BECAUSE OF YOU

MOUNT CARMEL

Provider Handbook for Information Security and Privacy

Trinity Health
Livonia, MI

INTRODUCTION

Mount Carmel is committed to being a transforming, healing presence within the communities we serve. Inspired by our Mission, Mount Carmel achieves excellence in all we do through devotion to our Core Values. To serve this Mission, we rely heavily on extremely sensitive information resources. Mount Carmel is a trusted steward of patient, Provider and other mission-critical information. Because we are committed to our Core Values and protecting these vital resources, Mount Carmel provides an Information Security and Privacy Awareness Program to help us live our values of Reverence, Commitment to Those Who Are Poor, Justice, Stewardship and Integrity.

Controls are set up to provide a defense against cyberattacks, to provide timely but minimum necessary access to patient information, to identify a security event as quickly as possible, and to minimize the impact of an event by timely restoration of services.

The User Handbook for Information Security and Privacy provides an overview of proper information security ethics and etiquette. It does not replace your responsibility to read and understand the Information Security and Privacy policies and procedures, and the Trinity Health Code of Conduct.

To be successful, we need to be partners in security and work diligently together.

Sincerely,

Tom Enneking
Regional Information Security Officer

Christie Santa-Emma
Privacy Officer

ACCEPTABLE USE POLICY

Mount Carmel's information resources must be used for authorized purposes only in support of the Mission. Mount Carmel users must refrain from engaging in illegal or otherwise inappropriate activities that may result in harm to the organization's information systems and computing resources. Use of information resources for personal activities should not interfere with productivity, preempt any business/clinical activity, or reflect other forms of inappropriate use. Mount Carmel reserves the right to access, monitor, or disclose, as it deems necessary, the contents and history of each user's email messages and network activity for any purpose.

This document establishes security standards for Mount Carmel. It is a supplement, not a replacement, to the Code of Conduct, policies, tools and other resources developed for Trinity Health. It recognizes and incorporates, to the extent applicable, the policies already established in support of Mount Carmel, including the Acceptable Use Policy.

PERSONAL RESPONSIBILITY

Mount Carmel Providers are responsible for the security of Mount Carmel information and information systems. Providers will notify their management and the Trinity Health Service Desk 614-234-8700 or Physician Information Services (PIS) 614-234-8999 if they suspect that security may have been compromised in any way. Security incidents can also be directly reported to the Regional Information Security Officer or Privacy Officer. Security and Privacy reports will be handled with confidentiality as may be afforded or required to the matter and individuals reporting incidents will be protected from retaliation. Security incidents include, but are not limited to: a computer virus, spyware, a breach of security, discovery of inappropriate material on a computer system, loss or disclosure of data, unauthorized use, or violation of any security policy. Additionally, Mount Carmel users will not attempt to remediate any security incident independently.

WHAT ARE INFORMATION SYSTEMS?

Information Systems refers to all computing resources, such as:

- **Computers:** Servers, desktops, laptops, tablets and public computers in airports, coffee shops, bookstores, libraries or a relative's house.
- **Mobile Communications:** Smartphones and tablets.
- **Storage Devices:** Backup tapes, CDs, USB thumb drives and flash drives.

INFORMATION CLASSIFICATION

Mount Carmel has four major levels of data classification: Unclassified, Internal, Confidential and Protected Health Information **(**PHI) Confidential. Information classification refers to the sensitivity of the information and identifies information that is required for the continuation of normal operations or for compliance with the law. Assignment of data classifications is the responsibility of the data originator for internally generated data or the first Mount Carmel recipient of legally acquired information.

- **Unclassified information** is information that has been made available for public distribution through authorized Mount Carmel channels. Unclassified information is not proprietary in context or content.
- **Internal information** is when the intended use of the information is to conduct business and is proprietary in nature. Mount Carmel internal information, if released or disclosed, could have competitive value to others and/or could adversely impact Mount Carmel in other ways; but the likelihood of serious harm is low
- **Confidential information** is of the highest sensitivity. Access is restricted to users on a need to know and/or minimum necessary basis when performing their job duties. Mount Carmel Confidential is information that, if released or disclosed, could have competitive value to others and/or would adversely affect Mount Carmel in other ways and is not to be communicated outside Mount Carmel.
- **PHI confidential** means information that: (i) is created or received by a health care provider, health plan, or health care clearinghouse; (ii) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and (iii) identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the individual).

HIPAA

Health Information Portability and Accountability Act (HIPAA) Security and Privacy Standards Regarding Patient Health Information

- Privacy standards provide more control over how personal health information is used and disclosed to ensure that individually identifiable health care information remains confidential and secure.
- Security standards are intended to ensure the integrity, confidentiality and appropriate availability of all electronic protected health information (ePHI) using administrative, physical and technical safeguards.
- All entities covered under HIPAA must comply with the Privacy and Security Regulations.

It is important to note that Trinity Health and ministry networks are interconnected. As responsible stewards, we should be diligent and implement basic security practices as strong as those required under HIPAA.

USER ACCESS – SECURITY & PRIVACY IMPERATIVES

For security purposes, Providers and office staff shall not connect to the Mount Carmel network by any means other than those specifically defined by the Mount Carmel Information Security procedures. Furthermore, each Provider and office staff is responsible for the ethical utilization and the security of Mount Carmel information and systems.

To support these security measures and to maintain compliance with regulations such as HIPAA Security and Privacy Rules, Mount Carmel requires each Provider and office staff to have a unique login account consisting of an ID and password on information systems, including the network, individual applications and email.

Mount Carmel has created processes and procedures to manage authorized access to information resources and areas where resources are stored. The information systems, access rights and user accounts are issued at the level necessary to effectively perform job functions and are the property of Mount Carmel.

To maintain privacy, Providers and office staff must not record, monitor or intercept the communications or activity of anyone through the use of any electronic, mechanical or other recording devices except for official business use. In addition, Providers and office staff consent to allowing authorized Mount Carmel management and the Trinity Enterprise Information Security department to access and monitor information systems.

BRING YOUR OWN DEVICE

Providers who have access to Mount Carmel email on a smartphone or other personally owned device are required to install security software on the mobile device. This software will provide security of sensitive information in the event the device is lost or stolen. This software provides Mount Carmel the ability to secure, and wipe our corporate and patient data without affecting the personal aspects of a user's chosen device. This software client will secure that data, and keep it "in the bubble" of our security controls.

WHEN TRAVELING

Most mobile devices and laptops are at a higher risk for theft while traveling. It is recommended that personnel devices remain in their control while traveling. Recommendations include: Maintain physical contact with the device

- Do not check devices with hotel porters or airline handlers.
- Do not leave any device in plain sight, even in a locked vehicle.
- Do not leave any device alone to charge.
- Ensure that when using your device in a public area, you do not allow others to view sensitive information.

The famous words we often hear are, "I only laid it down for a second." If your device is lost or stolen, report it promptly to the Trinity Health Service Desk 614-234-8700 or Physician Information Services (PIS) 614-234-8999 for immediate support and intervention.

PASSWORDS – MAKE 'EM STRONG!

Mount Carmel systems require you to have a strong password. Weak passwords are the single largest computer security threat because they are often not selected with security in mind, but more with the intent to easily remember them. Unfortunately, this also makes them a security weakness. Weak passwords tend to be easily guessed, too short or based on information that is easily known about a person (date of birth, children and pet names, sports teams, etc.). These passwords are often in the most basic toolkit the hackers use to crack passwords – a dictionary file. This file contains every word in the dictionary and tests thousands of possible passwords in mere seconds.

As more personal and professional resources on the Internet become available, we are acquiring more and more account names, each requiring a password. For ease of use, many users attempt to choose the same account name and password so that having one account password cracked may lead to all their accounts being cracked – or guessed. Guessing passwords is just that – guessing – so don't make it easy. The most easily guessed passwords are usually one of these three options:

- Your user name — ID=joesmith and Password = joesmith
- The word "Password" — ID=joesmith and Password = password
- The application name — ID=joesmith and Password = Lawson

Remember – Providers and office staff are responsible for all transactions made using their IDs and for safeguarding their passwords. No Provider or office staff may access a Mount Carmel computing resource using another user's account.

What Makes a Password Strong?

- **Length.** The longer, the better. When permitted, choose a password that is at least 8 characters long. Some operating systems permit users to choose passphrases, which are essentially very long passwords that can include spaces and punctuation. Passphrases are tougher to crack and many users find them easier to remember than ordinary passwords. Use a passphrase that is a sentence or the first letter of each word in a sentence such as:
    - I am a Taylor Swift Fanatic! = IAATSF!
    - A Person's A Person, No Matter How Small! = APAP,NMHS!

- **More complex.** A complex password will include at least three of the following: UPPERCASE LETTERS (A-Z), lowercase letters (a-z), numeric digits (0-9) and special characters (@,%,#,?).
- **No easily guessed or slang words.** Do not use words found in the Webster's dictionary - these can be found in many "cracker dictionaries" used by hackers. They include words from songs, television shows, movies, video games and other "pop culture" references. They also will test for common substitutions (e.g., "u" for "you", "4" for "A", "gr8" for "great").
- **Consecutive strokes.** Do not use keyboard keys such as "asdfg" or "qwerty."

Once you have chosen a strong password, keep it to yourself. Do not share it with anyone. The Trinity Information Services support staff will never ask you for your password.

New User Passwords – Change Them Immediately!

Change the new user password immediately. If you don't change the passwords for these new user accounts, they will be easy targets for unauthorized persons to gain access to your information.

CYBER THREATS

The Department of Homeland Security describes cyber threats as "unauthorized attempts to access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders." Some of the most common cyber threats are listed below:

Shoulder Surfing & Social Engineering

Shoulder Surfers are people who watch what you type, especially when you are logging on with your user name and password while in a public area. Social Engineers gather nuggets of confidential information from you perhaps posing as a Help Desk employee who asks for your password in order to fix a problem. Never grant access to a computer (yours or anyone else's), unless you are satisfied that it is for legitimate purposes.
If you suspect that a Shoulder Surfer or Social Engineer has obtained your password, change it immediately and contact Trinity Health Service Desk 614-234-8700 or Physician Information Services (PIS) 614-234-8999.

Phishing

Phishing is fraud that uses an email and a masquerading website to get victims to unsuspectingly enter personal information (passwords, Social Security numbers, birth dates, bank account numbers, financial data, etc.) into a website. The phishers will then sell or use this information to commit identity theft and various other crimes. You need to be skeptical of any "phishing" emails designed to trick you into clicking on a link or opening/downloading an attachment to capture your personal information. In this situation, some of these emails may look like they're coming from a business you trust. The message will contain authentic logo graphics (copied from the company's legitimate website) and will appear to be genuine. The text will vary, but usually will refer to some problem with your account or ask that you verify your account information and instruct you to click on a link provided.

Never open or respond to any suspicious messages or if you don't recognize the sender (be sure to determine the email address of the sender before opening).

- DO NOT click on any links in email.
- DO NOT open or download any attachments that arrive with email.
- DO NOT reply to the email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open, if you have clicked on a link in email.

All Providers are asked to delete phishing messages from Mount Carmel email immediately and, if unsure, to contact Trinity Health Service Desk 614-234-8700 or Physician Information Services (PIS) 614-234-8999 for assistance. Providers are additionally cautioned to notify authorities if they become aware of any unusual credit, loan or bank activities taking place without their knowledge, permission or engagement.

Identity Theft Protection

Be vigilant. Do not give out personal information on the phone, through the mail or on the Internet unless you've initiated the contact or are sure you know with whom you're dealing. Identity thieves have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers and other identifying information. Identity thieves also rummage through dumpsters to find discarded personal items like bank and credit card statements that have not been properly shredded.

Businesses and institutions should never solicit you via email for confidential information. If you receive such an email and believe it to be legitimate, contact the company directly to confirm the solicitation.

Malware

One consequence of opening an attachment is that an attacker could not only install Malware (malicious software), but could also use your machine to attack and infect other computers on the network.

Here are some common types of malware:

- **Viruses -** programs that produce destructive results; distributed as attachments in emails.
- **Worms -** replicating programs that spread to other computers.
- **Trojans -** programs that hide within another program.
- **Backdoors -** programs that allow remote access to an infected computer.
- **Spyware -** software that tracks keystrokes, mouse movements, clicks and websites visited. Usually distributed in "free" software such as search engine plugins, non-standard screensavers, toolbars and file sharing applications.

MOUNT CARMEL EMAIL STANDARDS

The Mount Carmel email and computer network services are to be utilized for business needs to support our Mission. Users of the Mount Carmel email and computer network services are responsible for protecting the data that is accessed, stored or transmitted.

When using email, remember:

- Unless expressly authorized by Mount Carmel senior management or included in Providers' normal responsibilities, sending or transmitting confidential information such as protected health information, as defined by HIPAA, is strictly prohibited.
- Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or unlawful may not be sent electronically or store system resource.
- Providers and office staff are reminded that communications of business information through the use of Internet mail, chat rooms, instant messenger or other "peer-to-peer" applications are prohibited.
- Providers and office staff may not alter the "From" line or other attribution-of-origin information in email, messages or postings.
- Providers and office staff shall not forward Mount Carmel email containing confidential information to personal email accounts.
- Emails are deleted after 180 days.

Did you know that email attachments are the leading source of computer infections and compromises?

Opening suspicious email attachments exposes your computer to serious security risks. It could allow a hacker to not only install malicious software, but also to attack and infect other computers on the network. Never open or send file attachments including files that end with the suffix .exe, .vbs, .bat, .reg. Data may be lost or compromised.

Secure/Encrypted Email

Email that stays within the Mount Carmel email network is secured and protected. Email that is delivered to non-Mount Carmel email addresses must be secured/encrypted if it contains confidential information and/or protected health information (PHI). Outgoing email is monitored to ensure compliance with the

email standards. Outgoing email can easily be secured:

- Create, address and compose internet bound (outside Trinity email)
- Click on Send Options tab
- Click on Classification drop down list
- Select Confidential
- Select Send

SOCIAL MEDIA

Using the Internet has become a normal part of everyday life. Internet access and social networking from Mount Carmel information systems is a privilege and must be consistent with Trinity Health Code of Conduct. Social networking is a common form of professional and personal communication.

Examples of social media include: Facebook, LinkedIn, Instagram, Snapchat, Twitter, YouTube, etc. Be aware that your social media activities may impact Mount Carmel and Patient Privacy. Internet access and social networking from Mount Carmel information systems is a privilege and must be consistent with the Trinity Health Code of Conduct.

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.

INTERNET USAGE

The Internet is a worldwide network of computers that contains millions of pages of information, some of which may contain offensive or inappropriate material. Mount Carmel has implemented Internet monitoring software to reasonably restrict access or delivery of this type of material; however, absolute protection from such material may not be possible. In the event Providers encounter inappropriate material on the Internet, Providers are required to disconnect from the site promptly and notify their supervisor. Mount Carmel is not responsible for content viewed on the Internet while using company information systems.

Auto-Fill

Most browsers have a feature that will remember and automatically insert information that you regularly enter into web forms such as name and address. This also means that information such as user names and passwords can also be easily remembered, which is not a good idea. We recommend you disable this feature and never check the “Remember Me” button to prevent others from taking advantage of your credentials.

PHYSICAL SECURITY

The importance of physical security cannot be overstated. Providers and office staff are responsible for taking all reasonable measures to physically secure all Mount Carmel information systems, including locking up your laptop, computer discs and flash/thumb drives when you are away – even momentarily. If a device can store or access confidential data, it is considered an information system and should be physically secured at all times. Only non-critical or non-sensitive data may be stored on a removable media (flash/thumb drive/computer disk/CD).

Unattended Computers

Many users do not consider the possibility of compromises, damage and theft of information that can occur when a system is left unattended. Walking away from an unlocked computer gives an unauthorized person the opportunity to enter illegitimate transactions into the billing application you are logged into or allows them to install a keystroke logger without your knowledge. **When you leave your workstation for lunch or breaks,** please be sure to **log out or lock the system** by simultaneously depressing the **<ctrl><alt><del>** keys.

Dispose of unnecessary documentation that contains confidential information or sensitive data in the specified work area secured bins so it may be properly destroyed.

SECURITY INCIDENTS & REPORTING

The Enterprise Information Security department investigates all reports of security incidents. A security incident is an activity involving a computer resource that is not in keeping with our Core Values or violates our Acceptable Use Policy. Providers are responsible for reporting all suspected information security incidents to the Trinity Health Service Desk 614-234-8700 or PIS 614-234-8999.

What are Examples of Incidents?

Some security incidents may require review and analysis by an expert to confirm. You may not be able to determine if specific activity is a security incident, but any abnormal event should be reported.

- Harassing or inappropriate email.
- Using another Provider's account, sharing a password or password changes that you did not initiate.
- Discovering inappropriate material on any Mount Carmel information system resource.
- Loss or disclosure of confidential data (lost or stolen laptops or thumb drives).
- Unauthorized use of Mount Carmel computing resources or violation of any security policy.

APPLYING INFORMATION SECURITY AND PRIVACY POLICIES

Scenario 1: Using electronic health record (EHR) access privileges to view a relative's medical record

Situation: Sally is an RN in a physician office. The physicians admit patients to a Trinity Health hospital and Sally has been granted access to Trinity Health's electronic health record (EHR) system. Her mother was admitted into a Trinity Health hospital, but is not a patient of the physicians for whom Sally works. Is it permissible for Sally to use her access rights to view her mother's electronic medical records?

Response: No. By accessing this information, Sally will violate the Federal Health Insurance Portability and Accountability Act (HIPAA) regulations, Trinity Health policy and her mother's privacy. Sally does not need this information to do her job and would be accessing the information for personal reasons. Such actions may result in disciplinary action by her employer and termination of Sally's EHR access privileges by Trinity Health.

Scenario 2: Disclosing information to others inappropriately

Situation: Joan works in a cardiology practice. The physicians in the practice admit patients to a Trinity Health hospital. Joan schedules a hospital admission for a friend, Nell, who attends the same church as Joan. At church the following Sunday, several members ask Joan if she knows anything about Nell's condition. How should Joan respond?

Response: Joan must not disclose any information about Nell obtained as a result of her work in the cardiology practice, not even with Joan's family or friends. Joan should politely inform the concerned church members that federal laws prohibit the sharing of confidential information about patients without their expressed permission.

- Never access a patient's chart unless current clinical or business relationship exists
- Never access a person's medical record out of curiosity or personal concern.
- Only disclose the minimum necessary.

General Reminders:

- Ask visitors to leave the room prior to discussing medical care.
- Use low voice in shared space when discussing sensitive medical situations.
- Limit access to information to only those persons with a need to know.
- If traveling with patient information is a requirement, then it must be in your control at all times.
- Never share your password for any reason/nor ask others to share theirs.
- Double check each page of a document for patients name PRIOR to providing written information to a patient or family member at discharge.

For additional information please contact:

Tom Enneking
Regional Information Security Officer
O: 614-546-3668
tenneking@mchs.com

Christie Santa-Emma
Mount Carmel Health System Privacy Officer
O: 614-546-3284
csanta-emma@mchs.com

Revision: 6/17/2019