**Cybersecurity Practice #1: Email Protection Systems**

Review Conducted on:
Reviewed By:

Scheduled Employee Training Date:

**This section includes:**
***Email system configuration:*** the components and capabilities that should be included within your email system.

***Education:*** how to increase staff understanding and awareness to protect your organization against email-based cyber-attacks such as phishing and ransomware.

***Phishing simulations:*** ways to provide staff with training on and awareness of phishing emails.

**Email System Configuration Checklist:**

**\*check with your IT provider if you need help.**

Email service provider:

Company email address:

Do you use your domain (i.e. admin@orthosmile.com)?

Do you encrypt your email?

Verify your encryption method complies with industry standards.

Is spam and malware filtering on?

Do you use desktop security software to protect computers from malicious email?

Is this software updated now?

Is this software set to update automatically?

Have you enabled multi factor authentication?

Does each employee have a unique email address?

Do you force a secure password process that includes at least 8 characters long and include a combination of upper and lower case letters, numbers, and special characters?

**Browser Configuration**
Do you update browsers automatically?
Do you filter traffic to prevent access to non-business related websites?

Have you disabled auto-fill?

Have you installed ad-blockers?

DO you use a Virtual Private Network to access websites?

Resource
Web Browser Secure Settings.” University of California Santa Cruz Information Technology Services. September 25, 2020. https://its.ucsc.edu/software/release/browser-secure.html.

Employee Education

Have employees taken the annually required HIPAA and Cybersecurity awareness training?

Register your team at <http://www.donedeskedu.com/cyber>

Does your employee onboarding checklist include cyber and HIPAA training?

Do you have a process to re-train employees to maintain awareness?

Do you highlight the importance of cybersecurity and protecting patient data monthly?

Do your employee know how to send secure email via encrypted means?

Does your training include noticing and awareness of fraudulent email?

Do your employees know who to report suspicious activity to?

Resource

“How to Recognize and Avoid Phishing Scams.” Federal Trade Commission. May 2019. https://www.consumer.ftc.gov/ articles/how-recognize-and-avoid-phishing-scams.

Phishing Simulations

Have you conducted employee training on phishing and social engineering?

Have you scheduled future training to ensure you have budgeted the time?

Resource

“Free Cybersecurity Services and Tools.” Cybersecurity & Infrastructure Security Agency (CISA). https://www.cisa.gov/ free-cybersecurity-services-and-tools.