Email & HIPAA-Compliance

By Marlene M. Maheu, PhD

The convenience of email has made it an attractive way for counselors to communicate with clients both quickly and easily. The HIPAA Omnibus Final Rule[1], effective March 26, 2013, states that a healthcare professional is permitted to send health information via unencrypted email if the patient has been advised of the risks of email. It is recommended that the counselor engage in a thorough discussion about such risks, and obtain a written informed consent agreement from the patient to document the detailed discussion.

Risks of Sending PHI via Unsecured Email

There may be several risks involved with sending unsecured email. The factors may be related to technology, as well as human error or intentional deception. This article will highlight risks to consider that may compromise an individual's right to privacy by sharing Personal Health Information (PHI):

- Email may be transmitted through many unsecured servers and may be intercepted or misdirected during transmission. The email services may not have security protocols in place for employees with access to email. For example, employees may not have the proper security clearance or training to handle the data.
- Email can be captured electronically en route, lost, delayed, or fail to be delivered.
- Email can be sent to or be accessed by an unintended person, perhaps due to a typing error, selecting the wrong name in an auto-fill list, or malfunctioning hardware/software.
- "Free" email can and often is read by the free email software programs. Such companies often run automated searches of email for words that suggest an interest in products related to potentially confidential topics being discussed. The identity of the parties conducting these searches is unknown.
- Email can be sent prematurely, before the author intended to release it.
- A common error occurs when a sender of an email forgets to remove previous exchanges in the same thread. This information can have a negative impact on vulnerable clients and patients for a wide variety of reasons when there are others using their email box see such past exchanges.

When working with clients, there may be other risks involved in sending PHI through unsecured email. You may be able to think of other scenarios that may have been problematic for you in the past when using email to communicate with family or friends. Although such occurrences with loved ones can be forgivable, sharing PHI in email with a clinical population demands a higher level of professionalism. It is the responsibility of counselors to prevent HIPAA security and privacy violations that can damage the client. Healthcare professionals need to be competent to handle PHI before offering such services to the public.

Securing Connections from Both Sides

An electronic transmission should be secured from both sides of the transaction — the patient as well as the healthcare professional. Imagine an email, text, or video message as similar to a handshake, wherein the agreement has to be entered into by each party. To seal the deal, secured code sets have to lock into each other in order to secure the transaction. Without the involvement of both sides, the agreement is not valid.

HIPAA Email Privacy Compliance Checklist

The healthcare practitioner or entity should obtain a written consent from all patients before any communication via email or other technology. If you should choose to utilize email in your clinical setting, the following are a few hints to guide you:

- Include an automatic email signature disclosure to remind patients that email is not secure, and to delete an email not meant for them. You can find samples of templates at www.exclaimer.com/email-signature-handbook/10026-101-email-signature-templates to consider when you create your email practice signature statement.
- Assure that the connection between all computers, smart devices and the email server are encrypted. To achieve this goal, conduct frequent risk assessment of all devices to be sure that they are in compliance with security standards. There is a U.S. Government Security Risk Assessment tool available for downloading at www.healthit.gov/providers-professionals/security-risk-assessment, which produces a report that can be provided to auditors.
- Avoid transmitting diagnoses and sensitive PHI via email or text messaging. When engaged in telehealth of any type, communicate diagnoses and other PHI via telephone or surface mail.
- To increase email privacy and security when transmitting sensitive medical information, consider email programs that offer encryption. Programs such as Google, Gmail for Work, or Office 365 from Microsoft build the security features into the software, negating the need to log in and out of separate software to check patient email. Some practice management and videoconferencing platforms build email functions into the interface so that all exchanges with patients are conveniently found in one place.
- Use an email service that provides a HIPAA Business Associate Agreement (BAA). Refer to this the TBHI blog post located at https://telehealth.org/blog/google-agrees-to-sign-baa-as-means-to-hipaa-compliance for details of the Business Associate Agreement and how Google has handled it. There are other companies offering BAAs as well.
- Create unique email passwords and store them in a password manager, such as: Keepass (http://keepass.info), Dashlane (www.dashlane.com), or LastPass (www.lastpass.com).
- Install an antivirus program on every computer that accesses email.
- Enable settings in all email software to block emails that may have viruses.
- Use two-factor authentication for email, without exception. Such authentication prevents hackers from accessing your email, and this feature is available at no cost in programs such as Gmail for Work.
- Be sure to have a written privacy and security policy. Document that all staff members have received and understand it.
- Always update software to the newest version. HIPAA violations have occurred and led to negative publicity and files when outdated software has been used in healthcare settings and hackers have accessed PHI.
- Organize a formal training session to educate staff on what is allowed to be sent via email and SMS. Document time and location of training for such HIPAA-compliance policies. One topic that may be included in the training can be on phishing with online training sites such as OpenDNS Phishing Quiz or McAfee Phishing Quiz.

Disclaimer and Caution

In summary: Ignorance is no defense in the face of the law. Data protection and legal compliance are your responsibility. The Telebehavioral Health Institute (TBHI) strongly advises you to hire a local telehealth attorney in your state for a thorough document and telehealth process review. If you cannot afford such a service privately, TBHI encourages you to approach your professional association to hire an attorney on behalf of their entire membership.

Marlene Maheu, PhD, is the founder of the Telebehavioral Health Institute. Focused exclusively on telebehavioral health, she has written four textbooks and trained more than 20,000 clinicians from 60 countries. Recognized as one of the leading experts in telepractice, she is the originator of the Online Clinical Practice Model (OCPM) for ethical telemental health, telepsychiatry, telepsychology, distance counseling and online therapy. As a world-class leader in the field, she offers practical strategies, straightforward solutions and the hands-on wisdom that only develops through time and diligence. She will be offering a full-day pre-conference workshop in Telebehavioral Health Best Practices at the 2017 NAADAC Annual Conference on Friday, September 22.

(Endnotes)

[1]Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 17 (January 25, 2013) (codified at 45 CFR Parts 160 and 164).