SCENARIOS: Applying Trinity Health's 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
Sharing unique IDs and passwords

Situation: Alice is an employee of a vendor that provides services to a Trinity Health hospital. She comes to the hospital accompanied by a colleague, Mark. Mark's access privileges to Trinity Health's network and applications have not yet been activated. Can Alice let Mark use her ID and password until he is assigned his own?

Response: No. Sharing unique IDs and passwords is a violation of Trinity Health policy and may result in termination of Alice's access privileges to the Trinity Health network and applications. Mark must wait until Trinity Health completes his access request and he has signed a Trinity Health Confidentiality & Network Access Agreement.

Scenario 3
Secure disposal of confidential information

Situation: Matt works for a collection agency that contracts with a Trinity Health. Matt has been provided access to Trinity Health's patient accounting systems in connection with his job. Matt frequently prints documents containing patient information for his work. When no longer needed, Matt discards the documents in the regular trash. Is this a permissible practice?

Response: No. All patient and business confidential information must be discarded in a secure manner, either in a locked bin or a receptacle designated for confidential information. Confidential materials must be destroyed by shredding, burning or another method that prevents others from accessing the information. Matt 's actions may result in disciplinary action by his employer, removal of his access privileges by Trinity Health, and possibly termination of Trinity Health's business relationship with Matt's employer.

Scenario 4
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.

Scenario 5
Accessing a celebrity's electronic health records

Situation: Tom is a health tech for a hemodialysis company. Tom has been granted access to the Trinity Health's EHR for patient care reasons. The football coach of a large state university was recently admitted to a Trinity Health hospital. The coach is not receiving treatment from Tom or Tom's company. His only reason for accessing the coach's medical records is curiosity or concern for the coach. Is it permissible for Tom to use his EHR access to look at the coach's records?

Response: No. Tom will violate federal HIPAA regulations, Trinity Health's policy and the coach's privacy. Tom is not caring for the coach and would be accessing the information for personal reasons. Such actions would result in disciplinary action by Tom's employer, removal of his access privileges by Trinity Health, and possibly termination of Trinity Health's business relationship with Tom's employer.

Scenario 6
Accessing your own medical information

Situation: John works for a rehab company with offices on-site in a Trinity Hospital. John has been granted access to Trinity Health's EHR for patient care reasons. John is also a patient of the hospital and recently had lab tests performed there. John is eager to know the results of the lab tests and is considering using his EHR access privileges to review his medical records. Is this permitted?

Response: No. Trinity Health policy prohibits individuals from using their EHR access privileges to review their own information. Access privileges may only be used for patient care or other business purposes.

Trinity Health
Livonia, MI

Privacy Official – Monica C. Lareau
(734) 343-0037

Security Official (Mid-West) –
Richard Runion (734-343-1535)

Security Official (East) – Marty Devine
(610) 335-2175

Information Privacy and Security: Your Responsibilities

A Quick Reference Guide
For Individuals Given Access to Trinity Health's Confidential Information & Information Systems

RESPECT PRIVACY

Stewarding the Health Information Entrusted to Us

The Purpose of This Brochure

You have been provided access to Trinity Health's confidential information and information systems. This brochure summarizes your responsibilities to protect the privacy and security of all confidential information and of Trinity Health's information systems.

If you have questions after reviewing this brochure, you may contact your supervisor the HIPAA Compliance Office of Trinity Health at 734-343-1407, or the Integrity & Compliance Line at 1-866-477-4661.

IMPORTANT INFORMATION

- Your access to Trinity Health information and information systems is monitored for compliance with Trinity Health's security and privacy policies.
- Trinity Health reserves the right to deny or disable your access to Trinity Health's information or information systems in the event of inappropriate access, use or disclosure of Trinity Health's confidential information or information systems. Such actions may also result in termination of Trinity Health's relationship with your employer.

RESPECT PRIVACY

Stewarding the Health Information Entrusted to Us

Your Responsibilities

Thank You for Your Support

Trinity Health is committed to building trusting relationships with patients, colleagues, physicians and communities. Key to maintaining that trust is protecting and respecting the privacy and confidentiality of all patient and business information and ensuring the integrity of our information systems. We rely on all who are permitted access to our information and systems to do their very best to help us achieve this goal. You play a vital role in our success!

General Requirements

- Read, sign and abide by Trinity Health's Confidentiality and Network Access Agreement.
- Comply with Trinity Health's security and privacy policies and procedures as summarized herein.
- Understand that the appropriate use and protection of Trinity Health's confidential information applies to information in all forms - electronic, paper and oral.
- Immediately report privacy or security issues or concerns to your supervisor or a Trinity Health Privacy or Information Security Officer.
- Immediately report the loss or theft of any mobile device/media or paper files containing Trinity Health information to your supervisor or your Trinity Health Privacy or Information Security Officer.
- You may also report issues and concerns to Integrity & Compliance Line at 1-866-477-4661.

Protection of Trinity Health Information and Information Systems

- Actively protect the Trinity Health network and information on your workstation, in your work area, and on mobile devices and other media.
- Login only with your unique Trinity Health user ID and password
- Sign-off or log-out of your workstation when you leave or walk away.
- Protect your confidential password and never share or disclose it to others.
- Report any observed password sharing to your supervisor or your Trinity Health Privacy or Information Security Officer.
- Protect the privacy of your computer when viewing Trinity Health information.
- Appropriately dispose of Trinity Health confidential information (e.g., shred, delete, etc.) when no longer needed.
- Lock file cabinets and office doors where confidential information is stored.
- Protect Trinity Health information when transporting it off-site.
- Turn-off mobile devices when transporting.
- Make sure mobile devices/media and paper files are always protected in a locked and secure location.
- Never leave mobile devices/media and paper files in open and unsecured places – especially public locations.
- Be wary of unsolicited email messages and avoid clicking links or attachments until you are certain they are from legitimate sources and safe to use. If you are uncertain, contact your local Information Security Officer.

Appropriate Use of Trinity Health's Information and Information Systems

- Access and use Trinity Health's information systems only as needed to do your job.
- Access, use or disclose Trinity Health's patient and other confidential information only for legitimate business purposes, and never for personal or other reasons.
- Access only the minimum necessary amount of confidential information that you need in order to perform your job.
- Do not use Trinity Health's information systems to transmit information that is abusive, offensive, disparaging or in violation of the law.
- Do not access Trinity Health's information systems or access, use or disclose confidential information after your association with your employer or Trinity Health ends.
- Do not attempt to download, copy or install software residing on Trinity Health's network onto any other computer.
- Do not make any changes to Trinity Health systems without Trinity Health's prior written approval.