Privacy, Confidentiality & Cybersecurity Training & Awareness

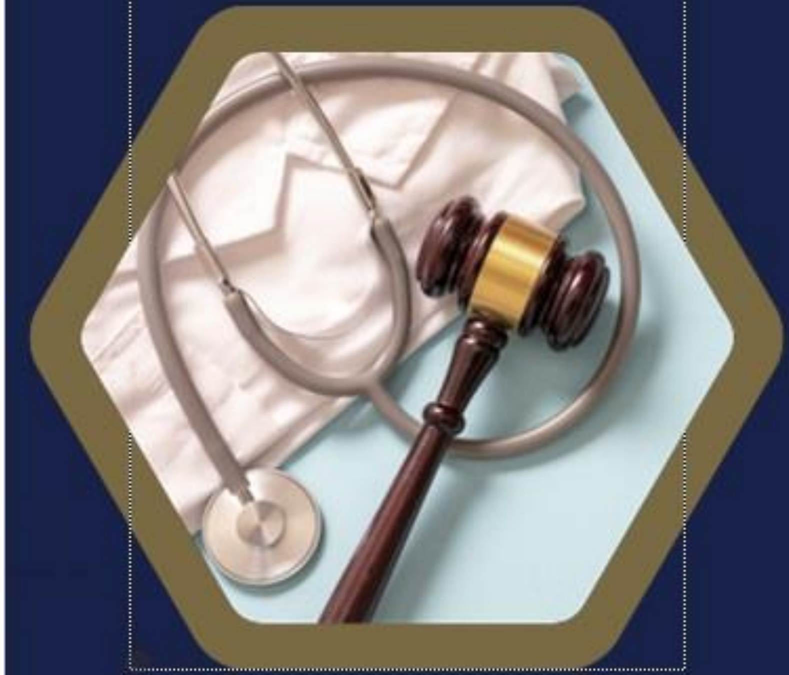
TransForm
SHARED SERVICE ORGANIZATION
Better Solutions. Better Care.

Overview

Cybersecurity, privacy, and confidentiality training are all critical for safeguarding our organization and our people. By raising awareness of potential threats, employees are better able to recognize and respond to cyber risks while also understanding the importance of protecting sensitive personal and organizational information. Learning best practices, such as securing sensitive data, maintaining strong passwords, and handling confidential information with care, plays a vital role in preventing breaches and unauthorized access. This training promotes both safe online behaviors like recognizing suspicious emails, securing browsing activities, ethically handling private data and ensuring compliance with regulatory standards. This training not only protects our data but also helps maintain trust, ensures legal compliance and prevents costly legal penalties.

This training will help end-users:

- Understand and comply with key regulations
- Protect & handle privacy, sensitive data & EHRs
- Create and manage strong passwords
- Secure mobile devices
- Navigate remote access securely
- Follow proper incident reporting protocols
- Identify different types of cyber threats & phishing



Module 1:

Personal Health Information Protection Act (PHIPA)

Module 1: PHIPA

What is PHIPA?

Personal Health Information Protection Act (PHIPA) is a privacy law in Ontario, Canada, that governs the collection, use and disclosure of personal health information (PHI). PHIPA ensures that health information is protected while allowing effective delivery of healthcare services.

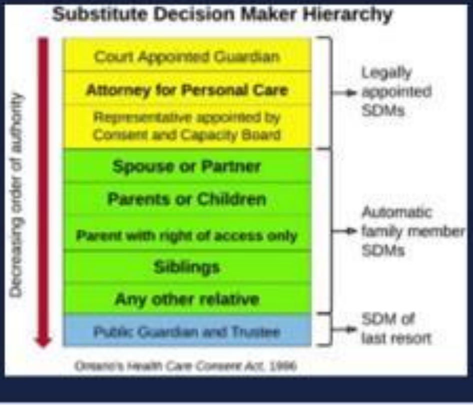
Who does PHIPA apply to?

- Health Information Custodians (HICs), their agents, substitute decision markers (SDMs), individuals or organizations in Ontario, including doctors, employees such as nurses and administrative staff, contractors such as IT service providers, volunteers and students.
- Agents are required to follow the same privacy standards as the HICs and must handle personal health information (PHI) according to the rules set out in PHIPA.

Key definitions to know

- PHIPA defines an agent to include any person who is authorized by a custodian to perform services or activities in respect of personal health information on the custodian's behalf and for the purposes of that custodian.
- A substitute decision maker (SDM) is someone who is appointed to make health and personal care decisions on a patient's behalf if they are unable to do so. Everyone in Ontario has an SDM even if he/she has never appointed someone in that role."

**Please review and be familiar with Privacy Confidentiality policies within your organization.*



Substitute Decision Maker Hierarchy

Decreasing order of authority

Court Appointed Guardian

Attorney for Personal Care

Representative appointed by Consent and Capacity Board

Legally appointed SDMs

Spouse or Partner

Parents or Children

Parent with right of access only

Siblings

Any other relative

Automatic family member SDMs

Public Guardian and Trustee

SDM of last resort

Ontario's Health Care Consent Act, 1996

What does Personal Health Information (PHI) include?

- Physical or mental health (past, present or future)
- Provision of healthcare services
- Family health history
- Health card number
- Any other identifying information collected during healthcare provision (e.g., medical records, diagnostic imaging reports, health insurance information)

How do you safeguard PHI?

PHI is best protected when proper administrative, physical and technical measures are used including:

- Encryption and limiting who can view or modify PHI.
- Securing disposal methods such as shredding paper records or using secure digital deletion.
- Seeking consent of individuals before their PHI is collected, used or disclosed.
- Maintaining accurate records of how PHI is handled, including access, updates and disclosures, as required from all HICs and their agents.
- Following policies, e-learning modules and confidentiality and user agreements.
- Providing access only to information and/or records needed for a particular role, as pertinent to circle of care.
- Not taking pictures at work and reviewing media consent and social media policy.
- Never sending identifiable patient information via email, except where policy allows for encryption and/or secure transfer.

*PHI is only to be accessed on a need to know basis and due to direct involvement in provisioning or assisting in provisioning health care services to an individual. PHI must be kept confidential even after discharge from the Hospital.

Scenario: Violating PHIPA

A nurse accesses a medical record of a neighbour's chart without the permission of the patient, out of curiosity.

This is a violation of PHIPA, which may lead to disciplinary action against the nurse and a fine for the hospital.

Proactively report privacy breaches to your Chief Privacy Officer (CPO). TransForm SSO and member hospitals utilize several auditing tools to detect breaches. If a breach meets certain thresholds, your CPO must report it to the Information and Privacy Commissioner of Ontario. Through this process, affected individuals will be notified as soon as possible.

Impact of PHIPA Violations

Violating PHIPA has various negative consequences, including enduring monetary penalties and experiencing reputational harm.

Reputational Harm

Privacy violations involving PHI undermines public trust, deters current and potential patients and damages an organization's overall reputation.

Patient Harm

Privacy violations can impact a patient's dignity and cause harm as it can result to stigma, embarrassment and discrimination.

Monetary Penalty

As of January 1, 2024, the IPC is authorized to charge monetary penalties to violators of the PHIPA. Penalties are up to a maximum of $50,000 for individuals and $500,000 for organizations.

Module 2:

Privacy

What is Privacy?

Privacy is the right of individuals to control the collection, use and disclosure of their personal information.

In Ontario, this includes PHI under PHIPA.

What are examples of key information that must be protected?

- Personal and sensitive information such as names, addresses, birthdates, social insurance numbers and contact information.
- PHI such as medical records and mental health data.

Module 2: Privacy

What are best practices to ensure protecting privacy?

Protecting privacy throughout daily operations is best attained through:

- Use of strong passwords
- Encryption of sensitive data, especially data containing PHI.
- Securing physical **and** digital records.
- Compliance with privacy laws by obtaining patient consent before sharing health records.

How should you respond to privacy incidents?

Healthcare providers are required by PHIPA to report breaches to the IPC that meet specific reportable criteria, and to potentially notify affected individuals. Privacy incidents include, but are not limited to, unauthorized access or disclosure (e.g., snooping), accidental access or disclosure (e.g., misdirected fax), or cyberattacks on health records. Please report any suspected privacy incident to your Chief Privacy Officer/Office.

What are some of the key privacy laws and regulations that you should know?

- Personal Health Information Protection Act (PHIPA)
- Freedom of Information and Protection of Privacy Act (FIPPA)

Categories of Severity for Privacy Breaches

Category	Description
🟡	- Isolated incident - non-identifiable health information. - Inadvertent breach using Electronic Patient record (EPR) (viewing of a previous screen due to incomplete system log out by user). - Faxed information to wrong recipient - non-identifying, non-confidential single incident.
🟡	- Faxed report to wrong recipient - PHI of a single patient.
🟠	- Faxed report to wrong recipient - PHI of multiple patients. - Unintentional breach or release of sensitive PHI of a single patient or PHI of multiple patients due to theft or loss of files, computer or portable information storage or computer device.
🟠	- Intentional unauthorized access of PHI of a single patient or multiple patients without further release to other parties.
🔴	- Deliberate release of patient, employees, affiliate or organizational confidential information to the media or other parties. - Deliberate use or release of patient, employee, affiliate, organizational confidential information for personal gain or malice. - Potential for fine or penalty under the PHIPA and its regulations.

Releasing information to law enforcement

Key information to know:

- Police are never in the circle of care and are **not automatically entitled** to obtaining patient information.

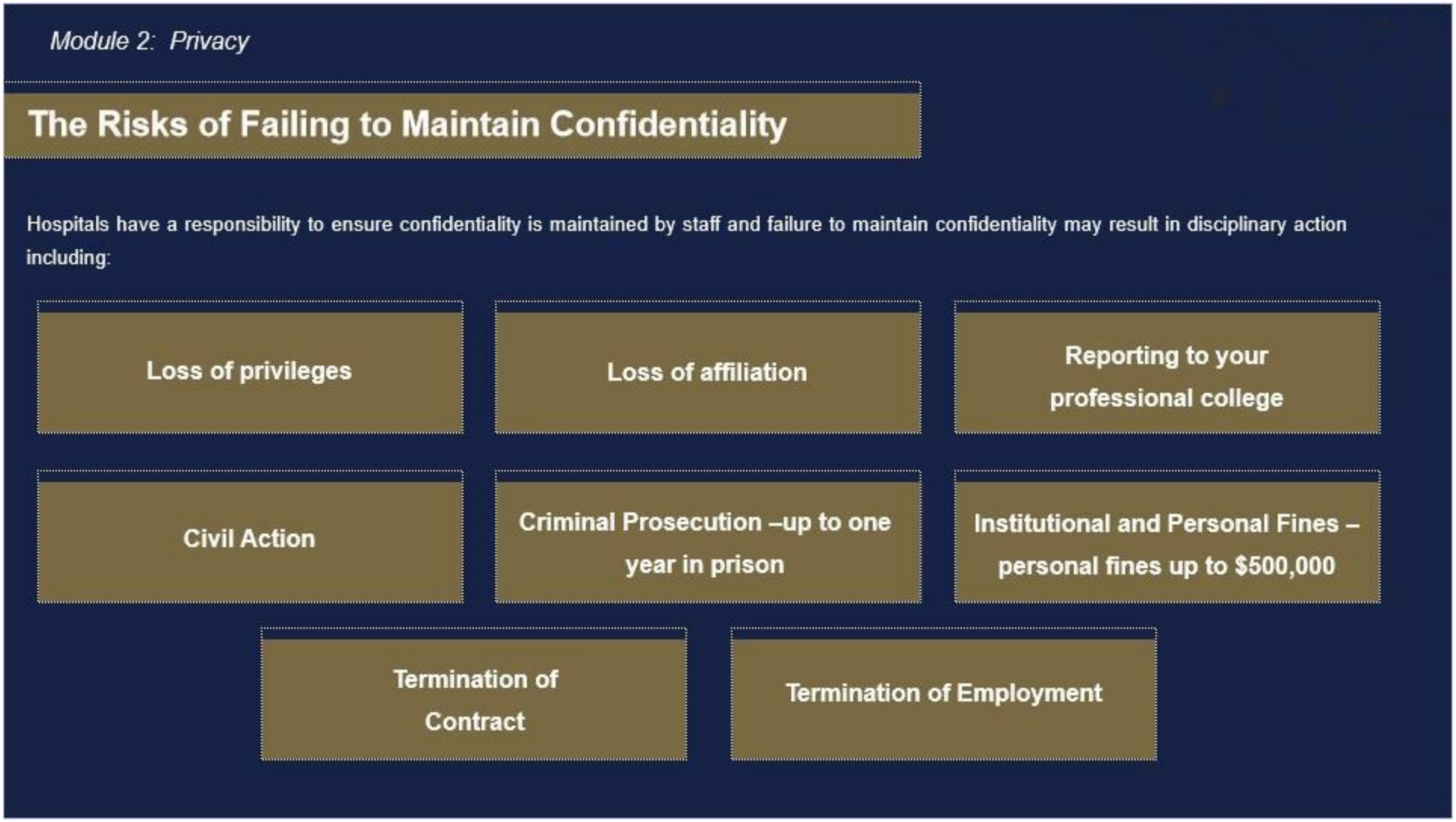
- Safety trumps privacy if there is an immediate risk of harm to the patient or to others.

When to release information to law enforcement:

1. The patient has given consent; or,
2. A search warrant has been produced; or,
3. A summons has been received to testify in court.

When in doubt:

- Contact your Risk Manager, Chief Privacy Officer or Manager on Call during after hours.
- Review the applicable section on release of information to law enforcement agencies within the privacy policy.



The Risks of Failing to Maintain Confidentiality

Hospitals have a responsibility to ensure confidentiality is maintained by staff and failure to maintain confidentiality may result in disciplinary action including:

Loss of privileges

Loss of affiliation

Reporting to your professional college

Civil Action

Criminal Prosecution –up to one year in prison

Institutional and Personal Fines – personal fines up to $500,000

Termination of Contract

Termination of Employment

Important Principles to Understand for Use of Information

Consent:

- Consent may be express or implied.
- Consent is required from the patient to collect, use, share (disclose) and retain information (unless the collection is reasonably necessary for the provision of health care, and it is not reasonably possible to obtain consent in a timely manner.)
- **Implied consent** is used for "most" core activities of the hospital. Implied consent is inferred based on the individual's actions and the facts of a particular situation. For example, if a patient gives you their personal health information directly so that you can provide a service, you may imply their consent to use the information for this purpose.
- **Express Consent** is a clear, conscious, and willing statement of agreement that can be verbal or in writing. This consent is required if PHI is to be disclosed to a person who is not a Healthcare Provider or to a Healthcare Provider who intends to use the information for other purposes than providing care to the patient.

Lockbox:

Patients have a right to make choices about their personal health information. One way a patient can exercise this choice is to ask to use "lockbox" (also known as a consent directive) to:

- Hide clinical information from healthcare providers within a hospital (note: an inpatient's records can't be locked until after they've been discharged) or
- Not disclose clinical information to external community healthcare providers for healthcare purposes.

*Only designated personnel in the Privacy Office can implement a lockbox. If a patient asks you about a lockbox, refer to your Lockbox policy and them to the Privacy Office.

Important Principles to Understand for Use of Information

Individual Access:

- Patients have the right to access their information, including viewing or requesting a copy of their record. They can view their information if they are accessing it via ConnectMyHealth.

- If the patient has been discharged and requires access or a copy of their record , please refer them to Health Information Management – Release of Information Office or to the provincial patient portal.

- Patients are part of their own care-team and provide information and contribute collaboratively with care team in the development of their medical record.

- Patients can access their own records by signing up for "Connect My Health", the Ontario portal to their own records and specific reports, which the hospitals contribute to: ConnectMyHealth Patient Portal: Access Your Health Records from Participating Southwest Ontario Hospitals

See Release of Information (ROI) Policy from your organization for guidance.

Module 2: Privacy

Inappropriate Access to Personal Health Information (PHI)

Review the Policies!

- Your hospital's privacy policy and acceptable use of information technology resources policy outline acceptable and inappropriate access to health records.

Examples of inappropriate access include, but are not limited to:

- Accessing electronic records of patients where access is not required to perform the duties for which an individual is employed or affiliated with the organization.
- Accessing including the user's own records and or those of family and friends using their system access privileges.
- Accessing patient records during times when not at work or on-call.
- Allowing or facilitating access to PHI by non-healthcare personnel.
- Accessing records of PHI that are not required of personnel in your role to provide care to the patient.

Inappropriate Access to Personal Health Information (PHI)

Staff or Friends as a Patient:

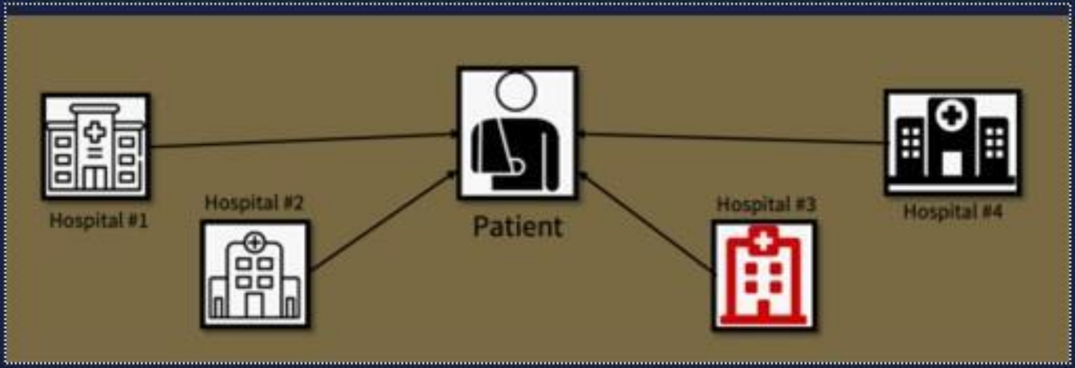
- If a friend or hospital staff member has received any health care services or treatment at the Hospital, they are then considered a patient/client in the context of the legislation, our Policy and our training practices and their personal health information is subject to the same policies and procedures as that of all Hospital patients/clients.

- Staff who wish to view their own records should follow the Release of Information (ROI) process and contact the Health Records department of the organization they originated. They may also access their own records through the provincial patient portal by signing up to " Connect My Health " .

- **DO NOT USE YOUR SYSTEM ACCESS TO VIEW RECORDS FOR YOURSELF, FAMILY, FRIENDS ETC., AS THAT WILL BE CONSIDERED A PRIVACY BREACH AND HANDLED AS SUCH.**

- Patients are notified of any accesses to their records that are investigated as a breach and have the right to know the name of the person who accessed their records.

Maintaining Privacy within a “Shared” Electronic Health Record System



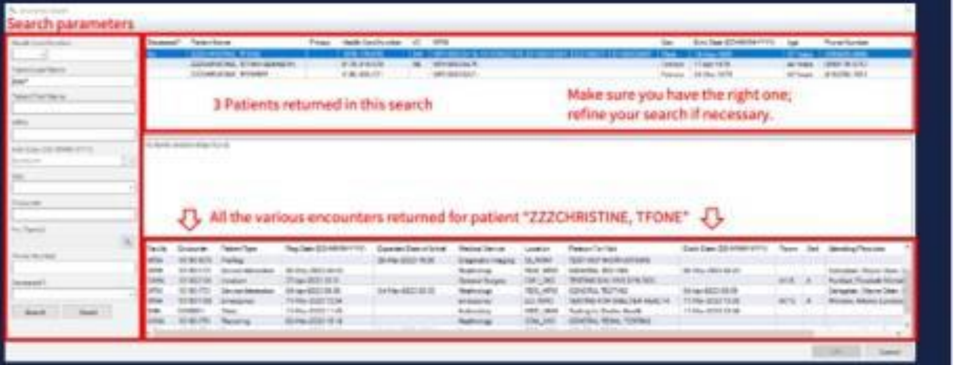
Assess whether you’re accessing the correct record:

Hospitals in the region often use systems such as the Oracle (Cerner) Electronic Health Record (EHR), Clinical Connect, Integrated Assessment Record (IAR) and other e-health supported systems. Often these systems provide global type access to our partners in order to better care for our patients who cross over the system and organizations caring for them.

Many system users are in a role where they have visibility to visit history and documentation created for patients within these hospitals, but have a responsibility under PHIPA to only access and use this information under the appropriate circumstance but are accountable for their access using these shared systems. Therefore, it is important to ensure you’re within the “circle of care” and that “you need to know this information to perform your duties to care for the patient” if you’re accessing these records.

Manual Searching Within Cerner: Exercise Caution When Performing a Manual Search for a Patient's Chart

Tip: Always use a patient list, whenever possible, to access the chart. Typically, the patient list is based on a physical location/unit or a "consult relationship" that is established when a patient is referred to your service. This will also ensure you're selecting the correct encounter.



Search parameters

3 Patients returned in this search

Make sure you have the right one; refine your search if necessary.

All the various encounters returned for patient "ZZZCHRISTINE, TFONE"

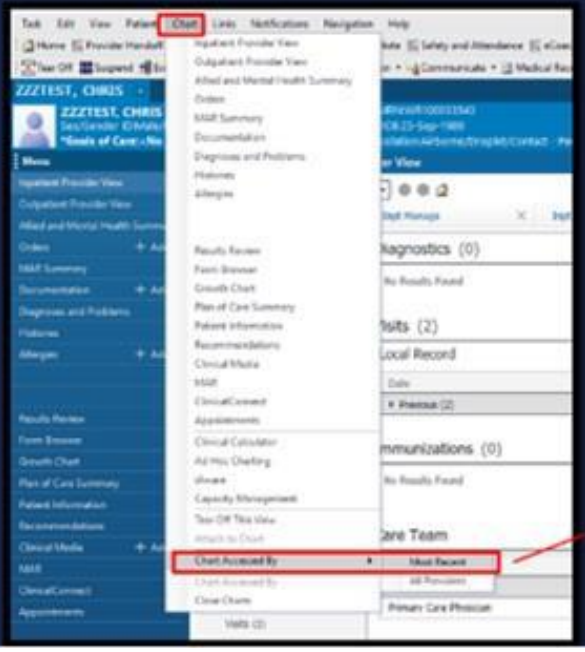
Within the manual search, you can use multiple variables (Name + DOB + MRN, etc.) to perform a look-up. Always attempt to use at least 2 identifiers to ensure you're accessing the correct record. You are responsible as a healthcare professional to ensure you're not accessing incorrect records.

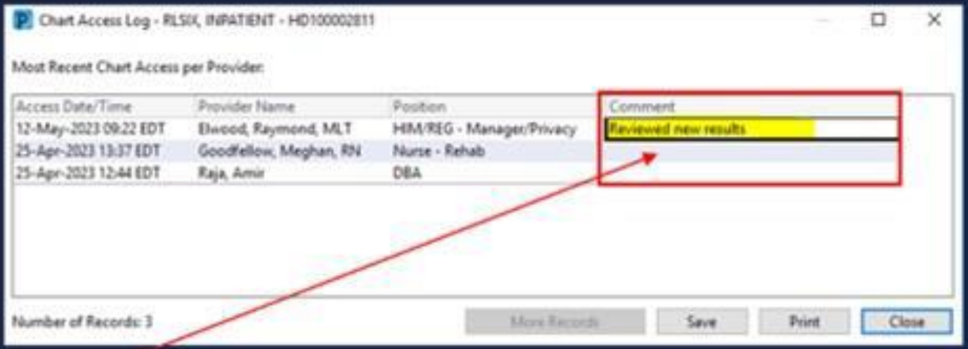
The top window will display the returns of various patients which match from the search, and the bottom will display the above selected patient's various encounter(s) within the regional system. Scrutinize the data presented in the columns before accessing the record to ensure you make the correct selection. Never assume the search has returned the correct chart without verifying the details (i.e., Facility, Location, Encounter, Registration/ Discharge Date, Medical Service, Attending Physician, etc.).

Documenting the Reason for Access within Oracle (Cerner)

In a privacy investigation, you may be asked why you accessed certain charts/records weeks or months after the fact. It would be prudent to ensure you document this reasoning within the chart (especially in circumstances where you access the chart but do not complete any documentation at the time).

When using our regional record, Cerner, when the Chart is open, select "Chart" in the top toolbar > "Chart Accessed By" > "Most Recent", and input a comment into the cell next to your name.





Most Recent Chart Access per Provider:

Access Date/Time	Provider Name	Position	Comment
12-May-2023 09:22 EDT	Elwood, Raymond, MLT	HIM/REG - Manager/Privacy	Reviewed new results
25-Apr-2023 13:37 EDT	Goodfellow, Meghan, RN	Nurse - Rehab	
25-Apr-2023 12:44 EDT	Raja, Amir	DBA	

Number of Records: 3

Proper Use of Email

PHI/sensitive information should not be sent via email internally or externally unless:

- Approved by the privacy office.
- Information is de-identified i.e. MRN or initials when sent internally.
- Encryption is utilized for emails being sent externally.
- Compliant methods to electronically communicate PHI and/or sensitive information e.g. Sync and Medical Teams.
- *Please consult your organization's Chief Privacy Officer for more information.

Freedom of Information (FOI) Requests

FOI requests allow individuals to access records held by public bodies, promoting transparency and the public's right to know. In Canada, the process for making FOI requests varies by province and at the federal level.

FIPPA Overview

What is FIPPA?

FIPPA (Freedom of Information and Protection of Privacy Act) is a law in several Canadian provinces (including Ontario, British Columbia, and Alberta) that governs how public institutions handle requests for access to information and the protection of personal privacy.

Module 2: Privacy

Key Features of FIPPA

1. Access to Information: Individuals have the right to request access to records held by public institutions, with some exceptions (e.g., personal privacy, law enforcement, and public safety).

2. Protection of Personal Information: FIPPA ensures that personal information collected by public bodies is managed properly, including guidelines on how it is collected, used, and disclosed.

3. Response Time: Public institutions are required to respond to FOI requests within a specific time frame (usually 30 days), though extensions may be granted in certain circumstances.

4. Exemptions: There are various exemptions under FIPPA that allow institutions to withhold information, such as information related to personal privacy, law enforcement, or confidential third-party information.

5. Appeal Process: If access to information is denied or if the requester is unsatisfied with the response, they can appeal the decision to an independent oversight body, such as an information and privacy commissioner.

How do you make an FOI request under FIPPA?

1. Identify the Institution: Determine which public body holds the information you seek.

2. Submit a Request: Complete an FOI request form (often available on the institution's website) and provide as much detail as possible about the records you are seeking.

3. Pay Fees: Some institutions may charge a fee for processing FOI requests.

4. Await Response: The institution will review the request and respond within the required timeframe.

Module 3:

Handling Electronic Health Records (EHR)

Module 3: Handling Electronic Health Records (EHR)

What is the purpose of Electronic Health Record (EHR)?

EHRs are digital versions of patients' paper charts, containing detailed health data, which medical histories, diagnoses, treatments, immunization dates, allergies, lab results, and billing information.

What are the benefits of using EHRs?

- A Improved patient care
- B Streamlined healthcare services
- C Easier data sharing amongst healthcare providers.

What challenges do EHRs pose?

- A Vulnerability to cyber threats
- B Complexity of securing digital data
- C Risk of unauthorized access

EHRs Security Risks

Unauthorized Access to EHRs

Unauthorized users, including internal staff, may gain access to sensitive patient data.

Phishing & Social Engineering Attacks

Phishing emails can trick employees into revealing sensitive information or login credentials.

Ransomware & Malware Threats

Malicious software can encrypt patient data and hold it hostage until a ransom is paid, severely disrupting healthcare operations.

Negligence or Malicious Actions

Employees may unintentionally or intentionally compromise EHR security through negligence or malicious actions, such as sharing passwords or accessing unauthorized data.

Module 3: Handling Electronic Health Records (EHR)

Best Practices for EHR Security

Strong Password Policies & Multi-Factor Authentication (MFA):

Employees must use complex passwords and enable multi-factor authentication for accessing sensitive systems.

Access Controls and User Role Management:

Access to EHRs must always be controlled and based on employees' roles and responsibilities and following the minimum necessary standard.

Data Encryption:

Encrypt sensitive health information to protect it from unauthorized access, both while stored on devices and while being transmitted over networks

Secure Data Disposal Methods:

secure methods for disposing of data, such as shredding paper records and securely wiping electronic storage devices.

Examples of EHR Security Breaches

In 2019, LifeLabs, a Canadian laboratory testing company, experienced a major data breach that exposed the health data of millions of Canadians.

In 2018, the University Health Network (UHN) in Ontario faced criticism for a privacy breach involving unauthorized access to patient records by a hospital employee.

Why are these examples important?

These breaches highlight the importance of:

- Access controls
- Employee training
- Robust incident response plans

Module 4:

Password Security & Authentication Best Practices

Module 4: Password Security & Authentication Best Practices

Importance of Password Security

- Passwords are the first line of defense against unauthorized access to sensitive information.
- Weak passwords can lead to data breaches, identity theft and financial loss.

How do I create a strong password?

- Use at least 12-16 characters.
- Combine uppercase letters, lowercase letters, numbers and special characters.
- Avoid passwords that can be easily guessed such as birthdays, names, pets or common words.

Module 4: Password Security & Authentication Best Practices

How should I manage my passwords?

- Use a reputable password manager to store and manage passwords securely.
- Avoid writing down your passwords especially on sticky notes or any paper that is not secured and can be accessed by anyone.
- Change passwords frequently, especially after known security incidents or breaches.
- Do not reuse passwords across multiple accounts; each account should have a unique password.

How should I set up password recovery?

- Set up recovery options that are secure yet accessible; use security questions that are not easily guessed.
- Ensure that recovery methods, such as email addresses or phone numbers, are also secured.

Password Authentication Methods

Single-Factor Authentication (SFA):

Involves one form of verification (e.g., a password). While common, it is less secure.

Two-Factor Authentication (2FA):

Requires two forms of verification, such as a password and a temporary code sent to your phone. This significantly enhances security.

Multi-Factor Authentication (MFA):

Involves two or more verification methods (e.g., password, biometrics, smart card), offering the highest level of security. TransForm uses MFA as the highest level of security.

Module 4: Password Security & Authentication Best Practices

Most Common Threats

Phishing Attacks:

Cybercriminals may use deceptive emails or websites to trick users into revealing their passwords.

Brute Force Attacks:

Attackers may use automated tools to guess passwords by systematically trying all combinations until the correct one is found.

Credential Stuffing:

Attackers exploit reused passwords across different sites, using leaked credentials from one site to gain access to another.

Social Engineering:

Manipulating individuals into disclosing confidential information. For example, an employee receives an email that states that there has been a "security breach" and requires immediate action. The employee is instructed to click on a link to reset their password and is asked to enter their current password along with the new one.

Module 5:

Mobile Device Security for Healthcare Applications

Mobile Device Security

With increasing reliance on mobile devices in healthcare (such as smartphones and tablets) for tasks like accessing EHRs and communicating with patients, the security of these devices has become essential in safeguarding data.

What are the risks associated with mobile devices in healthcare?

- Data Breaches
- Loss or Theft of Devices
- Cyber Threats

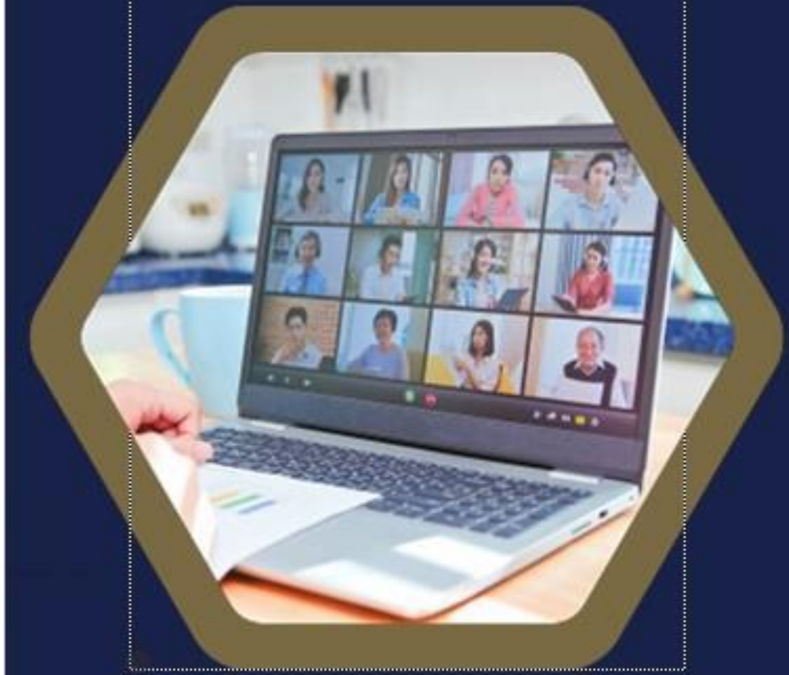
How can mobile device security risks be mitigated?

Mobile Device Management (MDM):
MDM solutions provide centralized management and security for mobile devices within healthcare organizations, enforcing security policies to ensure compliance with standards.

Secure Configuration and Settings/ Defaults:

- Change default passwords and disable unnecessary features that could compromise security.
- Enable screen lock to prevent unauthorized use and automatic lock device when not in use.
- Use strong passwords/PINs and biometric authentication methods (e.g., fingerprint) to secure access to devices.
- Keep up with automatic updates to keep operating systems and applications updated to patch vulnerabilities.

Please refer to your organization's appropriate use of mobile devices for information on what should not be transmitted



Module 6:

Secure Remote Access & Teleworking

What is secure remote access and why is it important?

Secure remote access allows employees to connect to their organization's network from outside the office securely. This is essential for maintaining operational continuity, especially as remote work becomes more prevalent.

What are the benefits of secure remote access?

A **Flexibility:** Employees can work from various locations, which can lead to better work-life balance.

B **Productivity:** Enables continuous access to resources, facilitating uninterrupted work.

C **Cost Savings:** Reduces overhead costs associated with physical office spaces.

What are the risks associated with remote access?

If not properly secured, remote access can expose organizations to risks such as data breaches, unauthorized access and malware infections.

How can these risks be mitigated?

A **Ensuring use of best practices:**

- Implementing Multi-factor Authentication (MFA)
- Promoting user education and awareness
- Utilizing strong passwords

B **Implement processes:**

TransForm has implemented processes to set up and maintain secure access. The processes include monitoring, network traffic, device security controls, and user training.

How is sensitive information best handled in organizations with remote workers?

Data Classification

Classify sensitive data based on its level of sensitivity and the necessary handling procedures.

Secure Communication

Use encrypted communication methods (e.g., secure email) to transmit sensitive information safely.

Incident Response

Establish procedures to manage data breaches or security incidents, ensuring that the appropriate team is contacted promptly.

Regulation Compliance

Follow regulations like PIPEDA and Ontario's PHIPA, which govern the handling of personal health information.

Compliance Measures

Align remote work practices with regulatory requirements to emphasize the importance of maintaining compliance.

What are the key threats to look out for as a remote worker?

Phishing & Social Engineering

Be aware of tactics that manipulate individuals into revealing sensitive information.

Malware Protection

Implement measures to protect against malicious software that can compromise data security.

Safe Browsing

Make use of the browser's security features that keep you protected by showing a warning message before you access an insecure site. Currently supported browsers are Google Chrome and Microsoft Edge.

Module 7:

Incident Reporting

Module 7: Incident Reporting

What is considered a security incident?

A security incident is any event that could compromise the confidentiality, integrity or availability of sensitive information. Security incidents may involve breaches of PHI under PHIPA, or violations of federal regulations like the Personal Information Protection and Electronic Documents Act (PIPEDA).

Why is incident reporting crucial for safeguarding your organization?

Timely incident reporting is essential for reducing damage and enabling effective responses. In healthcare, failure to report security breaches of personal health data can lead to significant penalties under PHIPA or PIPEDA, as well as loss of trust from patients.

What happens if you fail to report an incident?

Failing to report incidents promptly can result in increased damage, regulatory penalties, reputational harm and possible legal actions. In Ontario, healthcare institutions must notify the Ontario Information and Privacy Commissioner (IPC) of PHI breaches that are deemed reportable.

What is the current incident reporting procedure?

Initial Detection

Indicators could include unusual system behavior, unauthorized access to sensitive information or notifications from cybersecurity tools. In Ontario, identifying early signs of data breaches is especially important in healthcare and financial institutions.

Incidents should be immediately reported to:

*The Regional Service Desk by phone **519-464-4400** Ext **7771** or in Hospital Ext **7771***

Breaches require immediate action:

- Avoiding unauthorized data access is essential. Contacting the Regional Service Desk will prompt Security to isolate affected systems to prevent further spread of the breach. Securing patient data is a requirement by law.

- Document everything you observe (date, time, affected systems, users involved).

In accordance with the guidelines set out by PHIPA, organizations are required to report breaches of PHI that meet reportable criteria to the Information and Privacy Commissioner through their designated official, typically the Chief Privacy Officer. Additionally, they must notify the individuals affected by the breach.

Communication protocol during an incident

Internal:

All Staff Members	Authorized Person(s): Designated Communications Professional, Senior Leadership Team Member and/or Chief Privacy Officer
Avoid sharing or communicating any details through unsecured channels such as **Gmail**.	Avoid sharing or communicating any details through unsecured channels such as **Gmail**.
Only utilize approved communications channels such as **Microsoft Teams** to minimize operational disruption and communicate with co-workers and supervisors	Only utilize approved communications channels such as **RAVE** and **EMNS (Emergency Mass Notification System)** to communicate key and emergency messaging to all staff members, and **Microsoft Teams** to continue operations and communicate with co-workers and supervisors.
	Communicate with management, security and privacy team members and partners such as third-party vendors.

Communication protocol during an incident

External:

All Staff Members	Authorized Person(s): Designated Communications Professional, Senior Leadership Team Member and/or Chief Privacy Officer
Do not share any information or engage in any discussion regarding any incident with the media, public, family, friends or acquaintances in person, on social media or through any other communication means.	Ensure that any communications with the media and the public as well as any external messaging on social media or any other platform is managed by the authorized person and approved by the designated senior leadership team and/or legal team.
Forward any inquiries from the public, media or anyone outside of your organization to your communications team.	Ensure that all external communications are compliant with PIPEDA and that impacted individuals are notified in case of data breaches.

**In Ontario's healthcare sector, sharing information regarding PHI breaches must be done securely (not on social media) and in line with PHIPA guidelines.*

Incident Analysis

- The root cause of the incident will be reviewed, including the entry points, compromised systems, and affected data.

Reporting and Documentation

- Detailed incident reports will be completed, ensuring they comply with Canadian regulations such as PIPEDA or Ontario's PHIPA. This report must be saved and available for future audits and regulatory reviews.

Improvement Measures & Quality Assurance

- After analysis, areas will be identified where security protocols can be improved.
- Current measures will be monitored to ensure quality assurance.
- Additional measures will be implemented, whether through technology updates, process changes or employee training to prevent future incidents.

Module 8:

Types of Phishing

Module 8: Types of Phishing

What is Phishing?

Phishing is a form of attack that tricks the victim into giving personal information or downloading harmful software. The attack begins when the attacker sends a message to the victim, using bait to lure them in.

When is a Phishing attempt successful?

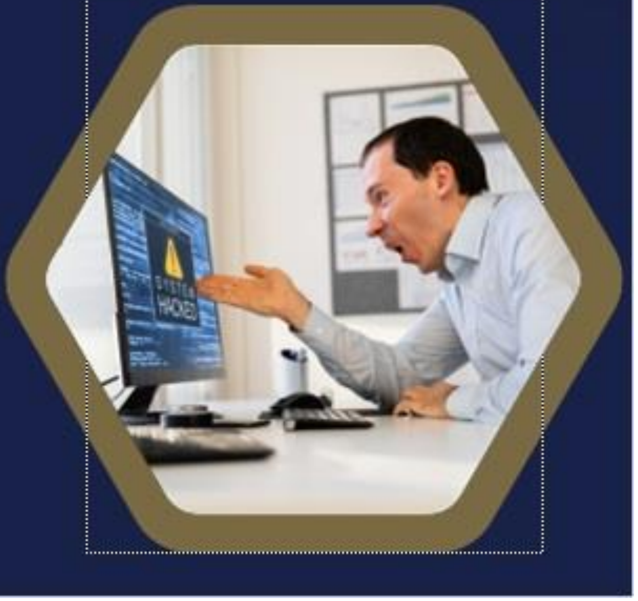
The attack is successful if the victim responds to the request either by clicking a link or opening an attachment, which triggers a threat to the system.

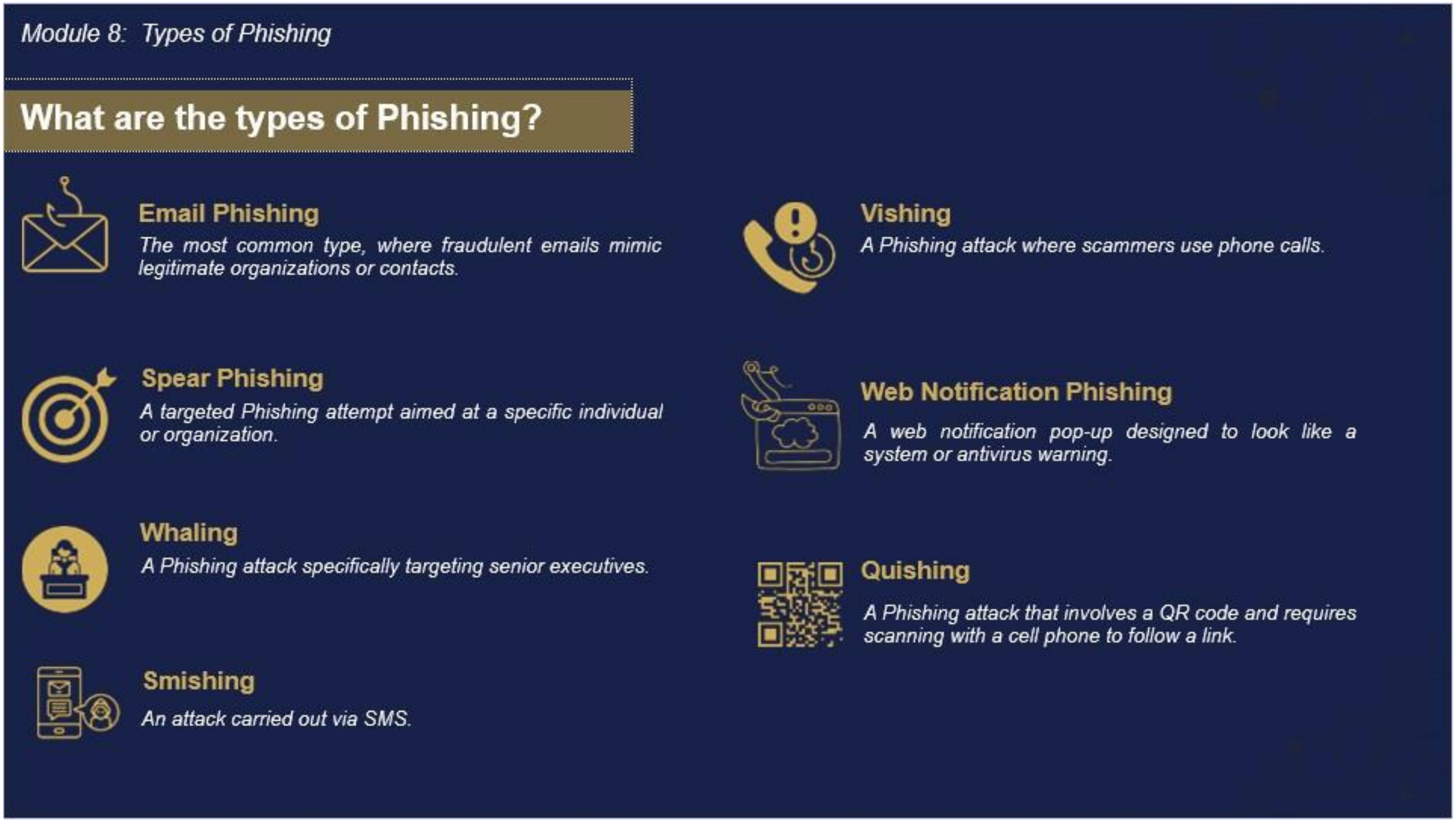
Other scenarios include the victim replying to the attacker's message or staying on the phone to speak with the caller.

What are common examples of Phishing?

Attackers typically rely on social norms and relatable stories to convince the victim to agree to their request. Common examples include:

- Asking the victim to run a quick errand that they can't refuse, where the attacker claims they need help to appease their "horrible" boss.
- Informing the victim about a fake issue with their account and offering assistance.
- Contacting the victim to update their account information for supposed security purposes.





What are the types of Phishing?

Email Phishing

The most common type, where fraudulent emails mimic legitimate organizations or contacts.

Spear Phishing

A targeted Phishing attempt aimed at a specific individual or organization.

Whaling

A Phishing attack specifically targeting senior executives.

Smishing

An attack carried out via SMS.

Vishing

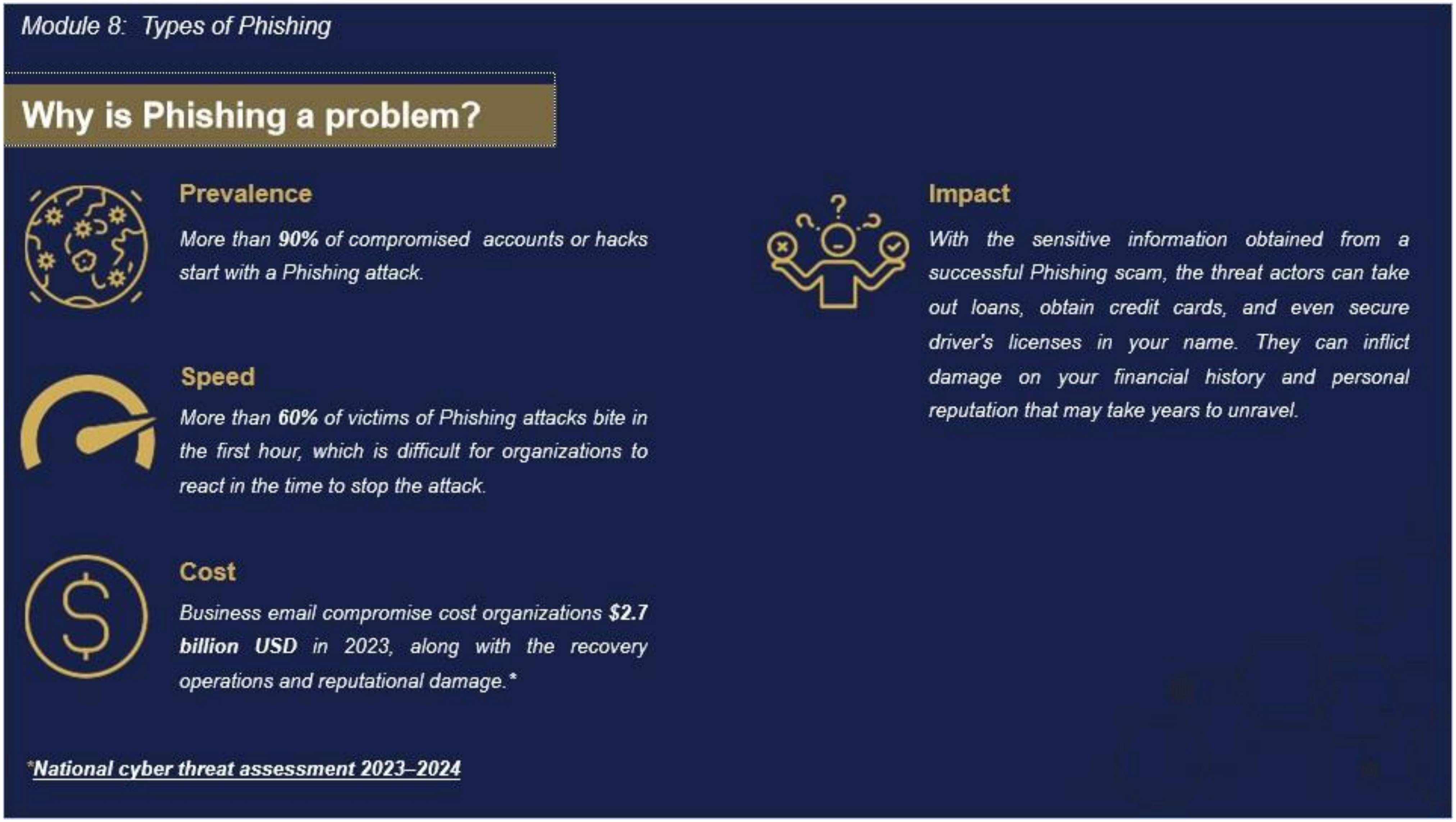
A Phishing attack where scammers use phone calls.

Web Notification Phishing

A web notification pop-up designed to look like a system or antivirus warning.

Quishing

A Phishing attack that involves a QR code and requires scanning with a cell phone to follow a link.



Module 8: Types of Phishing

Why is Phishing a problem?

Prevalence

*More than **90%** of compromised accounts or hacks start with a Phishing attack.*

Speed

*More than **60%** of victims of Phishing attacks bite in the first hour, which is difficult for organizations to react in the time to stop the attack.*

Cost

*Business email compromise cost organizations **$2.7 billion USD** in 2023, along with the recovery operations and reputational damage.**

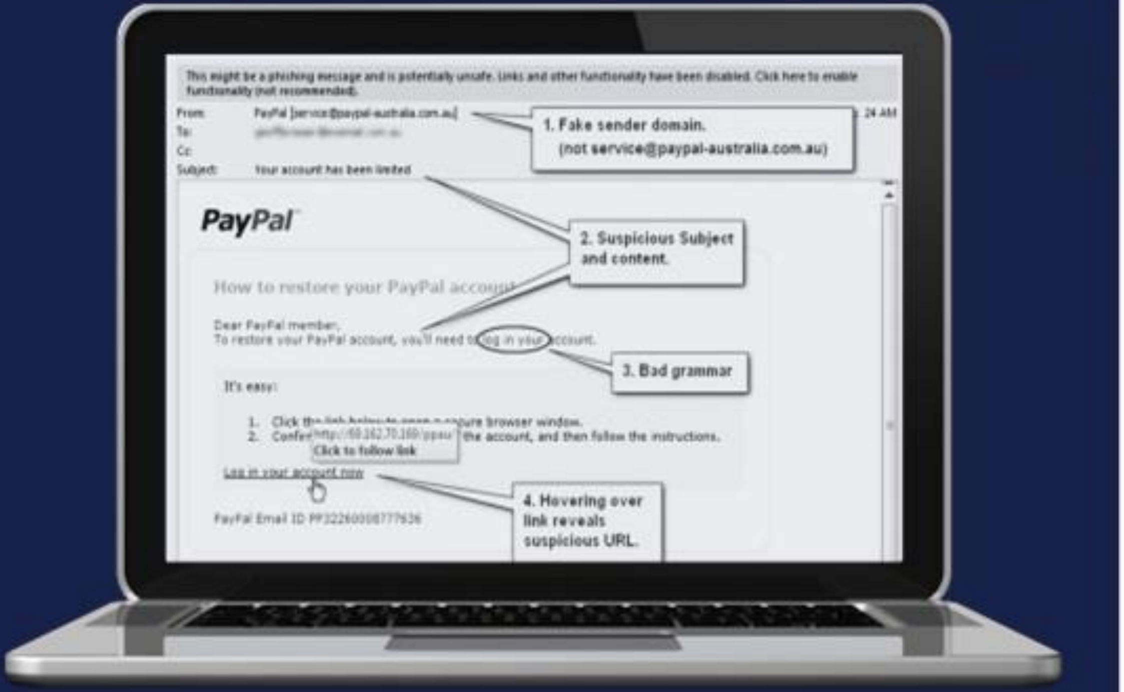
Impact

With the sensitive information obtained from a successful Phishing scam, the threat actors can take out loans, obtain credit cards, and even secure driver's licenses in your name. They can inflict damage on your financial history and personal reputation that may take years to unravel.

*[**National cyber threat assessment 2023–2024**]*

What are common warning signs?

1. You do not recognize the sender.
2. The subject line and email content seem suspicious.
3. The content contains grammatical errors and typos.
4. You are being prompted to click on a link and/or download a file.



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au]

To: [redacted]

Cc:

Subject: Your account has been limited

24 AM

1. Fake sender domain.
(not service@paypal-australia.com.au)

PayPal

How to restore your PayPal account

2. Suspicious Subject and content.

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

3. Bad grammar

It's easy:

1. Click the link below to open a secure browser window.
2. Confi the account, and then follow the instructions.

http://60.162.70.169/ppau/
Click to follow link

Log in your account now

4. Hovering over link reveals suspicious URL.

PayPal Email ID PP3226000877636

Detecting a tech support Phishing scam

A **Tech Support Phishing Scam** involves the attacker pretending to be from a legitimate company or bank and offers to fix a non-existent issue on your computer.

What are the warning signs?

- The contact is unexpected, and you didn't ask for help.
- They create a sense of urgency, prompting you to act now.
- Requests for payment or personal information.

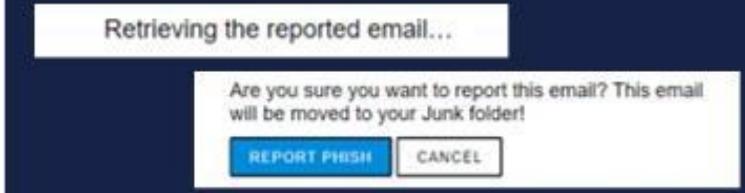
How can you protect yourself?

- Ignore unsolicited calls or pop-ups about tech support.
- Never give remote access to your computer unless you are 100% sure of the source.
- Contact the company directly through official channels if you're unsure.

How do you report a Phishing email?

If you suspect a Phishing email but did not click on a link or download a file:

1. Click on the "Report Suspicious" button. You will be redirected to a web page with the following messages: confirming if you want to report a suspected malicious email.



Retrieving the reported email…

Are you sure you want to report this email? This email will be moved to your Junk folder!

2. If you indeed want to report the email, click the "REPORT PHISH" button.

3.Shortly after, you will receive an email stating: "Thank you for reporting a suspicious email. It has been forwarded to your security team for further review. Your actions are helping to keep your company safe".

4.After an analysis is completed of the suspicious email by the cybersecurity team, you will receive an email message with the results of the investigation. Any email deemed safe is returned to the user's email. The average return time is 24 hours depending on the quantity of emails to be examined.

If you accidentally clicked on a link in a Phishing email or suspect that you clicked on one:

Call the Regional Service Desk (RSD) immediately to inform them. Mistakes can happen but it is crucial to let the team know as soon as this happens to mitigate the risk.

References & Resources

- **PHIPA:** https://www.ontario.ca/laws/statute/04p03-
- **FIPPA:** https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual
- **PIPEDA:** https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
- **National Cyber Threat Assessment:** https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf
- IPC: https://www.ipc.on.ca/en

By completing these learning modules and assessments, you acknowledge that you have read, understand and agree to the terms of our confidentiality agreement and agree to the Cerner system access user agreement

Thank you for completing this training to help protect our systems