HAVE YOU HEARD ABOUT TELEHEALTH SECURITY?

WHAT IS TELEHEALTH?

Telehealth is the use of electronic information and telecommunications to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration. Technologies include videoconferencing, the internet, store-and-forward imaging, streaming media, and terrestrial and wireless communications.

SOURCE: https://www.hrsa.gov/rural-health/telehealth

TELEHEALTH CYBERSECURITY IMPLICATIONS

Telehealth relies on technology and telecommunications to be effective. Unfortunately since it acts as any other healthcare network or IT system, telehealth is vulnerable to similar types of cyber-attacks. Telehealth technologies are vulnerable to data loss and theft, ransomware, phishing, etc. To ensure patient safety, healthcare organizations need to implement cybersecurity policies and infrastructure that allows for secure communications between provider and patient. Cybersecurity policies is one of the ten best practices outlined by the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

SOURCE: http://cliniciantoday.com/why-you-must-consider-cyber-security-for-telehealth/

BY THE NUMBERS

79% of patients said that scheduling a telemedicine follow-up visit was more convenient than arranging an in-person follow-up, according to Massachussetts General Hospital.

Source: American Journal of Managed Care (2019)

More than one-half of all U.S. hospitals have a telehealth program.

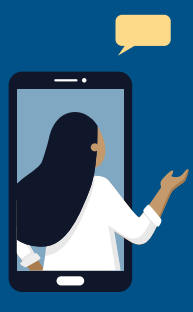
Source: The American Telemedicine Association (2019)

42.5% In a survey of health system clinicians, **42.5%** say they use telehealth to fill in gaps in care delivery.

Source: Fierce Healthcare (2020)

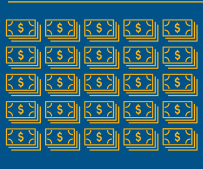
↑340% Clinician adoption has increased by **340%**, according to a 2019 survey of 800 physicians.

Source: American Well (2019)



Telemedicine users are very satisfied with the service. A 2019 survey found that **79% of respondents perceived telemedicine as more convenient** in terms of scheduling, **83% felt that the care was as good or better** than an in-person visit, and **66% felt personally connected to their telehealth practitioner.**

Source: American Journal of Managed Care (2019)



$125 The average cost per in-person visit is $125.

$45 The average cost for a telehealth visit is around $45.

Source: U.S. News & World Report (2018)

HEALTH INDUSTRY CYBERSECURITY PRACTICES:

Managing Threats and Protecting Patients

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication aims to raise awareness, provide vetted cybersecurity practices, and moves toward consistency in mitigating the current most pertinent cybersecurity threats to the sector. The main document examines cybersecurity threats and vulnerabilities that affect the health industry. Technical volumes 1 & 2 discuss ten cybersecurity practices for small, medium, and large healthcare organizations. Lastly, the resources and templates volume provides additional cybersecurity resources and references.

CLICK HERE TO ACCESS THESE DOCUMENTS.

LOOKING FOR MORE TELEHEALTH CYBERSECURITY INFORMATION?

Check out the below resources from across HHS and HSCC partners!

HHS 405(d) — Aligning Health Care Industry Security Approaches

405(d) aims to enhance cybersecurity and align health industry security approaches by developing best practices and mitigation strategies to attack the most common cyber threats facing the health sector. As telehealth continues to be a common practice throughout the Healthcare and Public Health (HPH) sector it is vital to institute cybersecurity policies to safeguard patient's data when telecommunicating or using telehealth to treat patients. The Health Industry Cybersecurity Practices (HICP) publication outlines the top five cyber threats and the ten cybersecurity practices to combat them. Healthcare organizations should check out HICP to ensure their telehealth networks and devices are cyber secure.

RESOURCES

Health Industry Cybersecurity Practices (HICP)

HICP Technical Volume 1: Cybersecurity Practices for Small Practices

HICP Technical Volume 2: Cybersecurity Practices for Medium/Large Organizations

HHS — Office for Civil Rights

The HHS Office for Civil Rights (OCR) is aware of the health sector's expanding need to offer telehealth to patients in times of crisis. OCR has exercised its enforcement discretion and will waive penalties for HIPAA violations against providers that serve patients via telehealth. As this new policy is being put in place, OCR has released an FAQ sheet to provide guidance on telehealth remote communications.

RESOURCES

Telehealth Discretion Notification

Telehealth FAQ

Telehealth Remote Communications Guidance

DHS — Cybersecurity and Infrastructure Security Agency

The Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to adopt a heightened state of cybersecurity during times of crisis. As healthcare organizations move towards telework and telehealth environments, they should implement an enterprise virtual private network (VPN) solution to connect their employees to their organization's IT network. CISA has detailed out cybersecurity considerations and mitigation recommendations when moving to a telework or telehealth environment.

RESOURCES

Enterprise VPN Security Guidance

HSCC — Healthcare and Public Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group developed a management checklist for organizations to utilize during crises and telework surges. This checklist provides a quick reference for healthcare enterprise management to consider important factors in a teleworking strategy that minimizes downtime and latency while supporting patient care, operational and I.T. security, and supply chain resilience. This checklist also outlines a few tips to ensure secure telehealth and telemedicine during crises.

RESOURCES

Telehealth Checklist

HHS 405(d) Aligning Health Care Industry Security Approaches

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov! Also check out our social media pages: @ask405d on Facebook, Twitter, and Instagram and LinkedIn!