Security Awareness Training

- Protect Sensitive Information
- Our Secure Distributed Workforce
  - Report Security Incidents
  - Report Suspicious Emails
- Be a Trinity Health Guardian
Identify Sensitive Information

The security of our Ministry and patients’ sensitive information is directly impacted positively or negatively by each of our actions. Whether you create a new password, click through a stack of unopened emails, or shred a document containing Protected Health Information (PHI), these seemingly minor decisions have a huge impact on information security.

Each of us is responsible for knowing and following the Trinity Health Acceptable Use procedure. By doing so, you help ensure our information and resources remain secure, protect our reputation, and help us avoid costly penalties for violating HIPAA and other regulatory requirements. There has never been a more critical time to stay vigilant and protect your home, personal devices and our network, from cyber-attacks.

Learning Objectives: Understand your role in identifying, protecting, and handling sensitive information including Protected Health Information (PHI). Sharpen your understanding of what security incidents look like and when to report them.
Identify Sensitive Information

UNDERSTAND YOUR ROLE
Information security is often thought of as being solely the responsibility of technology experts. The reality is that no matter your role at Trinity Health, you play a part to protect our confidential information and systems from unauthorized:

- Access
- Use
- Disclosure
- Disruption
- Modification
- Destruction

The Acceptable Use Procedure (available as a download as part of this course) provides guidance to each of us on the proper ways to use Trinity Health devices, systems, and data to protect the confidentiality, integrity, and availability of information.
IDENTIFY SENSITIVE INFORMATION

As a healthcare organization, Trinity Health holds extremely sensitive data within our systems, including personal data of both patients and colleagues. It is important that you understand the data you are handling so you know how to protect it.

We have four levels of data classification, used to identify the sensitivity of the information:

1. **Protected Health Information (PHI) Confidential** information is the most sensitive information held by Trinity Health. It is information related to the health, condition, care, or finances of an individual.

2. **Confidential** information is highly sensitive and includes benefits, financial information, payroll and colleague personnel records.

3. **Internal** information is used to conduct business within Trinity Health. It is proprietary and could have competitive value to others.

4. **Unclassified** information is anything that has been made available for public distribution through authorized Trinity Health channels.

The more sensitive the information, the more we need to do to protect it. Let’s look at some examples in the next exercise.
Safe Handling of Sensitive Information

Safe handling of sensitive information is critical to managing our risk of data loss, which if occurred could lead to lawsuits, loss of reputation or even severe regulatory fines. This means thinking carefully about collecting, accessing, protecting, and retaining the least amount of data necessary.

In this exercise, we will learn ways in which we can protect our colleagues’ and patients’ sensitive information.

Read each scenario and click whether the actions taken by your colleagues are SAFE or RISKY.
I keep paper containing sensitive information neatly stacked on my desk because it’s easier to find when I’m in a hurry. I have a filing cabinet, but I keep forgetting where the key is.
Correct

It is important to keep sensitive information physically secured so those walking by cannot accidentally view it.
I am careful to only share sensitive information with colleagues who have the authority to view the information.
Correct

It is important that only those individuals who have approval to view specific information have access to it. Make sure you don't share sensitive information with those who haven't been approved to see it, whether that information is in electronic or hardcopy form.
When we train our new colleagues, I often record those video conference sessions. Although we are displaying and discussing PHI, it is easier to have that saved recording to educate the next new hire.
Protect Sensitive Information

Correct

Not only is this risky behavior, this could put us at risk of non-compliance with legal or regulatory requirements! Do not record meetings in which PHI is discussed or displayed.
When I know I will need access to certain patient information later, I download it and send it to my personal email address, so I know I’ll be able to easily find it.
Correct

Not only is this risky behavior, this could put us at risk of non-compliance with legal or regulatory requirements! Patient information should never be emailed to your personal address.
Security Incident Vigilance

You can never be "too busy" to sound the alarm. Reporting an incident only takes a few moments, but may be one of the most important things you can do to protect our organization.

Not all incidents are obvious. In fact, many can go overlooked if you make assumptions or work around our processes. Trust your intuition. Play it safe. Report even suspected incidents without delay.

Learning Objectives: Sharpen your understanding of what security incidents look like and when to report them.
## Security Incident Vigilance

### Example Security Incidents

<table>
<thead>
<tr>
<th>SOCIAL ENGINEERING</th>
<th>WORK DEVICES</th>
<th>VISITORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clicking on a link in an email you believe is suspicious</td>
<td>Potential loss or theft of confidential information or a Trinity Health device</td>
<td>Unescorted visitors</td>
</tr>
<tr>
<td>Entering your username and password into a site you believe is suspicious</td>
<td>Observing unusual behavior on your computer or network</td>
<td>Individuals failing to &quot;badge in&quot; to secure doorways</td>
</tr>
<tr>
<td>Providing sensitive information over the phone to an individual whose identity you have not confirmed</td>
<td></td>
<td>Unauthorized individuals accessing sensitive data or systems</td>
</tr>
</tbody>
</table>

**OFFICE**

- You believe your password has been compromised
- Possessing access to systems that contain sensitive information not required to do your job

**PUBLIC**

- You accidentally left your device unattended for a period of time in a public place
- You believe someone saw or overheard PHI confidential data they shouldn’t have
Which of these scenarios should be reported?

Your home is burglarized, and a Trinity device may have been accessed or tampered with. REPORT

You observe your colleague sharing her password with another colleague so he can log into the system to perform his work. REPORT

You accidentally divulge your username and password to a sweet smooth-talking person over the phone. REPORT
Which of these scenarios should be reported?

1. Your home is burglarized, and a Trinity device may have been accessed or tampered with. **Correct**
   - REPORT
   - DON'T REPORT

2. You observe your colleague sharing her password with another colleague so he can log into the system to perform his work. **Correct**
   - REPORT
   - DON'T REPORT

3. You accidentally divulge your username and password to a sweet smooth-talking person over the phone. **Correct**
   - REPORT
   - DON'T REPORT
Which of these scenarios should be reported?

Before leaving work for the day, you take the sensitive documents on your desk and lock them up.

You accidentally click on a link in an email that looks suspicious and entered your username and password to access the webpage.

You find a detailed report of all colleagues’ personal information left on the shared printer.

REPORT  DON’T REPORT  REPORT  DON’T REPORT  REPORT  DON’T REPORT
Which of these scenarios should be reported?

Before leaving work for the day, you take the sensitive documents on your desk and lock them up.

Correct

You accidentally click on a link in an email that looks suspicious and entered your username and password to access the webpage.

Correct

You find a detailed report of all colleagues’ personal information left on the shared printer.

Correct
Phish Warning Signs

Phishing scammers get their way when colleagues like you get fooled. This means that cybercriminals will try anything to get you to click links, fill out forms, or download malicious attachments. That's why you've got to be hyper-vigilant about the clues that tip you off and make you suspicious.

If you encounter any of the warning signs of phishing, you should be on high alert.

---

Scammers are creative. They'll use a variety of tricks to get you to lower your guard and take the bait. Take a close look at the following elements of an email or website to spot a scam:

- The email message has the External Warning Banner
- Sender's email address seems out of place
- Website address seems off
- Use of alarmist or threatening language
- Generic or ambiguous message salutations
- Misspellings or other unprofessional writing
- Requests for personal information
- Message seems too good to be true
- Mysterious hyperlinks
- Unexpected business requests
- Impersonating well-known organizations
- Impersonating your coworkers or managers
Identifying Junk (Spam) and Phishing (Malicious) Messages

Feeling confident? Good, because it's time to put those phish-spotting skills to the test by playing "Find the Phish." You'll review examples of actual email messages sent to Trinity Health colleagues. Look carefully at URLs, ask yourself the right questions, and trust your skeptical instincts to decide which messages are junk (spam) and which are potentially malicious phishing messages.

Decide whether each message is **JUNK (SPAM)** or a **PHISHING (MALICIOUS)** message and click the corresponding "Junk" or "Phishing" button at the bottom of the screen. When you are finished, click NEXT.
From: email-admin@trinity-health.org
To: doctor@trinity-health.org
Subject: [External] RE: IT-Help desk Service

Warning: This email originated from the Internet!

DO NOT CLICK links if the sender is unknown, and NEVER provide your password.

Dear Staff, Employees.

We’re migrating the entire email account of employees and Staff into the Outlook 2019 Office Webmail. As a result, all active employees and Staff must review and sign up for an urgent update and migration to improve the security and efficiency of current spam email.

Please all employees and Staff should Click Here to switch to Outlook Webmail 2019 for employees.

Note that this migration to Outlook 2019 applies to all emails in this service.

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
CORRECT! This is an external phishing message NOT from the TIS Service Desk. It includes a suspicious link and a suspicious sender email address that was designed to make it look like a real Trinity Health email address.
Report Suspicious Emails

Identifying Suspicious Emails

Feeling unsure about an email? Here are some examples of suspicious messages. You can trust your instincts and mark these as junk.

Email Content:

From: exec.office@trinity-health.org
To: doctor@trinity-health.org
Subject: Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Warning: This email originated from the Internet!

**DO NOT CLICK** links if the sender is unknown, and **NEVER** provide your password.

Are you busy? There is something I need you to do. Am going into a meeting now so just reply my mail.

Decide whether this message is [Junk (Spam)] or a [Phishing (Malicious)] message and click the corresponding button.
CORRECT! This is an external phishing message using social engineering techniques. The perpetrator wants you to reply so they can validate your email address is real. Note the suspicious sender email address is designed to make it look like a real Trinity Health email address.

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
Identify and report suspicious emails.

Feeling uncertain about the authenticity of the email? Here are some tips to help you trust your instincts:

- **From:** inventory-reports@trinity-health.com
- **To:** doctor@trinity-health.org
- **Subject:** [External] Inventory Report
- **Attachment:** Document_20080101_0001.PDF
- **Attachment:** Document_20080101_0002.PDF

**Warning:** This email originated from the Internet!

**DO NOT CLICK** links if the sender is unknown, and **NEVER** provide your password.

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and **click the corresponding button.**

[JUNK (SPAM)](#)  [PHISHING (MALICIOUS)](#)
CORRECT! This is an external phishing message. It includes suspicious attachments you weren't expecting. It also has a suspicious sender email address that was designed to make it look like a real Trinity Health email address.

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
Use the Outlook "Report Message" Button

So how do you carry out your responsibility to be our front line of defense? When you identify suspicious emails, report them using the Outlook "Report Message" button.

Simply highlight or open the suspicious message, click the "Report Message" button and select "Phishing" from the drop-down menu (see screenshot below). Note: you can also select "Junk" to report Spam messages. It's just that easy.
Be a Trinity Health Guardian

Front Line of Defense: Learning Objectives

You have completed Trinity Health’s Security Awareness Training. Thank you for everything you do on a daily basis to keep our colleagues and our patients safe. Remember to always stay vigilant and if you see something, say something!

You completed the following learning topics:

- Leadership Introduction
- Your Security Responsibilities
  - Protect Sensitive Information
  - Report Security Incidents
  - Create Strong Passwords
  - Report Suspicious Emails
The Trinity Health Acceptable Use Procedure is provided separately. Please read it and save after training course completion.
Security Awareness Training

✓ Protect Sensitive Information
✓ Our Secure Distributed Workforce
  ✓ Report Security Incidents
  ✓ Report Suspicious Emails
✓ Be a Trinity Health Guardian

Congratulations!
You have successfully completed this course.