Andrew N. Pollak, MD
CHAIR

MARYLAND HEALTH CARE COMMISSION

Ben Steffen
EXECUTIVE DIRECTOR

Safeguarding Privacy and Security in Telehealth
Tips to Keep Your Practice Safe

Overview

The COVID-19 public health emergency altered a lot of ways we do business. A notable change in health care has been the expanded use of telehealth. Telehealth is a tool that leverages information technology (IT) to deliver patient care and other health services in a safe and convenient way. It allows practices to reach patients in new ways, which has helped them remain operational during the public health emergency.

It's important for practices to be mindful of IT-related risks involved with collecting, processing, transmitting, and storing electronic data. Risks range from loss of equipment and phishing attacks to ransomware that results in data loss or damage.[1] Use of telehealth increases risks to privacy and security as the IT vendor, practice, and patient must work together.[2] For this reason, practices should implement appropriate security measures to protect patient data, such as encryption (both in transit and at rest), authentication, and access control.[3]

What's phishing?

Phishing is an attempt to trick practice staff into giving out valuable information, such as credentials, insurance information, or medical records. These emails often appear to come from a legitimate source (e.g., accounts payable), which makes them harder to detect.[4] Phishing is a common way hackers deploy ransomware by getting a victim to click on a malicious link that denies access to patient records and other electronic systems until a ransom is paid.[5]

HIPAA and Other Considerations

Telehealth does not alter a provider's obligations under HIPAA[6] – the same requirements apply as in-person visits. Use of HIPAA-compliant technology can help a practice meet its compliance obligations through certain features, such as encryption or use of strong passwords.[7] However, these examples do not substitute for an organized, well-documented set of security practices.[8]

HIPAA requires practices and their business associates[9] (BAs) to implement reasonable and appropriate safeguards

[1] American Academy of Anti-Aging Medicine, *Telehealth IT Security: What Clinicians Need to Know & Tips to Keep Your Practice Secure*, May 2020. Available at: blog.a4m.com/telehealth-it-security-what-clinicians-need-to-know-tips-to-keep-your-practice-secure/.
[2] Clearwater Healthcare Cyber Risk Management, *Telehealth Insecurity: Evaluating Emerging Threats and Risk Response*, May 2020. Available at: www.clearwatercompliance.com/blog/telehealth-insecurity-evaluating-emerging-threats-and-risk-response/.
[3] Luxsci, *Telehealth: The Benefits & The Risks*, April 2019. Available at: www.luxsci.com/blog/telehealth-the-benefits-the-risks.html.
[4] Medical Economics, *The Growing Cyber Threat to Physician Practices*, May 2019. Available at: www.medicaleconomics.com/view/growing-cyber-threat-physician-practices.
[5] U.S. Department of Health & Human Services, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. Available at: www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf.
[6] The Health Insurance Portability and Accountability Act of 1996 contains standards for the protection of PHI. More information is available at: www.hhs.gov/hipaa/index.html.
[7] A strong password should use a minimum of six characters and include a combination of upper and lower case letters, numbers, and special characters. More information is available at: 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.
[8] Center for Connected Health Policy, *HIPAA and Telehealth*. Available at: www.cchpca.org/sites/default/files/2018-09/HIPAA%20and%20Telehealth.pdf.
[9] A business associate is a person or entity that performs functions that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. More information is available at: www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

(i.e., administrative, physical, and technical controls).[10] A business associate agreement (BAA)[11] is often required with an IT vendor. Practices must also consider applicable state law(s) (e.g., obligations for encryption, consent, and breach notification) as they may be liable for insufficient security safeguards or unauthorized access of protected health information (PHI).[12]

In March 2020, the U.S. Department of Health and Human Services, Office for Civil Rights announced the relaxation of some enforcement activities during the COVID-19 public health emergency. Use of popular, non-public facing video applications (e.g., Skype, Zoom, Apple FaceTime, and Facebook Messenger video chat) is temporarily permitted without risk of penalty for non-compliance with HIPAA. Practices seeking additional privacy protections for telehealth should use vendors that are HIPAA-compliant and will enter into BAAs. [13]

Practice Tips

Any data transferred over the internet runs the risk of interception by threat actors. This includes use of telehealth to communicate with patients remotely and transmit their biometric data through remote monitoring devices. Cybersecurity refers to preventative measures a practice can take to protect data from being stolen or compromised. Many practices already take steps to protect themselves and their patients. The following are some key considerations for telehealth.

Educate practice staff

Everyone has a role to play in cybersecurity. Proper guidance to practice staff is essential to increase their awareness about how to recognize security threats; nearly 95 percent of data breaches stem from employee error.[14] Training practice staff should minimally cover how to safeguard PHI and proper data handling procedures. This includes topics, such as:

- Common cyber-attack techniques, like phishing;
- Remote work policies, including permitted forms for remote access (e.g., using a virtual private network or "VPN" connection[15]) and personal device security (e.g., segregation of personal and health care applications and data)[16]; and
- Operating system and security updates.

Initial training should occur, followed by periodic refresher training (at least annually). Training should also be initiated if a change is made to telehealth policies, procedures, or systems.[17, 18]

[10] Maryland Health Care Commission, *The Health Insurance Portability and Accountability Act of 1996,* April 2019. Available at: mhcc.maryland.gov/mhcc/pages/hit/hit_hipaa/hit_hipaa.aspx.
[11] A BAA ensures that the BA(s) will appropriately safeguard PHI by clarifying and limiting permissible uses and disclosures of PHI by the BA. More information is available at: www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.
[12] Quarles & Brady, *Privacy and Security Considerations for Telehealth Use During COVID-19 Public Health Emergency*, March 2020. Available at: www.quarles.com/publications/privacy-and-security-considerations-for-telehealth-use-during-covid-19-public-health-emergency/.
[13] U.S. Department of Health & Human Services, *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, March 2020. Available at: www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html
[14] See n.1, *Supra*.
[15] A VPN connection encrypts data to and from the computer or mobile device and is not readable if it is intercepted.
[16] Health IT Security, *Must-Have Telehealth Remote Work Privacy and Security for COVID-19*, March 2020. Available at: healthitsecurity.com/news/must-have-telehealth-remote-work-privacy-and-security-for-covid-19.
[17] The Office of the National Coordinator for Health Information Technology, *Guide to Privacy and Security of Electronic Health Information*, April 2015. Available at: www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
[18] American Society for Health Care Risk Management, *Telemedicine Risk Management Considerations*. Available at: www.ashrm.org/sites/default/files/ashrm/TELEMEDICINE-WHITE-PAPER.pdf.

Sign a BAA with vendor(s) that handle PHI

BAAs protect your practice from liability in the event of a breach by outlining vendor roles and responsibilities, including appropriate uses and disclosures of PHI, and the implementation of certain features and technical specifications using HIPAA-compliant technology.[19, 20]

Install system updates timely

Anti-virus software protects patient data.[21] Automatic "patching" is an easy way to address known vulnerabilities. Consider implementing updates at least weekly.[22, 23]

Minimize and detect unauthorized access

Consider the following access control options:

- Restrict access to permissions based on staff roles
- Encrypt PHI to make it unreadable without a key or password[24]
- Have the capability to remotely disable or wipe IT devices in the event of loss or theft[25]
- Regularly audit data activities to verify users and data accessed, and detect potentially malicious or careless behaviors (e.g., provider looking at health information of individuals not in patient panel)[26]

Invest in cybersecurity insurance

In the event of a breach, insurance may offset the cost of an investigation, HIPAA fines, legal support, and patient notification and credit monitoring.[27]

Additional Resources

- MHCC Telehealth Virtual Resource Center

  mhcc.maryland.gov/mhcc/Pages/hit/hit_telemedicine/hit_telemedicine_virtual_resource.aspx

- MHCC Cybersecurity Self-Assessment Readiness Tool

  mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Cybersecurity_Self-Assessment_Tool.pdf

- Health IT Privacy and Security Resources for Providers

  www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers

- Privacy and Security Training Games

  www.healthit.gov/topic/privacy-security-and-hipaa/privacy-security-training-games

- Top 10 Tips for Cybersecurity in Health Care

  www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

- Checklist: Protecting Office Computers in Medical Practices Against Cyberattacks

  https://www.ama-assn.org/system/files/2020-04/computer-security-checklist.pdf

Questions?

Contact us at: mhcc.telehealth@maryland.gov

[19] InTouchHealth, *5 Things to Look for in a Telehealth Vendor*. Available at: intouchhealth.com/5-things-to-look-for-in-a-telehealth-vendor/.
[20] The Health Information Trust Alliance (HITRUST) Common Security Framework certification is a widely use industry standard. More information is available at: hitrustalliance.net/benefits-hitrust-certification/.
[21] American Medical Association, *What Physicians Need to Know: Working from home during COVID-19 Pandemic*, 2020. Available at: www.ama-assn.org/system/files/2020-04/cybersecurity-work-from-home-covid-19.pdf.
[22] HealthIT.gov, *Top 10 Tips for Cybersecurity in Health Care*. Available at: www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf.
[23] American Medical Association, *What Physicians Need to Know: Working from home during COVID-19 Pandemic*, 2020. Available at: www.ama-assn.org/system/files/2020-04/cybersecurity-work-from-home-covid-19.pdf.
[24] Encryption is a method of converting an original message of regular text into encoded text. More information is available at: www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
[25] American Telemedicine Association, *Core Operational Guidelines for Telehealth Services Involving Provider-Patient Interactions*, October 2018. Available at: www.americantelemed.org/resources/core-operational-guidelines-for-telehealth-services-involving-provider-patient-interactions/.
[26] Coding Leader, *Telehealth Security: Protect Patient Information and Your Practice*, June 2018. Available at: healthcare.trainingleader.com/2018/06/telehealth-security-protect-patient-information-and-your-practice/.
[27] Insureon, *Cyber Liability Insurance for Healthcare Professionals.* Available at: www.insureon.com/healthcare-professionals-business-insurance/cyber-liability.