HIPAA Security Training Manual

The final HIPAA Security Rule for Montrose Memorial Hospital went into effect in February 2005.

The Security Rule includes 3 categories of compliance; Administrative Safeguards, Physical Safeguards, and Technical Safeguards. These safeguards are designed to protect EPHI (Electronic Protected Health Information). The storage, access and transmission of this information is the focus of the Security Rule. To meet these requirements, we must:

1. Ensure that electronic information is available when needed, but only to authorized individuals, and that the information cannot be altered, corrupted, or deleted accidentally.
2. Anticipate and protect against threats including unauthorized access, and malicious software (a virus is an example) that would put this information at risk.

To accomplish this, we must all become *Security aware*. Each of us has increased responsibilities and accountabilities in the access and use of electronic information.

HIPAA imposes sanctions against violations. These sanctions may be applied against the organization or, in some cases, the individual employee. These sanctions are treated as criminal violations with criminal penalties:

- Misuse of PHI (Protected Health Information); fines up to $50,000 and/or jail time up to 1 year
- Misuse of PHI under false pretenses-fines up to $100,000 and jail time up to 5 years
- Misuse of PHI with the intent to sell, transfer or use the PHI for personal gain, commercial advantage or malicious harm; fines up to $250,000 and jail time up to 10 years.

The hospital has adopted policies that take our compliance with HIPAA seriously. Individuals who fail to comply with these HIPAA requirements, and hospital policies and procedures may be subject to disciplinary action, including the revocation of access to EPHI and in some cases, termination. Violations stemming from false pretense or willful disregard of policies or intent to do harm may result in legal action. If you have any questions regarding the use or access of electronic patient information you should talk with your supervisor, Department Director, or the HIPAA Security Officer.

All employees are required to receive security awareness training and periodic security reminders. This training manual is your awareness training, and periodic security reminders will be conveyed via your Director, email, and the annual training.

What you should know:

1. **Passwords:**

   a. Login accounts and passwords are assigned individually to access different software applications like Meditech, individual email accounts and computers.
   b. Your account and password are unique to you and cannot be shared with anyone. To share your password with someone else, or even for them to ask to use your account is a HIPAA violation and will be subject to disciplinary action.
   c. Your password should not be written down, but if you must, keep it in a secure place. You cannot have your password posted where it may be accessible to others.
   d. Passwords in Meditech need to be changed every 90 days. Different applications have different requirements. When you change your password you must use at least 6 alpha numeric characters, it cannot be the same as your login account, first or last name and it should be non-predictable.

2. **Virus:**

   a. It is the responsibility of all of us to ensure the computing technology is safe from malicious threats. These take many forms including viruses and spy ware.
   b. All computers have anti-virus software installed on them. No attempt to change the settings on this software, or stop this software from running is permitted.
   c. Only authorized software may be installed on individual computers. You should not install any software without first receiving approval from Information Services. There are software copyright laws in effect that make it illegal to install most software on more than one computer at a time unless it is properly licensed.
   d. You must not download and install any software from the Internet. This includes screen savers, background shots, games and ‘freeware’ programs.

3. **Email:**

   a. There is only 1 type of email software supported by the hospital. You may not install other types of email software on your computer. Personal Web based email accounts such as Yahoo, Hotmail and others may be used from hospital computers provided that your Department Director and Information Services has approved this.
   b. Generally, we will not use email to send patient information outside the hospital. Exceptions are handled on an individual basis and require the use of encryption solutions.
   c. You may not download email add-in programs, nor link to email applications or services including the popular ‘emotion icons’.

4. **Physical Security:**

   a. Restricting physical access to electronic PHI is an easy way to protect our information. Here are a few guidelines to help you:

- Make sure your monitor does not have line of sight viewing by unauthorized individuals. Privacy Screens are available through Materials Management.

- If the computer is in a secure area with locking doors, make sure that if you are the last person to leave that area, the door is locked when you leave.

- When you print data make sure you retrieve it from the printer in a timely fashion and you keep the paper out of easy viewing from those unauthorized to see this data.

- Portable devices like Laptops, tablets, and PDA's (Smart phones, Personal Digital Assistant, i.e., palm pilots) are particularly vulnerable because they are so portable. When these devices are not in use, make sure they are stored in a secure area.

- You may not use computers, laptops, notebooks or tablets on the hospital network until these devices have been staged and configured by Information Services. Generally, this means you can NOT bring a computer or laptop from outside the organization and plug it into the hospital's network.

5. **Internet Access:**

   a. Access to the internet is restricted and monitored. Information Services has implemented Internet monitoring tools that will record all Internet sites visited and control access to inappropriate content.

   b. Internet access is a resource to help you with your job responsibilities. You may not use the internet to play games, access sexually explicit content, or other personal use that is not specifically authorized by your Department Director. You may not download screen savers, background shots, programs and other content unless specifically authorized in advance by the HIPAA Security Officer.

   c. If there is a web site that is being blocked that you need to access, please contact the help desk at ext 2639. The site will be put up for review for approval or denial by Information Services. Your Supervisor will also be notified that you have made this request.

   d. Most computers will have the Montrose Hospital Intranet page set as the default home page. Our Intranet is a rich source of hospital specific information that applies to all employees. You may not change the home page or the internet browser on any computer.

6. **Network Resources**
    a. Resources on the hospital network are defined as software applications, files, intranet content, access to printers and other hardware, and backup devices.

    b. Network resources are to be work related only and available to the workforce in the performance of their job. These resources are for authorized use only. If your computer does not have access to these resources do NOT attempt to access them yourself. You should have your Department Director authorize the request to have access to those resources to Information Services.

    c. You should not browse the network to look for available files or applications. It is a violation to intentionally randomly browse our network and attempt to connect to resources you are not authorized to access.

    d. You should not make applications on your computer available for access on the network. All files must be saved to your personal H: drive, departmental S: drive, or My Documents folder.

7. **Workstation alterations**
    a. All workstation computers will be configured to adhere to HIPAA Security procedures. You are not to modify or circumvent any software settings on your computer.

    b. Personal use of hospital computers are at the discretion of your Department Director. If granted, you may not add additional software to the computer, or use floppy disks, USB memory devices or CD's to access personal software.

8. **Web development**
    a. A web committee is in place and is responsible for approving all content that resides on the intranet and internet pages for Montrose Memorial Hospital. You may not directly add to this content nor attempt to delete or modify the content therein unless you have been given the authority to do so.

    b. All web content will reside on servers in Information Services. You may not host web content from your local computer.

Procedures:

A. You must acknowledge this training material by signing Attachment A attached.

B. All users of computer resources in the hospital must establish a need to have access to those resources. The attached form 2 must be filled out and signed by the employee's Department Director requesting access to those resources.

C. You should report all violations, or suspected violations to your Department Director and the HIPAA Security Officer.

Contacts: HIPAA SECURITY OFFICER: Information Services Director
COMPLIANCE OFFICER

Acknowledgement of HIPAA Awareness Training

1. I understand that Montrose Memorial Hospital has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information.

2. I am aware that, as part of Montrose Memorial Hospital's responsibilities described above, Montrose Memorial Hospital provides privacy and security training to its workforce members.

3. I acknowledge that I have received HIPAA awareness training provided by Montrose Memorial Hospital.

4. I certify that I am familiar with the privacy and security policies and procedures of Montrose Memorial Hospital, and I agree to follow those policies and procedures.

5. I agree to attend future HIPAA awareness training sessions, when requested by Montrose Memorial Hospital.

6. I further agree that I will promptly report any known or suspected violations of those policies or procedures regarding the privacy of health information to Montrose Memorial Hospital's privacy official.

Print Name: ____

Title & Dept: ____

Signature: ____Date: _________

Computer User Attestation

As a User of *Montrose Memorial Hospital's* Technology Resources, I have read and agree to observe and comply with all policies, procedures, guidelines and other directives of Montrose Memorial Hospital governing the use and security of Montrose Memorial Hospital's Technology Resources and the Information maintained or transmitted by the Technology Resources, including but not limited to Protected Health Information and Electronic Protected Health Information (the "Security Policies").

I understand that a violation of the Security Policies may result in disciplinary action, including possible termination, as well as potential civil and criminal liability.

Signature: ____ Date:________________