



# Security Awareness 2019

## Colleague Security Guide



BE A  
**GUARDIAN**

---

## Introduction

Trinity Health faces a rising number of threats that could compromise the security of our colleagues, patients, information and resources. Threats and incidents may be caused by highly sophisticated attacks, but more often they are caused by our simple inattention to policies and procedures. Either way, each and every one of us has the responsibility, and power to stop most security threats.

This Colleague Security Guide has been established to communicate security standards for Trinity Health colleagues, contractors, and other individuals with access to Trinity Health resources. It supplements, but does not replace, the Code of Conduct and Acceptable Use Policy, Confidentiality Agreement, and other compliance, privacy, and security policies and procedures. Your attention to these policies and procedures is critical to protecting our colleagues, patients, and data against security breaches. Security Awareness training is assigned to all colleagues on an annual basis to educate you on your responsibilities. All colleagues are required to complete this course each year.

## Information is Everywhere

Your responsibility to protect Trinity Health information continues to grow as technology continues to evolve. It is no longer just your desktop, laptop or paper that you need to secure. You must secure any medium that stores or has access to Trinity Health information including:

- **Computers:** Servers, desktops, laptops and public computers
- **Mobile Devices:** Smartphones, tablets and readers
- **Storage Devices:** Databases, Backup tapes, CDs, USB flash drives and Cloud storage sites
- **Medical Devices:** Insulin pumps, pacemakers, EKGs, infusion pumps, blood pressure machines, pulse oximeter machines, X-ray machines, imaging machines and defibrillators.



All colleagues should protect equipment against security risks using both physical and technical controls.

## Everyone has a Role

LINES OF DEFENSE
<b>End Users</b> are our first line of defense! They are responsible for following policies and procedures when accessing, disclosing, sending, storing and deleting information.
<b>Managers</b> are responsible for ensuring colleagues understand their responsibilities to protect our data.
<b>EIS and TIS</b> set security requirements, policies and procedures.
<b>Trinity Health Executive Leadership</b> provides strategic direction and priority to securing critical colleague and patient data.

Even though you may not work in Information Technology, you have a role in protecting Trinity Health! You may have the ability to access, disclose, send, store and delete information. Because of this, all users must comply with Trinity Health's [Acceptable Use Procedure](#) when using Trinity Health resources.

(<https://intranet.trinity-health.org/web/enterprise-information-security/information-security-procedures>)

Security roles and responsibilities are defined in accordance with the [Information Protection Policy](#).

(same link as above)

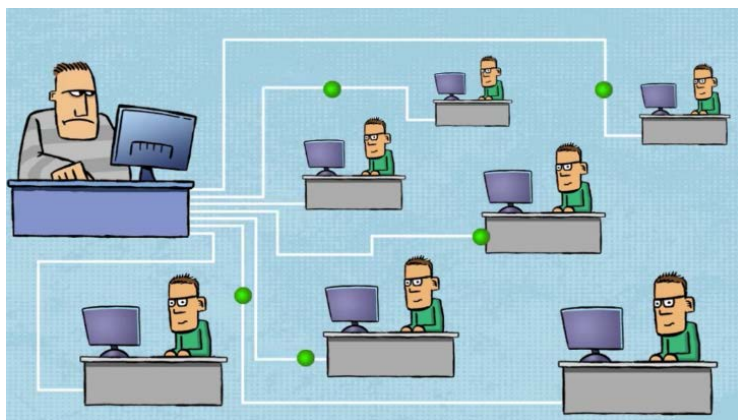
## Threats to Our Information

There are many individuals and groups with malicious intent that pose a threat to Trinity Health's information. Everyone including colleagues, contractors, business partners, affiliated physicians, students and others who access Trinity Health information systems have a major role in protecting data.

Threats can come from numerous sources, including hostile governments, terrorist groups, malicious intruders or disgruntled colleagues.

Users who are either unaware or not careful with the information they possess are an additional threat source you may not typically consider. While they may not have malicious intent, their human error could compromise Trinity Health information.

## Phishing



Phishing emails are malicious emails sent to lure recipients into doing something they shouldn't (e.g., click a link, open an attachment, etc.).

Some phishing emails direct users to a website that automatically downloads malware (malicious software) onto their device. Other phishing emails may request you to enter sensitive information such as your username and password into a phony website.

Phishers then sell or use this information to commit identity theft, to get access to the device or to commit

other crimes. Phishing emails can contain authentic looking logos or graphics and appear to be genuine.

**Spear Phishing** – Spear phishing is a more sophisticated phishing attempt that targets a specific person using personalized information to make the email appear legitimate. While top executives and those that support them are often prime targets for these attacks, spear phishing may target anyone.

**Phone Phishing / SMiShing** – Phishing is not all email based. Phone phishing is when a caller impersonates a legitimate company to take advantage of your trust to steal money and personal information. Cell phones and mobile devices may also be targeted for SMiShing, which is a text based version of phishing.

**Ransomware** – A type of malware that is often distributed via phishing attacks. It is an attack designed to access your computer systems and hold your files hostage. Attackers typically demand a financial payment (ransom) before they safely return your files or remove the ransomware.

*Phishing is the most successful method attackers use to gain access to confidential data.*

### Other Threats

**Shoulder Surfing** – Shoulder surfing is when a malicious individual watches what you type, especially your username and password, while in a public area such as a coffee shop, airport or library. Stay vigilant in public areas and be sure no one is watching you. If you suspect that someone has obtained your password, change it and contact the Integrity and Compliance line at 866-477-4661.

**Dictionary Attacks** – Attackers rely on the fact that general users do not utilize strong passwords. Attackers may run a password cracker using a "dictionary attack," which attempts to crack a password by leveraging words found in the dictionary. Once one password is cracked, savvy attackers may be able to compromise additional systems/passwords.

## Protecting Your Email

Hackers are counting on you being busy and rushing to get through your email and not thinking about what you are seeing. Be alert, slow down and pay attention for signs that something is not right with a message. When using email, remember:

- Users with a Trinity Health email address should not use personal or third party email accounts to conduct Trinity Health business.
- Never email a patient without express permission from your direct supervisor and properly securing the message.
- Do not send emails to multiple patients at one time. Certain colleagues responsible for sending emails to multiple patients must have express approval to do so, ensure to blind copy the recipients, secure the message, and do not include any confidential data in the message. .
- Share only the minimum amount of information needed and only with the individual(s) who need to access the information.
- Only include the minimum necessary information for any communications. Remove identifying information, such as name, and sensitive information such as social security numbers, whenever possible.
- When replying or forwarding look for and delete attachments or message content that includes PHI, confidential, or internal information when no longer needed. If saved, store attachments in a secure location.
- Never send, forward or store material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or unlawful.
- If you need access to work email on your personal device, you are required to install Trinity Health-approved security software on your mobile device. To obtain the software, you can initiate an Access Request through [Service Now](#).

4

## Identifying Suspicious Email

Opening suspicious email attachments exposes not only your computer, but the entire Trinity Health network to serious security risks. Hackers design many threats to move from machine to machine, or even design them to leave "open doors" throughout a network so they may come and go as they please in the future.

Never open unknown files that end with the suffix .exe, .vbs, .bat, or .reg. While not a complete list, these extensions are the ones you are most likely to see, and they all take action behind the scenes if you click them.

*Email attachments are the leading source of computer infections and compromises.*

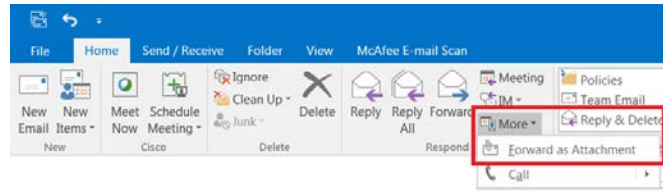
Here are a few tips:

- The text "[External]" appears in the subject line of any email originating from outside of Trinity Health. An external header also appears in the body of the email. These are explicit signs the email originated from outside Trinity Health and you should exercise additional vigilance.
- Never click on any links or open attachments if an email appears suspicious, especially if you do not know the sender.
- Never provide information such as your username, password, social security number, credit card information or other sensitive information.

Subject: [External] RE:

**Warning:** This email originated from the Internet!  
**DO NOT CLICK** links if the sender is unknown, and **NEVER** provide your password.

- **Forward as an attachment** all suspicious email to [Spam@trinity-health.org](mailto:Spam@trinity-health.org) then delete the message.
- If you think you clicked on something suspicious, don't panic! Call the TIS Service Desk at 1.888.667-3003 immediately for assistance.



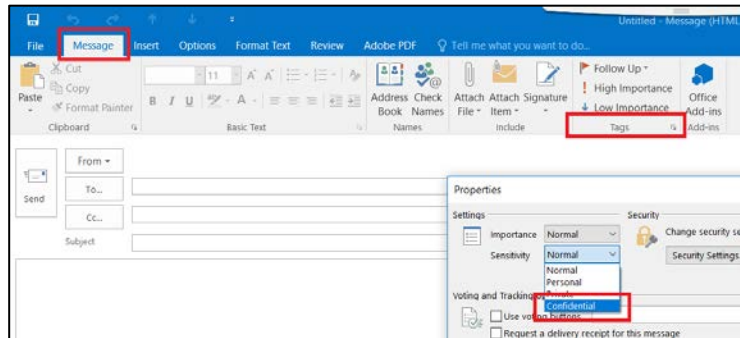
## Securing/Encrypting Confidential Email

Email that stays within the Trinity Health network is secured and protected.

**You must secure and encrypt email you send to non-Trinity Health email addresses if it contains confidential information and/or PHI.**

We monitor outgoing email to ensure it complies with the email standards. You can easily secure outgoing email with these two simple steps:

1. **Include the word 'Secure' in the subject line to encrypt it.** You can also use (secure) or <secure>. Ensure you do not merge the word 'secure' with any word that precedes or follows it, such as "SecureImportant message," which would not trigger the encryption.
2. **Change message to "Confidential" before sending.** From the **Message** menu, select **Tags** and update the **Security** to Confidential. The recipient will receive an email notice that they have been sent a secure message with instructions to open it.



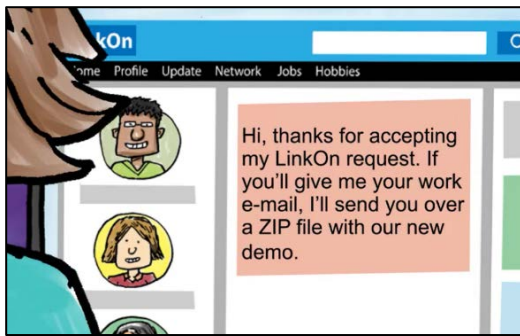
## Social Engineering

In today's workplace, you use your computer all the time—in the office, at home, even on the road and when you travel. It's not enough to know how to use your computer; now more than ever you also need to be aware of threats like Social Engineering.

People who engage in Social Engineering use deception and will readily lie to try to get you to help them. They may attempt to gain access to buildings or try to elicit passwords or other sensitive information from you. Social Engineering may occur on the telephone as a request for information, In person as a request for access, via e-mails as a request for information, or a number of other ways.



## Social Media (Facebook, LinkedIn, Instagram, Snapchat, Twitter, YouTube, etc.)



The use of the internet and social media sites have become common forms of professional and personal communication. Although the internet provides unlimited access to data, not all of that information is safe, correct or appropriate material.

Trinity Health monitors these sites and reasonably restricts access or delivery of inappropriate or unsafe material. However, we need your help. In the event you encounter inappropriate material on the internet, you are required to disconnect from the site promptly and notify your supervisor immediately.

As social media activities can affect Trinity Health and patient privacy, usage must be consistent with Trinity Health's Code of Conduct: and [Social Media Use Policy](#).

<http://content.che.org/sysoff/policy/SharedDocs/Communications/Communications 1 - Social Media Use.pdf>

- Do not post any information about patients including, but not limited to: photos, films, diagnostic imaging, treatment, diagnosis or prognosis, positive or negative comments. Any discussion related to a patient's condition (even without using the patient's name) could result in a HIPAA violation.
- Never initiate or accept a patient friend request unless an in-person friendship predates the treatment relationship.
- Excessive social networking during work hours is subject to disciplinary action.
- Do not create external websites or Facebook pages with your work team that Trinity Health has not sanctioned and approved.
- If you see any violations of Trinity Health social media standards, notify your supervisor or call the Trinity Health Integrity and Compliance Line at 866-477-4661.

6

## Approved Tools

Trinity Health provides a number of approved tools for sharing and storing information and for team collaboration.

Approved tools have been configured and tested to meet Trinity Health's information security standards.

If a valid business requirement exists for a tool not included on the approved list, a request should be made to the local TechOps Team. Depending on the business case and type of data accessed by the tool, additional assessments and approvals be required.

It is understood that when working with vendors or third parties who are leading a collaboration, you may need to use their tool of choice, which may not be among Trinity Health's approved tools. Such situations do not allow for the presentation or recording of Trinity Health PHI or confidential data.

INSTEAD OF THIS		USE THIS	
<b>FILE STORAGE</b> amazon S3, iCloud, Google Drive	→	pulse FILES, Trinity Health share drives	
<b>SHARING LARGE FILES EXTERNALLY</b> HIGHTAIL, Dropbox, box	→	ShareFile	
<b>EMAIL</b> YAHOO!, M	→	Outlook	
<b>MEETINGS AND COLLABORATION</b> skype, Flowdock	→	Cisco webex, pulse LINK, pulse FILES, CISCO JABBER	

\* When available in your RHM, you may use Trinity O365 services.

### Auto-Fill

Most browsers can automatically insert information that you regularly enter into web forms such as name and address. Trinity Health recommends you disable this feature and never check the "Remember Me" checkbox to prevent your username and password from being stored online.

### Need to connect to a work computer or resource from a remote location?

Trinity Health users are required to use approved secure and reliable methods using strong authentication and encryption to access sensitive Trinity Health information from a remote location.

VPN and approved cloud solutions (i.e., Office 365) are acceptable methods to connect and access information remotely. Contact your supervisor or the Trinity Health Service Desk 888-667-3003 for remote access options.

### Need to transfer large files securely?

You can create an account to use Trinity Health's Secure File Transfer tool to send large files in a secure manner to recipients both inside and outside of the organization. To begin, visit this URL: <https://transfer.trinity-health.org>. Follow the link labeled "Getting Started" to learn more about this tool.

*TIP: Because we don't typically stop throughout our day to classify data, follow this standard. "Unless it is public, consider it private."*

### Need to conduct secure clinical text messaging?

Doc Halo is an approved secure text messaging tool for physicians and clinicians to communicate PHI data in compliance with HIPAA privacy and security rules. **Clinical data may not be texted by any other means than an approved Trinity Health application.** For more information, visit the SharePoint page directly at <http://intranet.trinity-health.org/web/audio-video-web-conferencing/doc-halo>.

### Backups of Trinity Health Data

Colleagues are responsible for storing all data and other work related files on network drives, which are backed up on a regular basis. TIS managed devices that are connected to the network have a home drive, which is a personal network drive sitting on the network's file share. Files saved to locations such as My Documents are backed up on the network when the device is connected to the network. Note that not all local drives, folders and subfolders are mirrored to your home drive.

## Data Security

To adequately protect our information, Trinity Health has established four levels of data classification, which determine the sensitivity of the information and its related security requirements.

### 1. Protected Health Information

Protected health information (PHI) is information related to the physical or mental health or condition of an individual, their care, or payment/credit card information. This is the most sensitive information Trinity Health maintains and our patients entrust all of us to keep it safe and secure. In order to use, disclose, access, transmit or store, users of this data should only have minimum necessary access in order to perform their job duties. Federal laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) aim to protect the security and privacy of PHI. Compliance with HIPAA and other privacy laws is an important component of Trinity Health's Mission, Core Values and Code of Conduct.

Basic safeguards to secure PHI are critical to the sacred work we do. These simple precautions, some of which are found elsewhere in this document, are being highlighted here as critical in order to protect our patient's privacy and comply with regulations:

- Secure your devices (computers, phones, storage devices, etc.) and don't share passwords.
- Lock your computer screen when you leave a workstation and physically secure papers containing PHI.
- Do not discuss PHI in public areas such as restrooms, cafeterias, hallways, restaurants or cafes.
- Only access and disclose PHI if it is necessary to do your job.
- When sending PHI, double check the content you're sending to ensure it includes only the minimum information necessary and double check the phone/fax number, email and/or address.
- Do not post information about patients to social media.

All colleagues are accountable for the protection of PHI. If you become aware of an incident in which PHI was mishandled, inappropriately accessed, or disclosed, you are responsible for immediately reporting it to your local Privacy Officer. (Contact information at the end of this manual.)

Certain colleagues' roles require them to share PHI with other healthcare providers as part of a 'permitted disclosure' to care for the patient. In these specific situations, ensure the following;

- Verify the content you're providing to ensure it includes only the minimum information necessary.
- Verify the correct patient information, fax number, email and/or address before sending
- Use encrypted channels to send information
- Do not use shared credentials (including when using third party portals)
- Create strong passwords to protect sensitive information

(You can obtain more information on protections and proper handling of PHI from your local Privacy Officer. Contact information at the end of this manual.)

## **2. Confidential Information**

Confidential information is highly sensitive and includes benefits, financial information (including credit card information), payroll and personnel records. You should only access and disclose this information on a minimum-necessary basis when performing your job duties with minimum necessary access.

## **3. Internal Information**

The intended use of internal information is to conduct business within Trinity Health. Internal information is proprietary in nature and could have competitive value to others.

## **4. Unclassified Information**

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



## Credit Card Security

In addition to health information, we also need to protect our patients' confidential credit card information. The Payment Card Industry Data Security Standard (PCI DSS) is a standard that organizations like ours must follow when accepting credit card payments from patients and customers. It is a security standard created by the credit card brands (VISA, MasterCard, American Express, Discover) to protect consumer's information.

Trends indicate that more health care consumers are paying medical charges using credit cards and most of the health care organizations accepting those payments are capturing cardholder data using web services on their local PCs, which makes them vulnerable to hackers.

As Trinity Health sees an increase of credit card data under its protection, the security threats we face continue to evolve. This information found both electronically and in hardcopy form must be protected using the security strategies outlined within this document. Every colleague's attention to detail and adherence to Trinity Health security policies and procedures is our greatest strength to secure cardholder data and meet our PCI DSS compliance requirements.

## Different Types of Information Require Different Types of Security

The health care industry has moved to electronic records and that makes it much easier to access and disclose sensitive data - and lots of it! Think about the sensitivity of the information that describes you personally. Consider the potentially negative impact on you if someone gained access to your email address, social security number, the name of your employer or your credit card number.



Add to this the risks when working remotely of your home or outside Wi-fi network being infiltrated by data thieves. That's why you should always establish a secure connection or use a virtual private network (VPN) connection to make good use of all the protections of our approved network.

9

## Long Passwords are Strong Passwords

Parameters are in place to ensure your network passwords meet certain characteristics, like a minimum length and complexity, because weak passwords are a major security vulnerability. However, it is difficult to enforce the use of strong passwords for every application because colleagues and contractors are responsible for creating and safeguarding their own passwords.

Here are a few tips to follow when creating new passwords:

- The longer your password, the stronger it is. A fifteen character password is harder to guess or crack than an eight character password.
- Avoid keeping a unsecured record of passwords. If you must write down a reminder, then write down a hint rather than the password itself.
- Change passwords at any indication of possible compromise.
- Never use the same password for business and non-business purposes.
- **Never share your credentials (username and password) with anyone, not even Trinity Health Support Services.**
- If possible, use passphrases. Passphrases are tougher to crack and many users find them easier to remember than ordinary passwords.
  - The quick brown fox jumped could be 7heQwik8rownFoxxJu^pd
- Mix uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) or other characters (@, %, #, ?) to create obfuscated passwords. Examples of obfuscated passphrases:
  - I am a Taylor Swift Fanatic! could be 1\_m@7ayl0r5wift\_F4n4tic!!!

## Physical Security

Physical security refers to the protection of personnel, resources, and facilities from loss or damage from events such as theft, vandalism, fires, and natural disasters. Everyone at Trinity Health is responsible for applying physical security practices and procedures.

Be aware that your access to certain areas within Trinity Health facilities may be restricted or may have limitations. This is both for your protection and for the protection of the organization on a larger scale.



- Keep entrances and exits secure. Don't let unauthorized people follow you through a door, "tailgating" their way in. Follow Trinity Health's policies regarding access to facilities.
- Keep sensitive information locked up. Whether it is stored on paper, electronic media like thumb drives or CDs, laptops, or your network-connected PC, when not in use, keep sensitive files locked up in a secure space.
- Ensure visitors sign in and wear a visitor's badge.
- Watch out for suspicious and unknown people in the work area. Stay vigilant—if you see people loitering, report them to security.
- Keep your desk clean.
- Quickly retrieve sensitive information from printers, copiers, and FAX machines.
- Wipe whiteboards clean after meetings.

### Lost or Stolen Devices

Lost or stolen electronic devices are among the top threats to protecting Trinity Health's data. You are responsible for ensuring your mobile devices (laptops, tablets, USB drives, and even your personal smartphone, if used to connect to work in any way) remain in your personal control. Most mobile devices are lost or stolen while traveling, but it can happen anywhere.

Lost and stolen devices present a large risk to Trinity Health and our ministries when they can access PHI or payment card information. Lost or stolen PHI carries significant risk to the organization and may be a breach of federal and state law.

#### Don't:

- Leave devices in unlocked vehicles, even when you'll be gone "for a second."
- Leave your devices in a vehicle overnight.
- Leave unattended devices in plain sight anywhere.

#### Do:

- Keep the **TIS Service Desk** number, **888-667-3003**, in your wallet, to immediately report a lost or stolen device.
- In an emergency situation, you come first. If your safety is at risk, or emergency personnel direct you, take care of yourself before the device.
- Make sure others cannot see your screen when in a public place.
- Limit the information you save to your mobile devices and delete it when you no longer need it.
- Always save critical or confidential information on a network drive. If you save your data locally, it may be lost if you lose your device.
- Keep an inventory of the Trinity Health applications on your mobile devices.
- Protect your devices with strong passwords or PINs.
- Always double check that you have not left your devices behind.

Many users do not consider the possibility of compromises, damage and theft of information that can occur when they leave their systems unattended. Walking away from an unlocked computer gives an unauthorized person an opportunity to view or modify confidential information you have access to. It also provides them with the ability to install malicious software without your knowledge.



**Using Windows?**  
The key combination to lock a PC is Windows + "L"

**Using a Mac?**  
The key combination to lock a Mac is Ctrl + Shift + Eject



*When you leave your workstation, please be sure to log out or lock your system*

## Outside of the Office

Most mobile devices and laptops are lost or stolen while commuting or traveling. You are responsible for ensuring that your devices remain in your personal control while in transit. Recommendations include:

- Keep the device in sight. If the device is out of your sight, hide it from others seeing it too.
- Do not leave devices with others.
- Do not leave devices alone to charge.
- Double check your seat when leaving a taxi or airplane.
- When using your device in public, do not allow others to view sensitive information.
- Always lock your vehicle and keep devices out of sight.

## Removable Media and Storage Devices

Removable media and storage devices include external hard drives, USB drives, memory cards, CDs or DVDs. While these devices are very convenient, they tend to be small and easily lost. **Do not store PHI on removable media and storage devices.**

It is also important to understand that these devices can bring malware and viruses into Trinity Health's computing environment. Before you plug a device into the network, scan it to ensure that security risks are not introduced.

## Know Your Regional Security Official (RSO)

We have designated a Regional Security Official (RSO) for every Regional Health Ministry (RHM) and Eligible Provider (EP) to provide security support. The RSO provides day-to-day guidance on government security regulations as well as the local information security program to ensure the organization's information is properly protected.

**Do not attempt to remediate any security incident independently.** Call your designated RSO if you have any questions or concerns. Please visit this URL for specific RSO contact information: <https://intranet.trinity-health.org/web/enterprise-information-security/contact-us>

Your local contact information may vary as some RHMs may not yet be fully integrated with Trinity Health's Policies and Procedures.

## Know Your Privacy Officer

Each ministry has a local Privacy Officer who is responsible for compliance with HIPAA and other privacy regulations. Contact your Privacy Officer immediately if you believe PHI has been inappropriately accessed, disclosed, or used; if a patient has a privacy related complaint; if you suspect a privacy regulation or policy is not being followed; or if you simply have a privacy related question. Please visit this URL for specific Privacy contact information: <https://intranet.trinity-health.org/web/privacy-compliance/privacy-official-directory>

Print this page, and post the top part at your place of work for quick reference. Cut out the handy wallet card at the bottom, fold it in half and you'll have important contact information in your wallet in case you need it.

## Contacts for Security Concerns/Questions

It is the responsibility of all colleagues and users to report concerns and ask questions when they arise.


Every user should know that their actions may be monitored, and your consent to this is built into your use of any Trinity Health system. Prior to using any Trinity Health system, you agreed to follow Trinity Health's Acceptable Use Agreement, and you reconfirm this every year as a part of annual Security Awareness Training.

[Acceptable Use Procedure](http://tis.che.org/eis/EIS%20Published%20Procedures/IS%20-%20User%201%20Acceptable%20Use.pdf) - <http://tis.che.org/eis/EIS Published Procedures/IS - User 1 Acceptable Use.pdf>

<b>TIS Service Desk</b>	<b>888-667-3003</b>
<ul style="list-style-type: none"> <li>Your electronic device is lost or stolen.</li> <li>If the device or applications on the device contain PHI, also contact your Privacy Officer. <a href="https://intranet.trinity-health.org/web/privacy-compliance/privacy-official-directory">https://intranet.trinity-health.org/web/privacy-compliance/privacy-official-directory</a></li> <li>You discover password changes that you did not initiate.</li> <li>You believe someone has obtained and/or used your password or account(s).</li> <li>You suspect a virus on your workstation.</li> <li>You clicked on a suspicious link in an email and/or opened a suspicious attachment</li> <li>You have hardware or software issues.</li> </ul>	

<b>Phishing/Spam Mailbox</b>	<b><a href="mailto:spam@trinity-health.org">spam@trinity-health.org</a></b>
When you receive a suspicious email, forward the email as an attachment to mailbox above.	

<b>Integrity and Compliance Hotline</b>	<b>866-477-4661</b> or <a href="http://www.mycompliancereport.com">www.mycompliancereport.com</a> (access code THO)
<ul style="list-style-type: none"> <li>You receive harassing or inappropriate email.</li> <li>You discover unsecured content or inappropriate material on any Trinity Health device.</li> <li>You become aware of the unauthorized use of a Trinity Health device, application or information.</li> <li>You know of a violation of our Information Security or Privacy policies.</li> <li>You feel uncomfortable or unsure about calling the TIS Service Desk</li> </ul>	

<p><b>TIS Pocket Reference</b></p>  <p>Hardware, software or data issues? Something lost or stolen? Username or password compromised? <b>Call the TIS Service Desk at 888-667-3003</b> Forward suspicious email <u>as an attachment</u> to <b><a href="mailto:spam@trinity-health.org">spam@trinity-health.org</a></b>.</p>	<p>PHI affected? Privacy or Security Policy violation? Harassing or inappropriate email or content? Unauthorized use of systems?</p> <p><b>Call the Trinity Health Integrity and Compliance Line at 866-477-4661 or go to <a href="http://www.mycompliancereport.com">www.mycompliancereport.com</a> (access code THO)</b></p>
--	--