	Policy: Email Compliance – Prohibit Personal Email Usage	
	Department Responsible: PepperPointe IT	Date Approved: January 1, 2024
	Effective Date: January 1, 2024	Next Review Date: January 1, 2025

Intended Audience:
Entire workforce

Scope:
All Employees are required to utilize company-provided email accounts for all work-related communication involving patient health information and other sensitive data. The use of personal email for work purposes is strictly prohibited due to the risks it poses to data security, confidentiality, and HIPAA compliance.

1. **Data Security and Confidentiality:**
    a. Personal email accounts lack the robust security measures implemented in company-provided email systems, increasing the risk of unauthorized access to patient health information.
    b. HIPAA Privacy Rule (45 CFR 164.312(e)(1)) about transmission security is the requirement to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
    c. HIPAA Privacy Rule (45 CFR 164.312(e)(2)(ii)) requires a mechanism be in place to encrypt electronic protected health information whenever deemed appropriate. When emailing ePHI externally, it must be encrypted during transmission to ensure that the appropriate recipient receives the data and cannot be intercepted.
2. **Data Breach Risks:**
    a. Personal email accounts are more susceptible to hacking and data breaches compared to company-provided email accounts, potentially exposing sensitive patient information.
    b. Personal email account services are not covered under a Business Associate Agreement (BAA). A BAA is a contractual agreement between a covered entity (such as any dental practice) and a business associate (such as a software service provider like Microsoft/Google) that outlines the responsibilities of each party regarding the protection of Protected Health Information (PHI).
    c. The HIPAA Security Rule requires covered entities to enter a BAA with their business associates to ensure that these third parties also comply with HIPAA requirements regarding the protection of PHI. A BAA includes provisions specifying how PHI will be handled, the security measures the business associate will implement to protect PHI, requirements for reporting breaches or security incidents, and assurances that the business associate will not misuse or disclose PHI except as permitted by HIPAA.
        i. HIPAA Privacy Rule:
            1. 45 CFR 164.502(e) requires covered entities to have contracts or other arrangements (i.e., BAAs) with their business associates that ensure the

business associates will appropriately safeguard protected health information (PHI) in accordance with HIPAA rules.

ii. HIPAA Security Rule:

1. 45 CFR 164.308(b)(1) requires covered entities to implement policies and procedures to ensure the security of electronic protected health information (ePHI), including when working with business associates.

3. **<u>Audit Trail and Accountability:</u>**

a. Company-provided email accounts features such as message tracking and archiving, facilitating audit trail and accountability in compliance with HIPAA regulations.

i. HIPAA Security Rule: Audit Controls (45 CFR 164.312(b)): requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. This includes email systems where ePHI may be transmitted or stored. Auditing email activities helps track who accessed ePHI, what changes were made, and when they occurred.

ii. HIPAA Privacy Rule: Access Controls (45 CFR 164.312(a)(1)): While not explicitly addressing email archiving, this section requires covered entities to implement policies and procedures to limit access to PHI to only those persons or software programs that have been granted access rights. Archiving email communications with PHI can support access controls by providing a record of who accessed the information and when.

b. Failure to maintain proper audit logs and tracking mechanisms for electronic communication involving ePHI violates HIPAA requirements (45 CFR 164.312) and result in compliance issues during audits.

PepperPointe and our practices are legally obligated to comply with HIPAA regulations to protect patient health information and maintain the trust of our patients.
Violations of HIPAA regulations, including the use of personal email for work-related communication, can lead to significant fines, legal consequences, and damage to the organization's reputation (45 CFR Part 160, Subparts C and D).