Andrew N. Pollak, MD
CHAIR

MARYLAND HEALTH CARE COMMISSION

Ben Steffen
EXECUTIVE DIRECTOR

Understanding Consumer Privacy in Virtual Care

Have you interacted with a health care provider virtually using telecommunications technologies, such as mobile applications, email, text, video, or the web? If you have or are planning to, you might be wondering if it's safe. This flyer explains how the security and confidentiality of your personal health information is protected (as required by federal[1] and State[2] laws) as well as practical steps you can take.

Overview

As with everything we do online, there are risks to the privacy and security of our personal information that is collected, stored, and shared electronically.

It's important to recognize the difference between health information and other information shared on the internet. Health information is personal and recorded in an electronic health record or "EHR" (the electronic equivalent of a paper chart).[3] This information is protected by laws like the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[4, 5] HIPAA is a federal law consisting of rules to safeguard protected health information or "PHI."[6] Providers must comply with HIPAA to protect PHI whether in paper or electronic form.[7] In general, HIPAA rules require:[8]

- Only people authorized to view or use your health information, like a provider, have access, and only for specific purposes, like diagnosing or treating your health issue; and
- Individually identifiable information be encrypted (i.e., coded so that only someone authorized to receive the information can decipher it) and shared through secure communication channels and technologies.[9]

Other information (e.g., what you post on social media) is not protected the same way. Be mindful of mobile applications that you voluntarily download

[1] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that sets rules for who can look at and receive your medical information and prevents unauthorized use of your health information. More information is available at: www.hhs.gov/hipaa/for-individuals/faq/index.html.
[2] Maryland law builds on federal protections and places certain requirements and restrictions pertaining to the confidentiality, maintenance, use, disclosure, patient access, and scope of health information in any form (oral, written, and electronic) collected by providers and health organizations. More information is available at: codes.findlaw.com/md/health-general/md-code-health-gen-sect-4-302.html.
[3] Practice Fusion, Is my health data safe on the Internet? November 2011. Available at: www.practicefusion.com/blog/is-my-health-data-safe-on-the-internet/.
[4] Information about laws and regulations that affect who has access to your health information is available at: www.healthit.gov/topic/health-information-privacy-law-and-policy.
[5] Industry standards and best practices further guide how providers handle patient health information. Organizations like the American Medical Association, the American Health Information Management Association, and agencies like HHS offer guidance and best practices to health care providers for safeguarding patient health information.
[6] PHI is information about a patient's health status, health care, or payment for health care that is created or collected by health care professionals and organizations that can be used to identify the individual patient. More information is available at: www.healthit.gov/topic/your-health-information-security.
[7] Privacy Rights Clearinghouse, Protecting Health Information: the HIPAA Security and Breach Notification Rules. Available at: privacyrights.org/consumer-guides/protecting-health-information-hipaa-security-and-breach-notification-rules#:~:text=Are%20there%20any%20rules%20for,(PHI)%20in%20any%20format.
[8] HIPAAnswers, What is HIPAA compliant telemedicine? November 2017. Available at: www.hipaanswers.com/what-is-hipaa-compliant-telemedicine/.
[9] In general, telehealth technology is designed to meet HIPAA requirements. Many remote electronic communication products being used during the COVID-19 pandemic also have security features. More information is available at: healthitsecurity.com/news/ocr-clarifies-hipaa-liability-on-telehealth-use-during-covid-19.

and other third party web sites.[10] If you receive an ad or other targeted messaging about health conditions, it's typically generated from a place where the condition was self-disclosed (not from an EHR), such as signing up for a subscription, or entering information on a self-help application or web site.

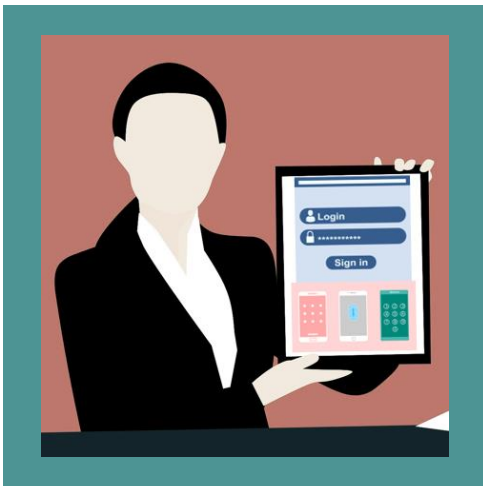
How Do Providers Protect My Health Information?

COVID-19 made telehealth an indispensable part of the health care. In March 2020, many providers began offering video visits (similar to Skype or FaceTime) as a safe and convenient alternative to in-person care. Video visits sometimes require you to set up an online account and submit information on your medical history, pharmacy, primary care provider, insurance, and credit card for billing purposes; you may also need to download and log in to a mobile application so the provider can see and hear you. Only the provider and anyone observing the visit with your consent will be able to access your health information.

Protecting your privacy is mainly the provider's responsibility. HIPPA-compliant technology[11] is used for the collection, display, storing, processing, and transmission of PHI. The following are some actions providers take to mitigate risk:[12, 13]

- *Educate Practice Staff* – Includes training and frequent reminders on how to protect PHI, such as logging off of a system when walking away and recognizing suspicious and unsolicited emails that attempt to trick staff into clicking a link to a fraudulent website and providing credentials (e.g., username or password).
- *Limit Access* – Encryption and password-protecting computers and mobile devices, including cell phones, tablets and laptops, keeps health information secure and accessible to only authorized individuals.
- *Secure Technology* – Install security software to protect health information and guard against viruses and malicious software (or malware) that can damage systems.

What Steps Can I Take to Protect My Health Information?



Here are some steps you can take to ensure your privacy. These include:[14]

- *Guard Your Information* – Don't provide personal information over the phone, through the mail, or over the internet unless you've confirmed the identity of the person requesting the information.
- *Ask Questions* – Ask your provider how they will communicate and what information they might request before and after a video visit.

[10] Morgan Lewis, Health Apps and HIPAA: OCR Publishes New Guidance for Health App Developers, March 2016. Available at: www.morganlewis.com/pubs/health-apps-and-hipaa-ocr-publishes-new-guidance-for-health-app-developers#:~:text=On%20February%2011%2C%20the%20Department%20of%20Health%20and,collect%2C%20store%2C%20manage%2C%20organize%2C%20or%20transmit%20health%20information.
[11] HIPAA includes specifications for specific capabilities of technology to protect PHI. More information is available at: www.hipaaguide.net/hipaa-compliant-website.
[12] American Medical Association, How to improve your cybersecurity practices, 2017. Available at: www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/cybersecurity-improvements.pdf.
[13] American Medical Association, Steps Forward, Adopting Telemedicine in Practice, 2018. Available at: www.telemedecine-360.com/wp-content/uploads/2019/03/2018-AMA-Adopting-Telemedicine-in-Practice.pdf.
[14] HealthIT.gov, Protecting Your Privacy & Security. Available at: www.healthit.gov/topic/protecting-your-privacy-security.

- *Use a Private Space* – A space free from interruption prevents others from overhearing your interaction with a provider. Using headphones is recommended.
- *Send Information Securely* – If submitting information online, look for the lock icon on the status bar of your internet browser; this means the information will be safely transmitted.
- *Keep Passwords Private* – Use strong passwords or passphrases[15] and do not share them or display them anywhere someone else might have access.
- *Use Security Software* – Install anti-virus and anti-spyware software to protect your personal device. Set preferences to install updates regularly.
- *Be Alert to Phishing Attempts*[16] – Avoid clicking suspicious links or opening attachments in email unless you know or can confirm the sender.

Additional Resources

HIPAA FAQ for Individuals
www.hhs.gov/hipaa/for-individuals/faq/index.html

Podcast – Telehealth: 5 Things You Need to Know
nutritionmadeeasy.giantfood.libsynpro.com/telehealth-5-things-you-need-to-know

Your Health Information Security
www.healthit.gov/topic/your-health-information-security

What You Can Do To Protect Your Health Information
www.healthit.gov/topic/privacy-security/what-you-can-do-protect-your-health-information

Contact Alana Sutherland,
MHCC Program Manager, at:

alana.sutherland@maryland.gov

(410) 764-3330

Connect with us on Twitter and Facebook

@MHCCMD

[15] For more information on how to build a strong password see: www.healthit.gov/topic/privacy-security-and-hipaa/how-can-you-protect-and-secure-health-information-when-using-mobile-device/1-use-password-or-other-user-authentication.

[16] Phishing emails are used by hackers to gain access to your information by tricking you into clicking on a link or opening an attachment in an email. More information is available at: www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.