American Professional Agency

RISK MANAGEMENT

IN THIS ARTICLE

PREPARED BY

Risk Management Group
AWAC Services Company,
a member company of Allied World

Please contact American Professional Agency at psychiatry@americanprofessional.com or 800-421-6694 (x2318) to learn more about our comprehensive professional liability coverage and risk management programs.

www.americanprofessional.com

CONSIDER THIS…

Can You Send Me an Email or Text Me?

Not surprisingly, patients/clients increasingly desire to interact with their healthcare providers via social media, emailing and/or texting.[1] Before doing so, it is important to understand the risks involved, particularly as new devices, technologies, and platforms continue to emerge.

Texting and Email Use

Texting, e-mailing or other electronic communication should only be conducted in an established patient/client relationship and only after obtaining patient/client consent. Additionally, all clinically relevant treatment related communications should be part of the patient/client record.[2]

When deciding whether to correspond with patients/clients electronically, consider having an office policy and keeping the communication confined solely to scheduling, administrative, and non-clinical issues. Ensure that the patient/client is aware of your office policy and have them sign off on the policy.

The policy should inform your patients/clients about your frequency in monitoring incoming emails/texts, your typical response time, including the anticipated response time for communications received during non-business hours. Additionally, consider having an auto-response generated by incoming emails/texts that provides information on how to seek emergency treatment, if needed, and again, informs the patient/client about when they can expect a response.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule[3] applies to Covered Entities (CE) and their Business Associates (BA), and presumes electronic communications containing Protected Health Information (PHI) is encrypted. Encryption transforms an original message of regular text into encoded text.[4] The receiver must then use a password to decrypt the communication back into plain, readable text. Encrypted communications have a lower probability of being accessed/viewed by an unauthorized individual.

Despite the HIPAA Security Rule's encryption specifications, patients/clients may request to communicate with you via email/texting without regard to whether the information sent is encrypted. In the event that a patient/client requests you send unencrypted PHI, it is prudent to inform them of the risks involved with unencrypted communications, including the possibility of the PHI being viewed by unauthorized parties. Document this discussion in their record.

RISK MANAGEMENT

0320

Another consideration with emailing and texting with patients/clients is ensuring that the intended recipient receives the communication, and that the communication is not inadvertently emailed/texted to an incorrect email address or telephone number. Moreover, it is important that when emailing/texting with a client/patient, that it be to his/her personal (not work) account. Email sent to a patient/client work account may not be afforded privilege protections – as typically workplace emails are considered the property of the employer.

Texting has additional risk considerations. Anyone who uses a handheld device knows the perils of auto-correct. The device may auto-correct text that you may or may not have meant to type. Before you know it, you click send and off it goes with the wrong word/phrase typed. Another issue to consider, again, is ensuring that the person you are sending the text to is the one who actually receives it. Similarly to email, inform your patients/clients regarding an expected response time.

Can I Use Social Media with Patients/Clients?

Social media is an expansive term, which covers a large range of websites that allows users to interact with each other through the website. Facebook and WhatsApp are the most widely used major social media platforms. Smaller social media platforms include:

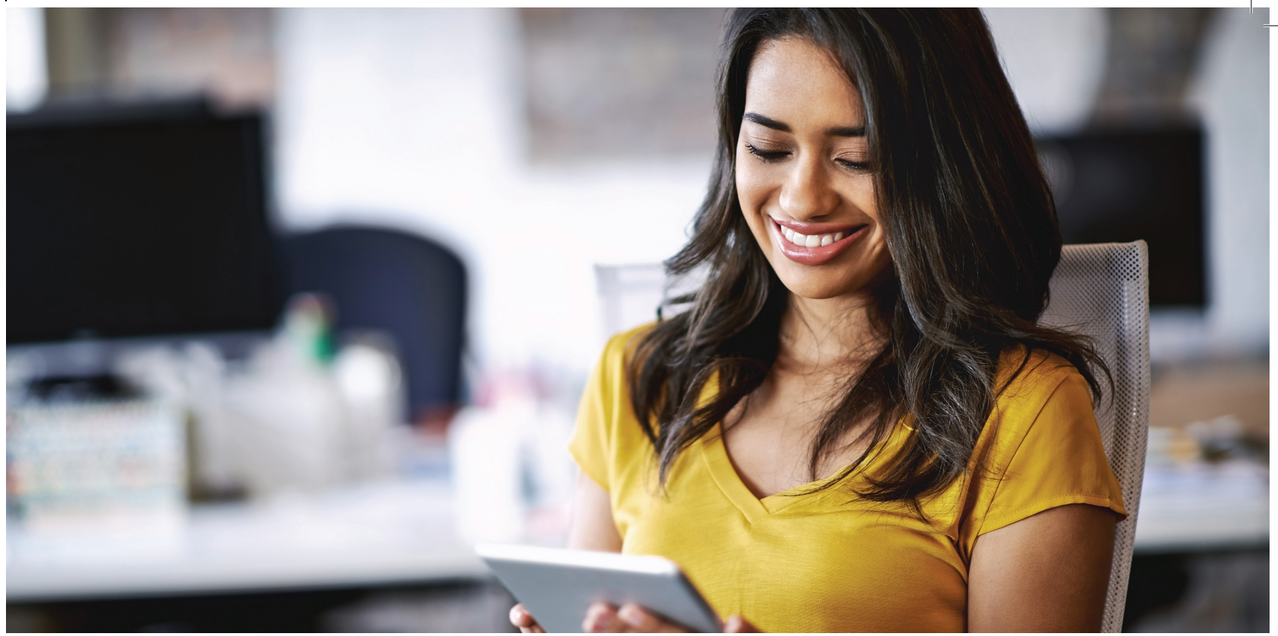
- Twitter, a social networking and microblogging service enabling users to send ("tweet") and resend ("re-tweet") 140 character text messages/pictures
- LinkedIn, a professional networking site
- YouTube, a video sharing network
- Skype, a software system that allows online voice calls and video conferencing
- SnapChat/Instagram

Corresponding with patients/clients via social media platforms present a unique set of issues, including:

- Preserving confidentiality;
- Maintaining professional boundaries;
- Professionalism concerns; and
- Adhering to standards of care.

Most, if not all, social media platform content is public by default. As such, when accessing or using any social media platforms to communicate with and about patients/clients, it is critical to determine the degree of privacy and security available within that medium to ensure compliance with state/federal laws. Thus, in order to protect confidentiality and preserve boundaries, you need to change and customize each platform's privacy settings, to limit who sees content or posts information about you. Patients/clients should not be included in your personal online interactions.

As with written or verbal communication, when communicating electronically, you are the guardian of your client/patients' confidentiality, and potentially liable for any breaches of confidentiality. Remember too, that any clinical/administrative employees must also be educated regarding communicating electronically with patients/clients. For example, consider a situation where your office assistant dealt with a difficult client/patient and later that day posts on Facebook about his/her interaction with them. Although you may not have interacted with the patient/client directly, may not have been in the office at the time, and may not have observed the interaction, these communications and postings could expose you to vicarious liability under the law.



Securing Mobile Devices

Electronic communications often occur through mobile devices. Although not an exhaustive list, if using a mobile device to correspond with patients/clients, particularly when storing PHI, keep the following risk management tips in mind:

- Use encryption when transmitting PHI electronically.
- Ensure ability to remotely erase/disable the device if stolen or misplaced.
- Password protect email systems and portable devices.
- Do not share usernames/passwords.
- Enable all available security features/updates. This includes firewalls and anti-virus software and any encryption capabilities for your device.
- Do not use file sharing applications.
- Configure web accounts to use secure connections ("HTTPS" or "SSL").
- Maintain physical control of devices.
- Avoid joining unknown "Wi-Fi" networks and using public "Wi-Fi hotspots."
- Delete all information before disposing of the device.

Conclusion

Communicating electronically with patients/clients poses benefits and challenges, particularly as new devices, technologies and platforms continue to emerge. Prior to communicating electronically, implement policies and procedures designed to safeguard confidentiality, maintain professional boundaries and adhere to applicable standards of care. Should you have questions about these issues, contact your Risk Management Consultant or local legal counsel for advice.

[1] Pew Research Center, *"Internet, social media use and device ownership in U.S. have plateaued after years of growth,"* (September 28, 2018).

[2] American College of Physicians and the Federation of State Medical Boards, *"Online Medical Professionalism: Patient and Public Relationships: Policy Statement,"* (April 16, 2013).

[3] 45 CFR Part 160 and Part 164, Subparts A and C.

[4] HHS, FAQ's, "What is Encryption?" (https://www.hhs.gov/hipaa/for-professionals/faq/encryption/index.html).