Jeffrey A. Passer, MD PC
Information Security Policy

1.0 Overview

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Protected Health Information (PHI) is any individually identifiable health information for patients.

The Payment Card Industry (PCI) standard requires that all entities that store, process or transmit credit card data must be compliant with the PCI Data Security Standard (PCI DSS).

Jeffrey A. Passer, MD PC is a covered entity as defined by HIPAA and a merchant under the definitions of the PCI DSS and major card brands, such as Visa. Jeffrey A. Passer, MD PC understands the importance of protecting all sensitive patient information, including financial account information. The failure to adequately protect PHI and credit card information could potentially lead to financial losses for both the patient and the clinic, potential physical harm to the patient, damage to Jeffrey A. Passer, MD PC's reputation, fines and legal consequences.

Measures must be in place which will minimize the risk to Jeffrey A. Passer, MD PC from threats including but not limited to unauthorized modification, destruction, or disclosure of confidential patient information, whether accidental or deliberate.

Effective security is a team effort involving the support of every Jeffrey A. Passer, MD PC employee and affiliate who has comes in contact with PHI or credit card information. It is the responsibility of every employee to know and understand the information in this policy, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to protect PHI, credit card and other sensitive information. This policy ensures that information is created and used in a secure environment and that information resources are adequately protected against loss, misuse, and abuse. Additionally, this policy ensures that individuals are aware of their responsibilities for protecting the security of confidential information.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other individuals working at or on behalf of My Office, including personnel affiliated with third parties who may have access to PHI and credit card information.

This policy may be modified or amended. Users will be notified of substantive changes to this policy.

4.0 Policy

4.1 Acceptable Use of Jeffrey A. Passer, MD PC systems and data
The following items apply to all individuals with access to confidential patient information.

1. Users must conduct themselves in accordance with all local, state, and federal laws, and in accordance with Jeffrey A. Passer, MD PC policies on ethics, privacy, security, and harassment.
2. While Company desires to provide a reasonable level of privacy, users should be aware that the data they create on the company systems remains the property of Jeffrey A. Passer, MD PC. Because of the need to protect Jeffrey A. Passer, MD PC systems, management cannot guarantee the confidentiality of information stored on any computer or network device belonging to Jeffrey A. Passer, MD PC.
3. Only computers owned by Jeffrey A. Passer, MD PC may have direct connectivity to any of company networks. In the event a vendor or contractor must have direct access to the network, the non-company asset must be specifically approved and must have anti-virus software installed, updated and running and personal firewall software installed/active. Access shall be revoked at a predetermined and limited time.
4. For security and network maintenance purposes, authorized individuals or service providers for Jeffrey A. Passer, MD PC may review files and data, monitor equipment, systems and network traffic at any time.
5. Management will only create accounts or provide computer resources to employees and agents of Jeffrey A. Passer, MD PC that have a legitimate business need for the resources.
6. Users are prohibited from modifying computer systems or network equipment to disable security features including but not limited to firewalls, intrusion detection systems, and anti-virus software.
7. Certain information is held to be confidential, proprietary, or sensitive. This includes, but is not limited to PHI and financial account information, including credit card numbers. Users should take all necessary steps to prevent unauthorized access to this type of information.
8. Occasional and reasonable personal use of Jeffrey A. Passer, MD PC's internet and e-mail services is permitted, provided that this does not interfere with work performance. These services may be used outside of scheduled hours of work, provided that such use is consistent with professional conduct.

4.2 Unacceptable Use
The following activities are, in general, prohibited. Under no circumstances is an employee or agent of Jeffrey A. Passer, MD PC authorized to engage in any activity that is illegal under local, state, federal or international law. The list below is by no means exhaustive, but is an attempt to provide a framework for activities which fall into the category of unacceptable use.

1. Copying, moving or storing of PHI onto local hard drives and removable electronic media when accessed through remote-access technologies (VPN, etc.) is strictly prohibited.
2. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
3. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. It also includes co-workers.

4. Using a company computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
5. Sending PHI, financial account or credit card information in an email or via end-user messaging technology is expressly prohibited.
6. Unauthorized use of an account or computer resource.
7. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
8. Any kind of harassment via email, telephone, paging, whether through language, frequency, or size of messages.
9. Providing information about, or lists of, Jeffrey A. Passer, MD PC patients or employees to parties outside Jeffrey A. Passer, MD PC.

4.3 Social Media

1. Remember that the Internet is not anonymous, nor does it forget. Everything written on the Web can be traced back to its author one way or another and very easily. Information is backed up often and repeatedly, and posts in one forum are usually replicated in others.
2. There is no clear line between your work life and your personal life in social media. Always be honest and respectful in both capacities. With the ease of tracing authors, finding the actual identity of a poster is not impossible. This creates an avenue for outside parties to link your personal writings to those you've done in a professional capacity. Always write as if everyone knows you. Never write anything you wouldn't say out loud to all parties involved.
3. Always keep confidentiality. Never disclose any confidential information about our patients or their business with us. Likewise, respect the clinic's confidentiality and proprietary information.
4. Avoid hazardous materials. Do not post, endorse, bookmark, or link to any materials that are defamatory, harassing, or indecent. Do not post any negative remarks about the clinic, its customers, its employees, its supervisors, or its competitors.
5. Do not return fire. If a negative post or comment is found online about the clinic, do not counter with another negative post. Instead, publicly offer to remedy the situation or report it to the office manager as soon as possible to defuse these types of situations.
6. Be smart about blogging. Personal web sites and blogs as good things and management respects your online activity as a medium of self-expression. However, please make it clear to your readers that the views you express are yours alone and that they do not necessarily reflect the clinic's views. To help reduce the potential for confusion, we would appreciate it if you put the following notice – or something similar – in a reasonably prominent place on your site: "The views expressed on this website/weblog are mine alone and do not necessarily reflect the views of my employer."
7. Think twice before forwarding emails. Jokes, urban legends, and get-rich email forwards are the oldest form of Internet-based social media. When it comes to clinic email, we ask that you think twice before hitting send and be judicious with the number of items you forward.

4.4 Password Guidelines

- System passwords for Centricity must be changed at least every 180 days.
- Passwords (yours or others) must not be inserted into email messages or other forms of electronic communication.
- Always use strong passwords, which have the following characteristics.
    - Contain upper and lower case characters.
    - Have digits and punctuation characters as well as letters.

    - Must be at least eight characters in length.
    - Must not be words in any language, slang, or jargon.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- Do not use the same password for Jeffrey A. Passer, MD PC accounts as for other personal accounts.
- Do NOT reveal a password over the phone to ANYONE.
- Do NOT reveal a password in an email message.
- Do NOT reveal a password to a co-worker or your supervisor.
- Do NOT talk about a password in front of others.
- Do NOT hint at the format of a password.
- Do NOT reveal a password on questionnaires or security forms.
- Do NOT share a password with family members.
- If someone demands a password, contact the officer manager.
- If an account or password is suspected to have been compromised, report the incident to the office manager and change all passwords.

4.5 Screensaver
All users must protect their PC's, and workstations with an automatically activated screensaver that is password-protected or which logs off after a period of inactivity. The period of inactivity should be no longer than 30 minutes for workstations in protected areas. Workstations in exam rooms must be logged off immediately when leaving the room.

4.6 Encryption
Encryption must be used anytime information is sent over a public network (i.e. the internet). Since email encryption can be expensive or inconvenient for recipients of emails, it is best to never send PHI, financial, credit card information or other sensitive information in an email. If processes require the transmission of sensitive information in email, please contact the office manager.

All systems accessed over the internet for the transmission of PHI and other sensitive information must use a secure connection such as SSL/TLS, IPSEC, SSH or VPN. (A good way to tell is to look at the URL for the site. If the address begins https:// then it is a secure connection. Sometimes there is a padlock icon that appears when accessing a secure site.)

If PHI or credit card numbers are ever transferred to removable media such as a CD, DVD, backup tape or external hard drive, it should be encrypted. Contact the office manager if transfer to removable media is ever required.

4.7 Portable Computers (laptops, mobile phones, tablets)
Because portable computers are especially vulnerable, special care should be exercised. It is recommended that portable computers not be used for the storage of PHI or confidential information. If this type of data must be stored on a portable system it is recommended that hard drive encryption technology be used to protect the data.

4.8 Viruses and Related Items

All computers must run anti-virus software and virus definitions must be kept current. Individuals should use extreme caution when opening e-mail attachments received from unknown senders, which could contain viruses, e-mail bombs, or Trojan code.

4.9 Clear Desk Policy
Computer screens must always be tilted away from view by the general public or passersby. Papers on the desk should be covered when others are nearby. When the desk is unattended, papers should be placed in a drawer or out-of-site. Lock up all papers at night and other times when the office is unoccupied. If handwritten notes include PHI, financial account numbers, credit card numbers or other sensitive information, shred them as soon as the information is transferred into the system.

4.10 Secure Areas
Jeffrey A. Passer, MD PC has a secure area where patient records and other confidential information may be kept. This area must be kept locked when unattended and visitors should not be allowed into this space without an escort.

4.11 Secure Destruction
All paper containing sensitive information must be shredded immediately when no longer needed, or stored securely in a locked area. Any removable media with PHI (CDs, DVDs, hard drives) must be destroyed or securely wiped before being discarded or reused. This includes hard drives in PCs, laptops, flash drives, mobile devices, fax machines and multi-function copiers.

5.0 Data Breach Response Procedures
A data security breach can occur from carelessness, accident or intentional theft of information. All employees, third-parties and contractors are responsible for reporting suspicious activity and known loss of information. Suspicious activity includes:

- Known loss of patient records
- A patient record that is unaccounted for
- Loss of computer hardware or mobile devices with unencrypted patient information
- Reports of fraudulent use of patients' personal medical or financial information
- Unexpected activity in patients' electronic records

In the event that suspicious activity is noted, it is every individual's responsibility to report the activity to the office manager for investigation. The office manager must keep accurate records, including dates and times, of all investigative activities. Any evidence collected must be strictly controlled. Local law enforcement should be contacted if theft of information is confirmed or highly suspicious.

When a breach of PHI is confirmed, whether intentional or due to carelessness, it must be analyzed and documented. If the breach involves 500 or more records, a risk assessment must be conducted to determine the extent of possible damage. If data is encrypted, the law currently allows that the risk of data compromise is low and the breach is not reportable. If the lost data is unencrypted then the breach must be reported the Secretary of Health and Human Services within 60 days of when the breach occurred. All individuals whose information may have been compromised must be contacted. Local media must also be notified of the loss.

If a breach of PHI involves fewer than 500 records, the breach must still be analyzed and documented, however it may be reported to the Secretary of Health and Human Services on an annual basis.

If a breach of credit card information is discovered, notify Visa Fraud Investigations and Incident Management group immediately at (650) 432-2978. An incident report must be provided to Visa within 3 days of the incident. More specific information can be found here: http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html

6.0 Annual Review

Management is responsible for initiating an annual review of this policy.

7.0 Acceptance

This policy requires annual acceptance confirmation by all employees, contractors, or other individuals with accounts on Company computer systems.

8.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Depending upon the infraction, violators may also be subject to criminal or civil penalties.

9.0 Revision History

This policy was issued on October 2, 2017. By: Jeffrey A. Passer, MD PC

Review dates:

Date: _____ By: _____

Date: _____ By: _____

Date: _____ By: _____