	Policy & Procedure: Email Security & Encryption	
	Department Responsible: PepperPointe IT	Date Approved: January 1, 2024
	Effective Date: January 1, 2024	Next Review Date: January 1, 2025

Intended Audience:
Entire workforce

Policy:
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 (covered information/ecovered information), as well as sensitive and confidential data it creates, receives, maintains, and/or transmits. For purposes of this procedure, covered information, ecovered information and sensitive and confidential data shall be referred to herein as "covered information."

The purpose of this policy is to ensure the secure and confidential transmission of covered information via email. This policy outlines the guidelines and procedures for users to follow when sending covered information through email, emphasizing the use of encryption to safeguard the information from unauthorized access.

Scope:
This policy applies to all employees and any other individuals who have access to covered information and are authorized to communicate covered information via email on behalf of the organization.

Procedure:
- Identifying covered information:
  - Users must be vigilant in recognizing information that qualifies as covered information.
  - Only send covered information through email when it is necessary for the business process.
- Encryption Software:
  - Users must utilize organization-approved email systems that support encryption.
  - Personal emails and/or email addresses not contained within the organization's email system are NOT compliant to send covered information.
  - All details about utilizing our email encryption can be found at Email Security & Encryption
- Recipient Verification:
  - Before sending any email containing covered information, verify the recipient's identity and ensure they have a legitimate need to access the information.
  - If uncertain about the recipient's identity, confirm their contact information through a secure means before transmitting the email.
- Subject Line Notification:
  - Ensure to place a clear indicator in the subject line of the email.
    - Utilize: “SECURE” or "ENCRYPT", to alert recipients that the message contains covered information and is encrypted. This ensures that the system always encrypts the message.
- Message Content:
  - Clearly state the sensitivity of the information contained in the email.

    - Avoid including unnecessary details in the email body and attachments.
- Recipient Instructions:
    - Some recipients may be unfamiliar with unencrypting a secure email, recommend sending instructions to the recipient on how to decrypt and access the covered information. Instructions for this process can be found here: Receiving & Decrypting Secure Email
    - Specify any security requirements or additional steps necessary for accessing the information.
- Access Monitoring:
    - Track and log access to encrypted PHI.
    - Regularly review access logs to identify any unauthorized attempts or breaches.
- Incident Reporting:
    - Report any suspected or actual breaches of encrypted covered information immediately to the designated security officer.
    - Follow the organization's incident response procedures for addressing and mitigating security incidents.

This policy will be reviewed annually or as needed to ensure its relevance and effectiveness. Any necessary updates will be made promptly to address changes in technology, regulations, or organizational processes.