radiology image showing an unusual injury or disease
- Blogging about care for a patient
- Posting a picture of a picture of a co-worker that also shows a patient or PHI in the background
- Responding to a patient complaint posted on social media
- Do not respond to "reviews" – negative or positive.

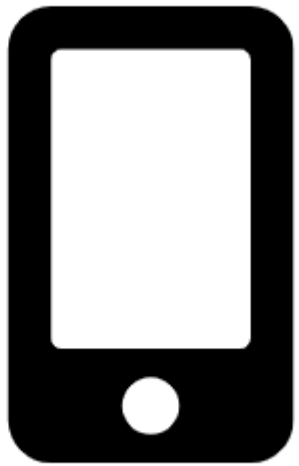
WEST CANCER CENTER & RESEARCH INSTITUTE

Prevent Breaches via Photography

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

Employees should not take photographs or recordings of patients for non-clinical purposes except as authorized for marketing or educational purposes.

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



WEST CANCER CENTER & RESEARCH INSTITUTE

Prevent Breaches via Photography

Patients, family members, and/or patient visitors are generally permitted to take photographs or recordings of one another provided that such activity does not involve other patients.

Staff may request to not be included in patient photos and/or recordings; however, patients may record without consent.

Patients may have a legitimate care purpose for the recording such as:

- Sharing health status with relative that lives out of town
- Patient is given sensitive diagnosis and needs to process or research once at home

WEST CANCER CENTER & RESEARCH INSTITUTE

Prevent Employee Breaches

West Cancer Clinic computers should be accessed by authorized personnel only.
Access to information and locations must be limited to the minimum amount necessary to do your job.

Access to an employee's PHI is unauthorized unless you are actively on the care team.

This includes PHI of any form belonging to:

•Other employees, providers, volunteers, contractors, and students
•An employee's family member(s)
•Yourself
• Your family
• Your personal friends

This is a federal law. Without permission as specified violations can result in immediate termination.
Check with your manager if you are unsure about your access to a patient's medical record.

WEST CANCER CENTER & RESEARCH INSTITUTE

Prevent Employee Breaches

An example of a less common - Asking Provider's for prescriptions or off the record medical advice.

Employees of West should **not ask our providers they work with for prescriptions**—even if they have a friendly or professional relationship—for multiple reasons:

- Ethical Boundaries and Professionalism Relationships- Providers may feel pressured to prescribe even when it's not medically appropriate. **It can create conflicts of interest, especially if the doctor is in a supervisory or evaluative role.**

- Legal and Regulatory Risks- **Prescribing medication without a formal patient-doctor relationship may violate medical licensing laws.** The American Medical Association (AMA) discourages prescribing to colleagues unless in emergency or isolated situations. If something goes wrong (e.g., side effects, misuse), the prescribing doctor could face liability or disciplinary action.

Prevent Unauthorized Access

Unauthorized people may try to access the work area.

- Always verify outside workers before allowing them into the work area.
- Pay attention to anyone without a West Cancer Clinic ID badge requesting access to an IT equipment room.
- Watch for anyone who may try to enter the employee entrance without an ID badge.
- Always log off a computer when you have completed your work and left the workstation.
- Keep your password confidential.

WEST
CANCER CENTER
& RESEARCH INSTITUTE

Patient Authorization FAQ

Does a patient need to sign an Authorization to get a copy of the patient's record?

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

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

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

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

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.

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

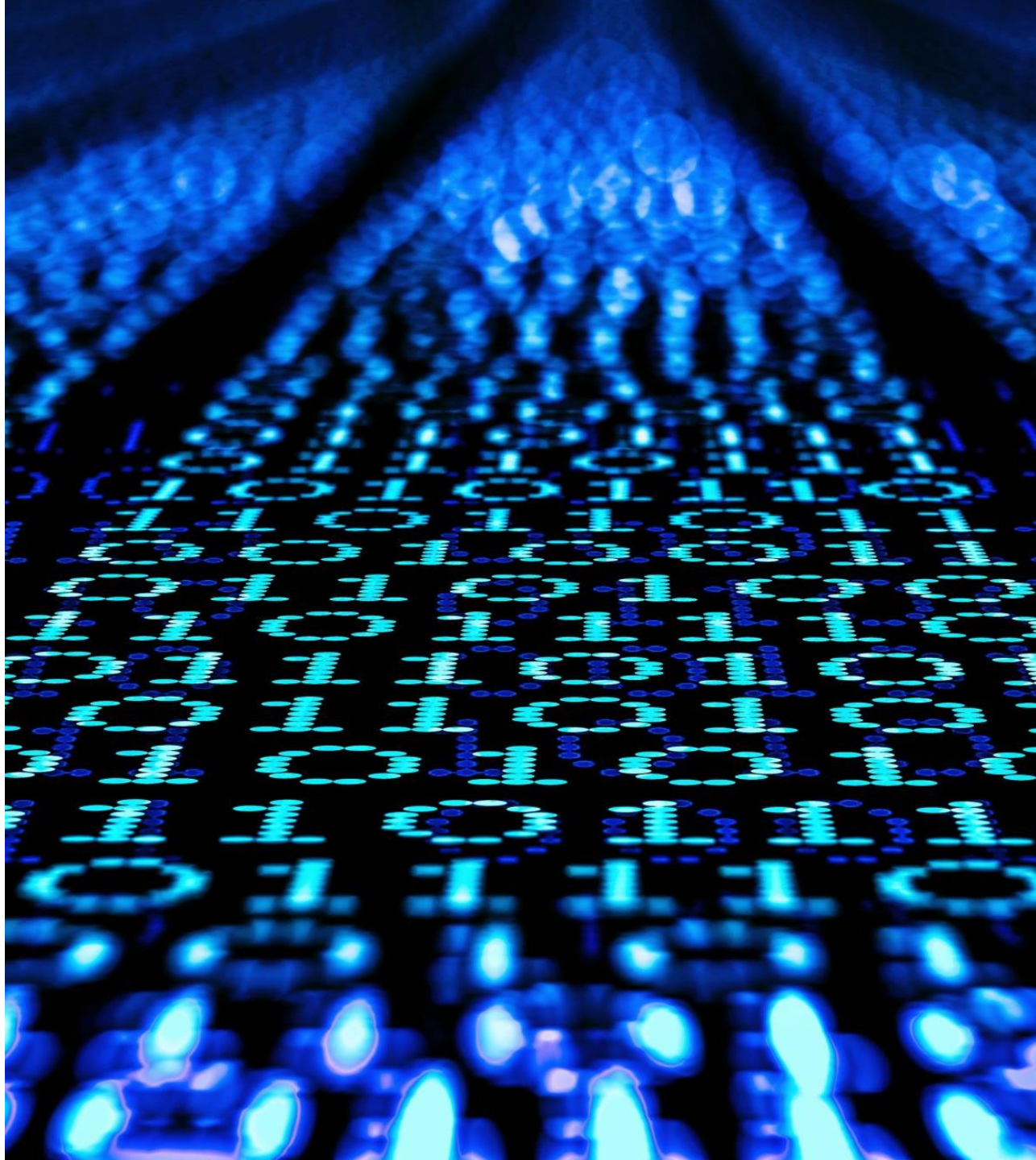
The patient's parent, guardian or other legal representative is treated the same as the patient. You may rely on the reasonable representation of the person's relationship the patient. You may ask for documentation to support the relationship.

WEST CANCER CENTER & RESEARCH INSTITUTE

Information Technology Security

Information Technology Security

- Email Security
- Ransomware
- Phishing Emails
- Data Security Concerns



What is Email Security?

Email security is the practice of protecting email accounts and communications from unauthorized access, loss, or compromise.

Organizations can enhance their email security posture by establishing policies and using tools to protect against malicious threats such as malware, spam, and email Phishing attacks.

WEST CANCER CENTER & RESEARCH INSTITUTE

Why is Email Security Important?

Email is one of the primary communication tools used in the workplace. More than 300 billion emails are sent and received daily worldwide. This creates an opportunity for cybercriminals to use malicious emails to attack businesses.

Ninety (90) percentage of cyberattacks begin with a malicious email.
Emails attacks cost companies billions of dollars a year.

Encrypting email messages help protect sensitive information such as Patient Health Information (PHI) and Financial information from being read by anyone other than the intended recipient(s).

What are the benefits of Email Security?

An email security solution that safeguards employee communication and reduces cyberthreats is important because:

- It helps protect a company's sensitive information and ensure compliance with data protection laws such laws.

- It can help circumvent business disruptions, legal fees, regulatory fees, and operational losses that stem from an email cyberattack.

WEST CANCER CENTER & RESEARCH INSTITUTE

What can I do to protect our email accounts?

There are a couple of things we can do to protect our email accounts, email content, and communication against unauthorized access, loss, or compromise.

1. Always verify the intended email recipient's email address is correct before sending an email.

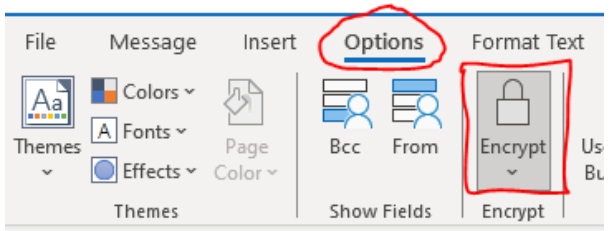
2. Always use an email encryption method when sending sensitive information to a non-West (external) email address.

WEST CANCER CENTER & RESEARCH INSTITUTE

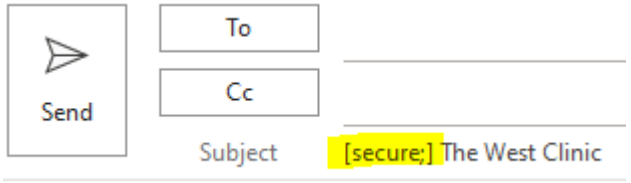
Encrypted Emails

There are 2 ways to send an encrypted email.

Option 1: Before sending an external email with sensitive information, click on options and click the Encrypt button.



Option 2: Adding [secure;] in the subject line of the email will also provide email encryption to the message. Either option will work to secure you email messages.



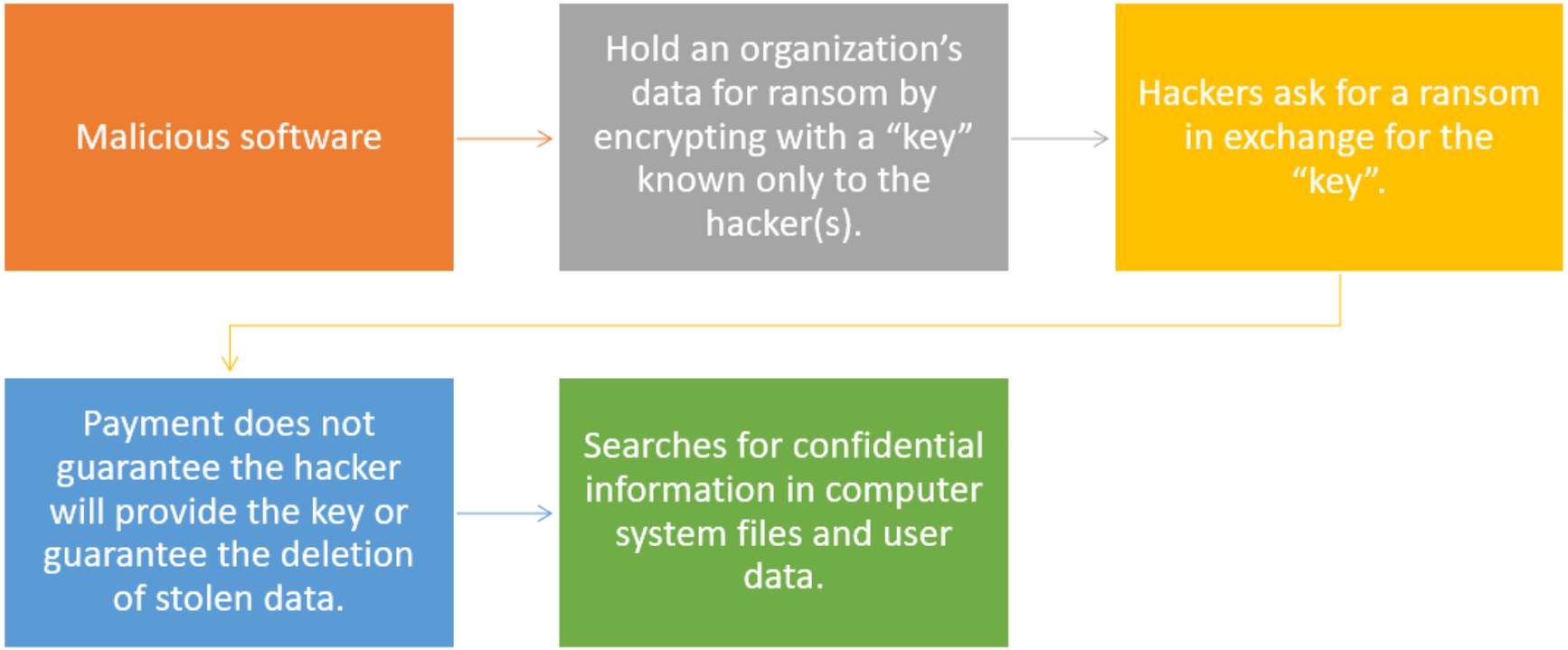
WEST CANCER CENTER & RESEARCH INSTITUTE

What is ransomware?

Ransomware is a type of code that holds a victim's sensitive data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker.

It is intentionally written to harm computer systems or their users

How does ransomware work?



Types of Ransomware

There are several types of Ransomware, but the three main types are:

Locker Ransomware – Denies access to a computer or device it is installed on.

Crypto Ransomware – Prevents access to all files or data.

Scareware –Tactics to trick the user to install ransomware without knowing.

Examples include popups on the computer or emails that state

- “Attackers can see your IP address, click here to protect your computer.”
- “Your PC is running slow, click here to speed it up.”
- “Your password has been compromised, click here to update it immediately.”

What is Phishing?

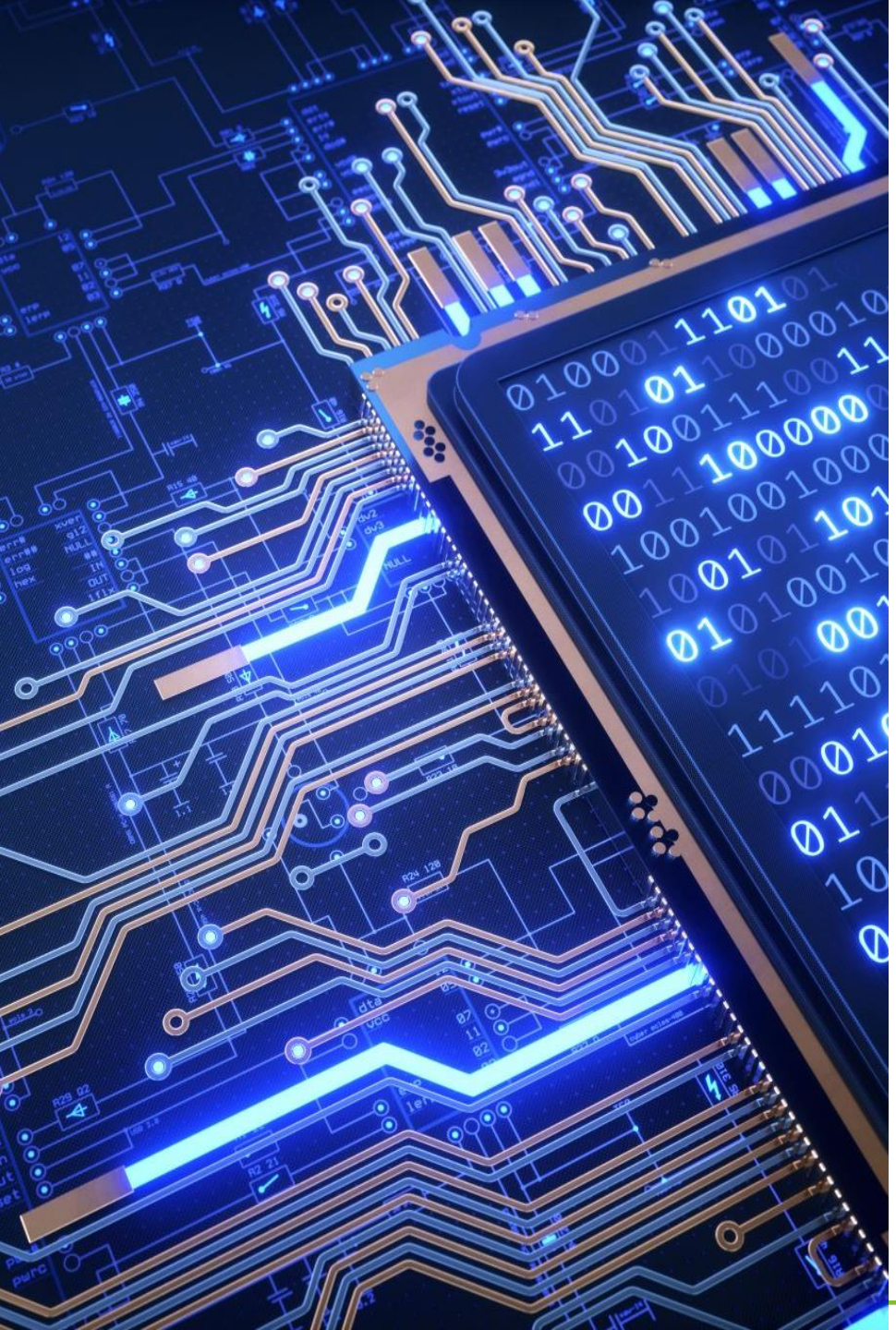
Phishing email messages, websites, and phone calls are designed to steal money or sensitive information.

Cybercriminals can do this by installing malicious software on the computer, tricking users into giving them access to sensitive.

Four ways a phishing attack is designed to trick users:

Click an Unsafe Link	Click Here!
Open an Unsafe File	
Type in your password	**********
Transfer funds	

WEST CANCER CENTER & RESEARCH INSTITUTE



Types of Phishing Attacks

Social Engineering – A social media profile often has personal information such as: Name, Date of Birth, Location, Workplace, Interests, Phone number, and Email Address This is everything a cybercriminal needs to fool a user into thinking that an electronic message or email is legitimate.

Link Manipulation - Phishing websites, also known as spoofed sites, are fake copies of real websites that you know and trust. Hackers make these spoofed sites to fool you into entering your login credentials, which they can then use to log into your actual accounts.

Voice Phishing - Attackers will attempt to convince targeted individuals over the phone to disclose personal information that can later be used for identity theft. Many robocalls are phishing attempts.

WEST
CANCER CENTER
& RESEARCH INSTITUTE

Tricks of the Trade

Phishing messages are designed to get you to react quickly without thinking or thoroughly reviewing the message.

Requesting services

Offering money

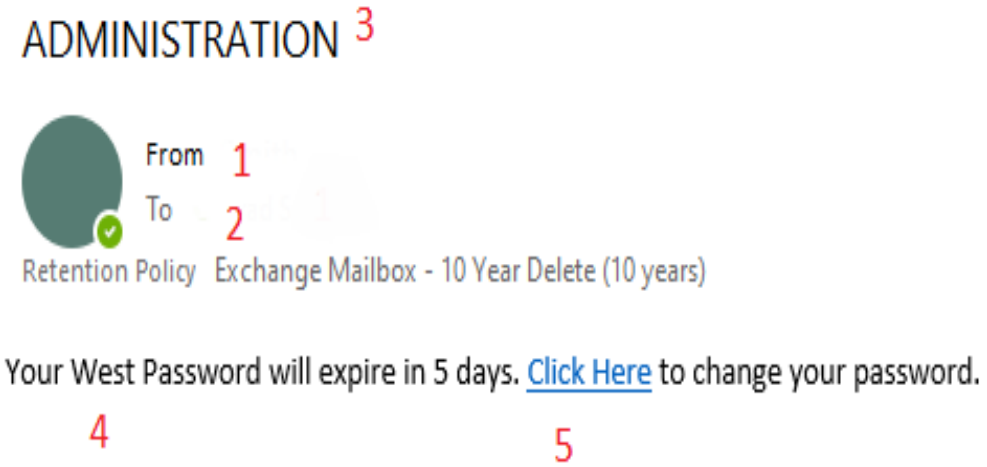
Requesting confirmation

Creating a sense of urgency

Offering rewards or incentives

Posting as IT support

Spotting a Phishing Email



1. Review the “From” field. Do you know the person? Or Are you expecting an email from that person? If the answer is **no** to either question you should take a harder look at other aspects of the email.

2. A large amount of phishing emails will blank out the “To:” or “Cc:” fields. The user cannot see that this is a mass email sent to a large group of people.

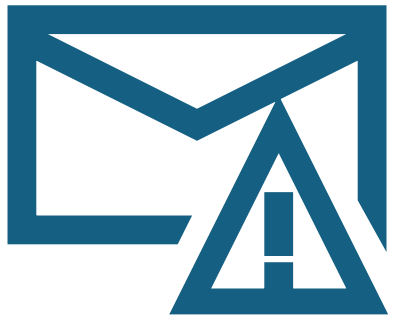
3. Phishing emails will often come with subject lines that are in all capitals or have multiple exclamation marks to make the user believe the email is important and follow the instructions in the email.

4. This is a targeted email (Spear Phishing) to West Cancer Clinic. It was likely sent to everyone at West Cancer Clinic found in the sender’s address book.

5. Hovering over the link will allow the user to see that this is not directed to the WCC address, but an external site. This site would prompt you for a password and steal the password or download a malicious file infecting the computer.

WEST CANCER CENTER & RESEARCH INSTITUTE

Tips to protect yourself from Phishing attacks…



- Do not click any links inside an email. Investigate!
- Be cautious about opening attachments and downloading files from emails.
- If you receive a suspicious email from a sender you recognize, contact the sender and verify the email is legitimate.
- Don’t open spam email messages.
- Contact IT if you suspect your computer has or application(s) have been compromised.
- IT will never ask for passwords through email. Never send passwords, bank account numbers, or other private information through email.

WEST CANCER CENTER & RESEARCH INSTITUTE

Email Encryption Protection

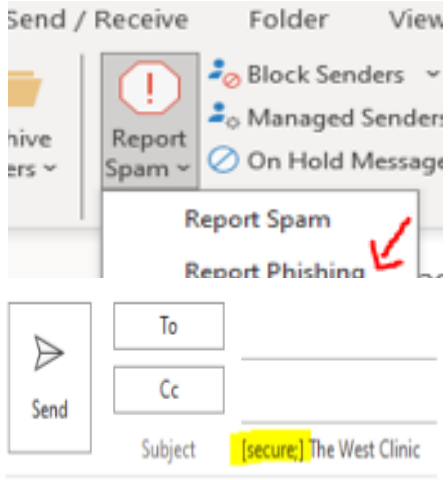
There are things we can do to protect our email accounts, email content, and communication against unauthorized access, loss, or compromise.

- Always verify the intended email recipient's email address is correct before sending an email.
- Always use an email encryption method when sending sensitive information to a non-West Clinic email address.

There are 2 ways to send an encrypted email.

Option 1: Before sending an external email with sensitive information, click on options and click the Encrypt button.

Option 2: Adding [secure;] in the subject line of the email will also provide email encryption to the message. Either option will work to secure you email messages.



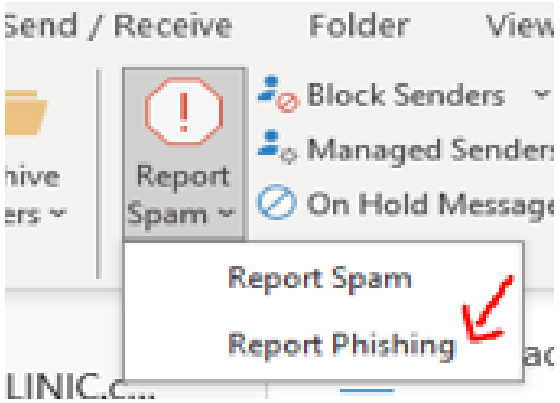
WEST CANCER CENTER & RESEARCH INSTITUTE

Phishing Protection

If you receive a suspicious email, do not click on any links within the email.

You should highlight the email in your inbox and click on Mimecast at the top of outlook.

1. Next, find the button on the toolbar called “Report Spam”.
2. Then click the down arrow on the Report Spam button
3. Select Report Phishing.



If you believe you have received a phishing email or phishing phone call at work, contact IT support at:

support@pathforwardit.com

WEST CANCER CENTER & RESEARCH INSTITUTE

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.

WEST CANCER CENTER & RESEARCH INSTITUTE

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.

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

WEST CANCER CENTER & RESEARCH INSTITUTE

Tennessee Whistleblower Act

The **Tennessee Whistleblower Act** and related laws provide strong protections for employees who report illegal, unethical, or unsafe practices in the workplace.

- 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

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 and concerns about activity that may not be truthful or honest to your manager/supervisor, the Compliance team, or Hot Line.

Be accurate and factual in your communication

WEST CANCER CENTER & RESEARCH INSTITUTE

This concludes Module 2 – HIPAA Compliance

Thank you!

WEST
CANCER CENTER
& RESEARCH INSTITUTE