

	Policy: PepperPointe Information Technology Acceptable Use	
	Department Responsible: PepperPointe IT	Date Approved: December 31, 2023
	Effective Date: January 1, 2024	Next Review Date: January 1, 2025

INTENDED AUDIENCE:

Entire workforce

PROCEDURE:

In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as "regulatory requirements"), PepperPointe Partnerships is committed to ensuring the confidentiality, integrity, and availability of protected health information and electronic protected health information (PHI/ePHI), as well as sensitive and confidential data it creates, receives, maintains, and/or transmits. For purposes of this procedure, PHI, ePHI and sensitive and confidential data shall be referred to herein as "covered information."

The purpose of this procedure is to define roles and responsibilities, set expectations, and establish processes associated with acceptable use of organization or personally owned information technology.

Scope and Goals:

The scope of this procedure is to define the organization's expectations for acceptable use of information technology in or outside the workplace or as a representative of the organization while performing tasks or fulfilling job responsibilities. The goals of this procedure are as follows:

- Define acceptable and unacceptable behavior when using information technology assets (i.e., organization or personally owned), the internet, social media, and email.
- Define security and privacy requirements that pertain to the protection of covered information and employee, patient, and practice's safety.
- Define preventative measures that help avoid confidentiality breaches or loss of property.
- Define technology care, protection, and disposal requirements.
- Establish privacy expectations when using information technology.
- Define reportable incidents and the procedure used to report such incidents.

Responsibilities:

Information Technology Director (IT Director):

The IT Director is responsible for a number of activities, including, but not limited to, the following:

- Revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Work with Human Resources (HR) to help them understand the severity of violations to this procedure.
- Approving the use of information assets and organizational systems by the PepperPointe Partnerships workforce and ensuring that the security requirements stated in this procedure are complied with while using said assets and systems.

Information and Technology Team (IT Team):

IT Team is responsible for a number of activities in connection with this procedure, including but not limited to, the following:

- Implementing technology controls to monitor workforce activities when using information technology and report to the IT Director events that are in violation of this procedure.

- Approving all software that will be installed on PepperPointe Partnerships information technology assets. IT Team will ensure the software will not damage or disrupt the network or other information technology resources.
- With respect to workforce members who have been approved to purchase software, information such workforce members whether IT Team can support the software once installed.

Human Resources (HR):

Human Resources will consult with the IT Director to help them understand the severity and scope of procedure violations so that they can determine the appropriate disciplinary action to take.

Workforce:

Workforce members (i.e., PepperPointe Partnerships employees and contractors; also refer to the applicability section below) are responsible for:

- Reading and signing off on all requirements stated in this procedure.
- Reading applicable information security policies and procedures at least annually.
- Actively participating in all security awareness and education training events.
- Reading security awareness documentation/email when made available.
- Bringing to the attention of the IT Director any questions or concerns related to information security.
- Promptly report upon observation, suspected and known privacy and/or security incidents to the IT Director by email or in person.
- Complying with the requirements described in this procedure and for reporting any deficiencies or instances of non-compliance to the IT Director.
- Workforce members are responsible for all activity performed under their assigned userIDs.

General Security Terms and Conditions:

Workforce members of PepperPointe Partnerships have a responsibility to perform their duties in an ethical and professional manner. A significant part of the duties of workforce members will involve the use of different types of information technology. As such, PepperPointe Partnerships expects workforce members to carry out their job responsibilities in the same ethical and professional manner as they would when not using technology. Improper or unacceptable use of information technology can easily turn into a breach of patient confidentiality, criminal and civil liabilities against the organization, and threats to the safety and welfare of patients, coworkers, and practices, etc.

This agreement is required to be read, signed, and complied with by all workforce members prior to being given any access to all PepperPointe Partnerships information systems. The information system user signing this Agreement will only access, use, and disclose covered information in any medium as needed to perform his/her job responsibilities as allowed by law, organization policies, standards and procedures, and/or as agreed upon between said user and PepperPointe Partnerships.

1. I will assume sole and absolute responsibility to protect covered information in my possession in accordance with PepperPointe Partnerships security policies. This includes safeguarding and maintaining the confidentiality, integrity, and availability of all covered information I use, disclose, and/or access at all times, regardless of where I am working or how I am accessing the information.
2. I will only access, use, and/or disclose the minimum necessary covered information I require to perform my assigned responsibilities and will only disclose it to other individuals/organizations who need it to perform their assigned responsibilities. Protected health information (PHI) is specifically protected, by law, from further disclosures without prior authorization.
3. I will not use unapproved systems/programs/applications to transmit covered information. (Note: This applies to information sent internally on the corporate network and externally to a third-party entity).
4. I will retain covered information only for as long as it is necessary.

5. I will not access my own, or any family member's or other person's, record in any information system without prior authorization from PepperPointe Partnerships' IT Director (unless the activity has already been approved as a requirement assigned responsibilities).
6. I will not disclose/share any covered information with others who have not been formally authorized to have access to or knowledge of the information.
7. I will not download covered information to any personally owned computing devices.
8. I will not divulge, copy, release, sell, loan, alter, or destroy any covered information except as authorized by PepperPointe Partnerships' policies/procedures.
9. I will not download any covered information off PepperPointe Partnerships information systems to store or use it on any system, workstation, mobile devices, portable media (e.g., flash/thumb drive, CDROM, etc.), except in situations whereby explicit approval to do so has been granted by PepperPointe Partnerships' IT Director.
10. I will not download any software program onto PepperPointe Partnerships equipment without prior written approval from PepperPointe Partnerships' IT Director.
11. I understand that access to all PepperPointe Partnerships' information systems, including email and internet, are intended for business purposes.
12. I will use approved secure communications for transmitting covered information to authorized entities, in accordance with PepperPointe Partnerships security policies.
13. I will only access or use the systems or devices that I am being authorized to access and agree not to demonstrate the operation or function of any of PepperPointe Partnerships' information systems or devices to unauthorized individuals.
14. I will never use tools or techniques to break/exploit security measures.
15. I will never connect to unauthorized networks with PepperPointe Partnerships' systems or devices.
16. I understand that I have neither ownership interest nor expectation of privacy in any information accessed or created by me during my relationship with PepperPointe Partnerships. PepperPointe Partnerships will audit, log, access, review, and otherwise utilize information stored on or passing through its systems for purposes related to maintaining the confidentiality, security, and availability of covered information.
17. I will not use PepperPointe Partnerships' information systems to transmit, retrieve, nor store any communications consisting of discriminatory, harassing, obscene, solicitation, or criminal information.
18. I understand that my user login ID (userID) and password(s) are used to control access to PepperPointe Partnerships' information systems and covered information. I will not share my userID and password/codes with anyone, nor allow anyone to access any information systems I am authorized to access, using my userID and password(s).
19. I understand that I will be held accountable for all activities associated with my userID.
20. I will not use anyone else's userID and password(s).
21. I will immediately notify the IT Director if my password has been seen, disclosed, or otherwise compromised.
22. I will immediately report to the IT Director any activity that violates this agreement, federal or state laws, or any other incident that could have any adverse impact on covered information and PepperPointe Partnerships.
23. Upon completion and/or termination of access to PepperPointe Partnerships' information systems, I will return all devices containing covered information or paper-covered information to my direct supervisor.
24. I affirm that I will maintain the confidentiality, integrity, and availability of all covered information even after termination, completion, cancellation, expiration, or other conclusion of access to PepperPointe Partnerships' information systems.

Mobile Device Acceptable Use:

The purpose of this section is to advise you of your responsibilities for the use and protection of PepperPointe Partnerships' mobile device(s) that have been issued to you. As a user of a PepperPointe Partnerships mobile device, you are responsible for complying with all information security policies and procedures which include the following specific requirements:

- You will not perform any kind of maintenance on this mobile device, unless it is within the scope of your job responsibilities.
- You will not change or disable any security settings that could negatively impact the security of the operating system, computer, or the information that resides on it. This includes jailbreaking or rooting the device.
- You will not upload or download any programs onto this mobile device without the approval of PepperPointe Partnerships' Information Technology Department, unless it is within the scope of your job responsibilities.
- All covered information stored on the hard drive of this mobile device will be encrypted in accordance with PepperPointe Partnerships' Data Classification and Handling procedure.
- Only approved application stores can be used to download software. The use of unapproved application stores is prohibited for company-owned and BYOD mobile devices. Non-approved applications or approved applications not obtained through the application store are prohibited.
- You will not store passwords, PINs, passcodes, etc. (to include flash/thumb drives, etc.), in the mobile device storage case.
- You are responsible for properly safeguarding this computer against unauthorized use in accordance with PepperPointe Partnerships' Information Technology Acceptable Use procedure and Teleworking Security procedure.
- For any reason should you or PepperPointe Partnerships terminate your employment/contract, all equipment will be returned to PepperPointe Partnerships, including the accessories (i.e., carrying case, backup drives, thumb/flash drives, power adapter, etc.). You will not give your mobile device to any other employee, unless instructed to do so by Human Resources or IT Team.
- Immediately report a lost or stolen mobile device to PepperPointe Partnerships' IT Director.

When traveling, you will take the following precautions:

- In situations where you cannot maintain physical possession of the mobile device, secure the mobile device in a manner that will prevent unauthorized access or theft (e.g., secure in trunk of a vehicle, hotel safe, or some kind of locking container that can only be accessed by you). If this is not possible, store the device out of sight (i.e., hotel room in a drawer underneath clothes).
- When traveling by plane, treat the mobile device as carry-on, never check as normal baggage.
- Never store in overhead compartments on mass transit systems (e.g., aircraft, buses, shuttles, trains, etc.)
- If you do a considerable amount of travel, talk to the IT Director about purchasing an anti-theft device.
- Always be aware of people who may be eavesdropping when you work in public places or in close proximity with other people (i.e., coffee shop, restaurants, aircraft, etc.). If necessary, consider the purchase of a privacy screen for your mobile device.
- If you have reason to believe that you have been working in a place that would be considered high risk for device tampering, interception of communications, etc., immediately report this to IT Team upon your return so that your device can be checked for tampering and malicious software.

Email Acceptable Use:

PepperPointe Partnerships' email system will be used for business purposes in an appropriate and professional manner and will not be used for any of the following unacceptable practices:

- Sending covered information via email outside of PepperPointe Partnerships' network without using approved encryption, in accordance with PepperPointe Partnerships' Data Classification and Handling procedure.
- Use that violates PepperPointe Partnerships' Professional Code of Conduct or Harassment policy.
- Knowingly distribute email chain letters or hoaxes.
- Knowingly distribute email malware.
- Advocating personal religious or political views and opinions.
- Solicitation for personal gain (unless approved by Human Resources, i.e., sale of personal property, fundraising, etc.).
- Gambling.

- To send messages with derogatory, discriminatory, or inflammatory remarks about an individual's race, color, age, sex, disability, religion, national origin, physical attributes, or sexual preference.
- To make false or misleading statements about PepperPointe Partnerships' patients/customers/clients, fellow workforce members, leadership, co-workers, business partners, etc.
- Forging or attempted forgery of email.
- Reading, deleting, copying, or modifying another coworker's email with malicious intent.
- Using abusive, profane, or offensive language within email.
- Violating the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or other local jurisdiction.
- Engaging in fraudulent activities.
- Sending or receiving material that is vulgar, offensive, pornographic, anti-Semitic, racist, or sexual in nature.
- Engaging in activities that disrupt or interfere with the performance of PepperPointe Partnerships' network or systems.
- Harassing, threatening, or stalking others.
- Disclosing someone's security code or password.
- Transmitting copyrighted materials or intellectual property to anyone without the permission of the copyright/property owner.
- Using "email anonymous" services to hide your identity or masquerade as someone else.
- Using another person's e-mail account to send or receive messages, without their approval.
- Forwarding email from a PepperPointe Partnerships account (all or in part) to an external address (i.e., personal email account).
- Sending personal comments or opinions via email that would give readers the idea that you are speaking on behalf of PepperPointe Partnerships.

If you receive an email that seems suspicious, immediately inform security. DO NOT respond to these types of email, as they could be a phishing attempt or another type of email that will infect your asset with malware. Keep in mind, that it is possible for these types of emails to look like they are from a credible source. Always be sure to check the email address of the sending entity as this will not normally match up with the content of the email. Also, do not open attachments or click links within these types of emails as they will likely lead you to a landing page for the purposes of collecting your access credentials or they will immediately infect your asset with malware.

Internet Acceptable Use:

PepperPointe Partnerships owned assets with the ability to access the internet will be used in a professional and appropriate manner. The following practices are unacceptable:

- Transmitting covered information over the internet without proper encryption in accordance with PepperPointe Partnerships' Data Classification and Handling procedure.
- Use that violates PepperPointe Partnerships' Professional Code of Conduct and Harassment policy.
- Advocating personal religious or political views and opinions, provided, however, that an employee is permitted to send emails to government officials and other lobbying groups concerning matters affecting PepperPointe Partnerships.
- For solicitation for personal purposes or for personal gain, to include gambling.
- To make false or misleading statements about PepperPointe Partnerships, patients/customers/clients, fellow workforce members, leadership, business partners, etc.
- To transmit or download content of a discriminatory, racist, or harassing nature.
- To transmit or download content of an obscene or pornographic nature.
- Violating the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or other local jurisdiction.
- Engaging in fraudulent activities.

- To view pornographic, racist, discriminatory, hate sites, or any other sites deemed inappropriate by PepperPointe Partnerships.
- Engaging in activities that disrupt, disable, or interfere with the performance of PepperPointe Partnerships' network, systems or applications. This includes the deliberate development and/or propagation of malware or the transfer of malware designed to crash, damage, or impair PepperPointe Partnerships' or a third-party network or their external or internal systems.
- To harass, threaten, or stalk others.
- To intentionally disclose anyone's security code or passwords without their authorization.
- To transmit copyrighted materials belonging to entities other than this company, without the permission of the copyright holder.
- To knowingly download or distribute pirated software.
- To post derogatory or unprofessional personal comments or opinions on newsgroups, blogs, social networking sites, etc. that could give readers the idea that I am speaking on-behalf of PepperPointe Partnerships.
- For the misappropriation or theft of intellectual property or copyrighted material.

Social Media Acceptable Use:

Refer to the Social Media policy for acceptable use guidelines regarding what you should and should not do when publishing content on social media.

Portable Media Use:

The general rule of thumb is that portable media (i.e., CD-ROM, flash/thumb drive, etc.) will not be used to store covered information. If you have justification to do so and approval from the IT Director, the following rules apply:

- Media will be encrypted using approved software.
- Maintain constant surveillance over the media and if you need to leave it unattended, it will be locked in a manner to prevent unauthorized access.
- In the event of a suspected or actual event where media is improperly disclosed, lost, or stolen, IT Team and/or the security team must be immediately notified.
- Personal portable media will never be used for covered information.

Software Use and Accountability:

Only software that has been approved for legitimate business requirements and has been evaluated and approved for use by IT Team will be allowed on PepperPointe Partnerships' information technology assets.

Voice Over Internet Protocol (VoIP) Use:

The use of voice-over internet protocol or VoIP is authorized at PepperPointe Partnerships. When using VoIP, the following security requirements must be followed:

- Only the following programs are allowed: Cisco Jabber using PepperPointe Partnerships userID and password.
- VoIP system performance is monitored by Nextiva's Administrative Portal.

Disposal of Software, Hardware and Media:

All software and hardware owned by PepperPointe Partnerships will be disposed of by IT Team. This is done to ensure that all copyright laws are obeyed, and computer hard drives are properly erased or destroyed and accounted for, in accordance with regulatory requirements, and organizational policies/procedures. Portable media will be destroyed in accordance with PepperPointe Partnerships' Technology Asset Management procedure.

Hardware Use:

The following rules apply to all PepperPointe Partnerships owned information technology hardware resources:

- All information technology hardware must be pre-approved by the IT Team to ensure it is compatible with PepperPointe Partnerships' network and complies with security requirements.
- Personally owned devices (i.e., computers, tablet PCs, smartphones, etc.) are not authorized for use with or connected to PepperPointe Partnerships' network unless approved by the IT Team and in compliance with PepperPointe Partnerships' Personal Device Use procedure.
- All PepperPointe Partnerships owned information technology hardware will be promptly returned to the IT Team when no longer needed or upon terminating employment. Information technology assets will not be repurposed, donated, disposed of, or returned to a leasing agency (if applicable) by anyone other than the IT Team and only after it has been properly sanitized in accordance with the organization's Technology Asset Management procedure.

Personal Device Use:

For those workforce members who have been approved to use personal devices for work-related purposes, they must comply with the Personal Device Use Policy.

Working Offsite:

PepperPointe Partnerships workforce members who travel or periodically work from home or from a public location (i.e., coffee shop, restaurant, etc.) will comply with PepperPointe Partnerships' Teleworking Security procedure.

Physical Security:

Workforce members will only print to and copy on approved business office machines (i.e., printer/copier/fax/scanner). Workforce members will immediately retrieve covered information from shared business machines unless the machine has a personal mailbox that is password controlled. At no time will covered information or other confidential data be left unattended on business office machines or at workspaces. Hard copies of covered information are secured in locked cabinets, drawers, etc. at the end of the workday.

Computers that work with covered information will not be located in public areas where access cannot be controlled or continually monitored.

When working on covered information, PepperPointe Partnerships workforce members will position their computer monitors in a manner that prevents unauthorized/casual viewing. If monitors cannot be positioned to prevent unauthorized/casual viewing, then privacy screens/filters will be used.

Restricted Areas:

Workforce members who have access to restricted areas will refrain from any activity that could lead to a compromise of restricted area security (i.e., leaving personnel who do not have access alone in a restricted area, disabling the locking mechanism of a door leading to a restricted area, propping the door open to a restricted area, etc.).

Workforce members who do not have access to restricted areas will not attempt to circumvent security or forcibly attempt to enter restricted areas.

Workforce members will return all building keys and badges to their manager or Human Resources on their last day of employment/contract work.

Workforce members who are issued keys will immediately report lost or stolen key to IT Director.

Password Use:

Password composition, change intervals, restrictions for reuse, etc., are enforced by each information technology system, thereby alleviating workforce members of this responsibility. Password requirements that are still a part of workforce members' responsibilities are as follows:

- Workforce members will log out of the system and off the network, if they plan to leave their computer unattended for any amount of time or will engage a password protected screensaver.
- Workforce members will use different passwords for each application/system they have access to. This prevents anyone from having full access to all systems a member has if their password is compromised.
- Workforce members will never share their passwords. If a password must be shared during an emergency or in the event there is a problem with his/her computer, change the password as soon as possible after the problem has been resolved.
- Workforce members will never transmit/send/email passwords in the clear (readable text and unencrypted) over the internet or any other untrusted network.
- For passwords that are not received as part of an automated process, workforce members will acknowledge the reception of passwords either through a direct phone conversation with the helpdesk or through some other form of communication (i.e., email, instant message, etc.)
- Workforce members will commit passwords to memory. However, it is understood that this may not always be possible due to the large number of passwords that members may have. Should it become necessary to write your passwords down, workforce members will protect them no differently than a personal ATM PIN, credit cards, checkbook, etc. Workforce members may also utilize smartphone password vault applications to store passwords, provided they are approved for use by the IT DIRECTOR.
- Workforce members will never store passwords:
 - In laptop cases
 - Unencrypted in files or directories on the network
 - Unencrypted on smartphones, etc.
 - Around the workspace/area

If workforce members suspect that their password may have been compromised, they will change it immediately. If there is reason to believe that the password was forcibly or inappropriately obtained, workforce members will immediately report the incident to the security officer.

Privacy Expectations:

PepperPointe Partnerships will make all reasonable attempts to provide security and privacy for its employees. However, the organization cannot guarantee absolute privacy for documents created, stored, transmitted or received on PepperPointe Partnerships' computers or while working on the internet. PepperPointe Partnerships routinely backs up computers and these backups are retained for varying periods of time. PepperPointe Partnerships also tracks and records where workforce members go on the internet and what phone numbers they call from the organization's telephone system. Management, Human Resources, or IT Team personnel occasionally access these files for different purposes, to include monitoring computer usage (e.g., email, internet activity, etc.) and examining file content.

PepperPointe Partnerships computer systems, email, telephone systems, and internet are for the exclusive use of PepperPointe Partnerships' workforce for work related purposes. Individuals using these resources with or without proper authority, or in excess of their authority, are subject to having all of their activities on these systems monitored and recorded in accordance with federal and statutory requirements. Use of these resources implies consent to such monitoring. If such monitoring reveals possible evidence of inappropriate or criminal activity as defined by PepperPointe Partnerships' information security policies, IT Team will provide this evidence to your immediate supervisor, Human Resources, and/or law enforcement officials for appropriate disciplinary or legal action.

Security Incident Reporting

Expeditious reporting of suspected or actual security incidents to the IT DIRECTOR cannot be stressed enough. Workforce members must not hesitate to report any of the following, suspected or otherwise:

- Use of another person's password and/or account to login to a system without consent.

- Failure to properly protect passwords and/or access codes.
- Installation of unauthorized software.
- Falsification of information.
- Loss or theft of equipment or software.
- Destruction or tampering with equipment or software.
- Posting of covered information on the internet.
- Use of personal email, text/instant messaging, etc. for work related purposes.
- Improper disposal of portable media and mobile devices.
- Terminated workforce member accessing applications, systems, or network.
- Insider threats (i.e. disgruntled employee that is suspected to pose a threat to the workforce or technology resources)
- A missing or misplaced technology asset
- A technology asset with no asset identification tag
- Discovery of an unidentified technology asset
- Unauthorized log-on or log-on attempts using your userID

Incidents, actual or suspected need to be reported immediately to:

- IT Director
- Systems Administrator
- Direct Supervisor

Workforce members can report incidents, actual or suspected, or suspicions of insider threat without fear of repercussion.

Terms and Conditions of Employment:

Workforce members will cooperate with federal, state and internal investigations (disciplinary or otherwise). Failure to do so, can result in disciplinary action up to and including termination.

Documentation Retention:

Previous versions of this procedure must be retained for at least 6 years.

Exception Management:

Exceptions to this procedure will be evaluated in accordance with PepperPointe Partnerships' Information Security Exception Management procedure.

Applicability:

All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for PepperPointe Partnerships, is under the direct control of PepperPointe Partnerships, whether or not they are compensated by PepperPointe Partnerships.

Compliance:

Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with PepperPointe Partnerships. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.