

ARIZONA
TELEMEDICINE
PROGRAM



Securing Telehealth: Information Systems, Devices, Communications, and Practices



Michael Holcomb, BS
Interim Director & Associate Director, Information Technology
mholcomb@telemedicine.arizona.edu



Disclaimer

- Any information related in this presentation is not legal advice and is intended for educational purposes.
- Consultation with qualified cybersecurity and legal professionals is recommended.
- No conflicts of interest to disclose.

Example Types of Telemedicine and Telehealth Communications (selected)

- Video call (Video and audio) consultations
 - provider to patient, provider to provider, multiple provider to patient, provider to multiple patients
 - Real-time medical imaging applications
- Audio only consultations
- Remote auscultation using electronic stethoscopes
 - Remote provider playback of recordings or listening via live streaming
- Tele-eICU
 - Vital signs alerts and trends, remote intensivist directing local care team
- Telestroke
- Diagnostic review of clinical images and data
 - Patient history, medical imaging, lab values and other test results, prescriptions etc.
- Secure messaging
 - Provider to provider, provider to patient
- Remote patient monitoring (RPM)
 - Clinical provider monitors patient metrics such as activity, weight, blood pressure, electrocardiogram, and more
- AI and robotic assisted examination and diagnosis

Why do we need to secure telemedicine and telehealth ?

- Protect patients, the healthcare provider and its business partners
- Good business practice to maintain confidentiality of patient information
- Health Insurance Privacy and Accountability Act (HIPAA) requires implementation of administrative, technical, and physical measures and business associate agreements to safeguard protected health information (PHI). Other federal and state regulations may also apply
- Securing telehealth is not just about maintaining confidentiality.
 - Also very important:
 - Availability of data and technology to conduct telehealth operations
 - Integrity of data used to make patient care decisions via telehealth



COVID-19 HIPAA transition period for telehealth expires

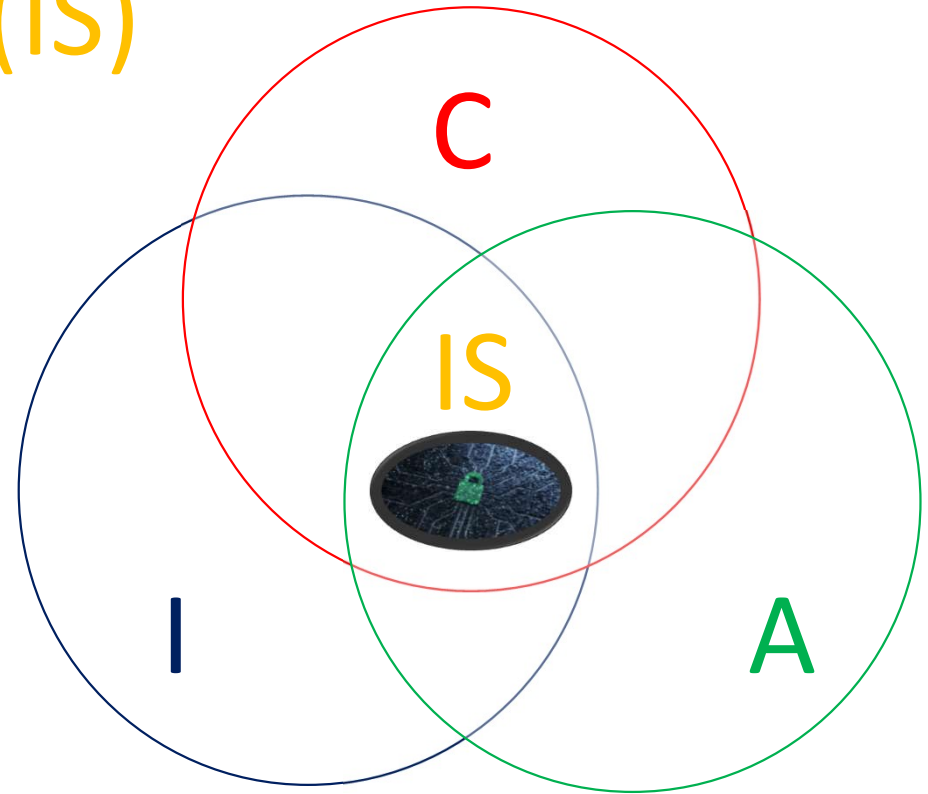
🕒 Aug 09, 2023 - 03:11 PM

“Health care providers must comply with the HIPAA rules with respect to telehealth effective Aug. 9 at 11:59 p.m., when the 90-day enforcement discretion period announced in April expires. The Department of Health and Human Services’ Office for Civil Rights implemented a HIPAA enforcement discretion policy for telehealth during the COVID-19 public health emergency, which ended May 11. This provided enforcement discretion to not impose penalties for HIPAA violations against covered health care providers in connection with their good faith provision of telehealth using non-public facing remote communications technologies during the PHE. Providers then had a 90-day transition period to come into compliance...”

<https://www.aha.org/news/headline/2023-08-09-covid-19-hipaa-transition-period-telehealth-expires>

Information Security (IS)

- Confidentiality (C)
 - Privacy of information is maintained among authorized entities and protected from unauthorized access and use
- Integrity (I)
 - Information is accurate, true, and protected from unauthorized changes
- Availability (A)
 - Information access is reliable and timely for authorized entities when needed



Information Security Triad



- About HHS
- Programs & Services
- Grants & Contracts
- Laws & Regulations

Health Information Privacy



- HIPAA for Individuals
- Filing a Complaint
- HIPAA for Professionals
- Newsroom

HHS > HIPAA Home > For Professionals > The Security Rule > Security Rule Guidance Material

HIPAA for Professionals	
Regulatory Initiatives	
Privacy	+
Security	-
Summary of the Security Rule	
Security Guidance	
Cyber Security Guidance	



Security Rule Guidance Material

In this section, you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information (e-PHI).

<https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>



Health Information Privacy



- HIPAA for Individuals
- Filing a Complaint
- HIPAA for Professionals
- Newsroom

HHS > HIPAA Home > For Professionals > Privacy > Guidance Materials > Guidance: How the HIPAA Rules Per...

HIPAA for Professionals	
Regulatory Initiatives	
Privacy	+
Security	+
Breach Notification	+
Compliance & Enforcement	+
Special Topics	+



Guidance on How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Use Remote Communication Technologies for Audio-Only Telehealth

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html>

2. Do covered health care providers and health plans have to meet the requirements of the HIPAA Security Rule in order to use remote communication technologies to provide audio-only telehealth services?

Yes, in certain circumstances. The HIPAA Security Rule applies to electronic protected health information (ePHI), which is PHI transmitted by, or maintained in, electronic media. ²⁰, ²¹

The HIPAA Security Rule does not apply to audio-only telehealth services provided by a covered entity that is using a standard telephone line, often described as a traditional landline, ²² because the information transmitted is not electronic. Accordingly, a covered entity does not need to apply the Security Rule safeguards to telehealth services that they provide using such traditional landlines (regardless of the type of telephone technology the individual uses).

However, traditional landlines are rapidly being replaced with electronic communication technologies such as Voice over Internet Protocol (VoIP) ²³ and mobile technologies that use electronic media, such as the Internet, intra- and extranets, cellular, and Wi-Fi. ²⁴ The HIPAA Security Rule applies when a covered entity uses such electronic communication technologies. Covered entities using telephone systems that transmit ePHI need to apply the HIPAA Security Rule safeguards to those technologies. Note that an individual receiving telehealth services may use any telephone system they choose and is not bound by the HIPAA Rules when doing so. In addition, a covered entity is not responsible for the privacy or security of individuals' health information once it has been received by the individual's phone or other device.

For example, some current electronic technologies that covered entities use for remote communications that require compliance with the Security Rule, may include:

- Communication applications (apps) on a smartphone or another computing device.
- VoIP technologies.
- Technologies that electronically record or transcribe a telehealth session.
- Messaging services that electronically store audio messages.

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html>

Advertisement

Elevate Your Patient Care With Our Industry-Leading e-Newsletter **Subscribe Now!** **Patient Care**

Billing and collections | Coding and documentation | Concierge Medicine | Malpractice | Patient Relations | Practice Management

SPOTLIGHT-Concierge Medicine 2.0 by Castle Connolly Private Health Partners | Physician Bootcamp | Physician Report

Health care leads cybersecurity breaches for 2022

Feb 7, 2023

Richard Payerchin

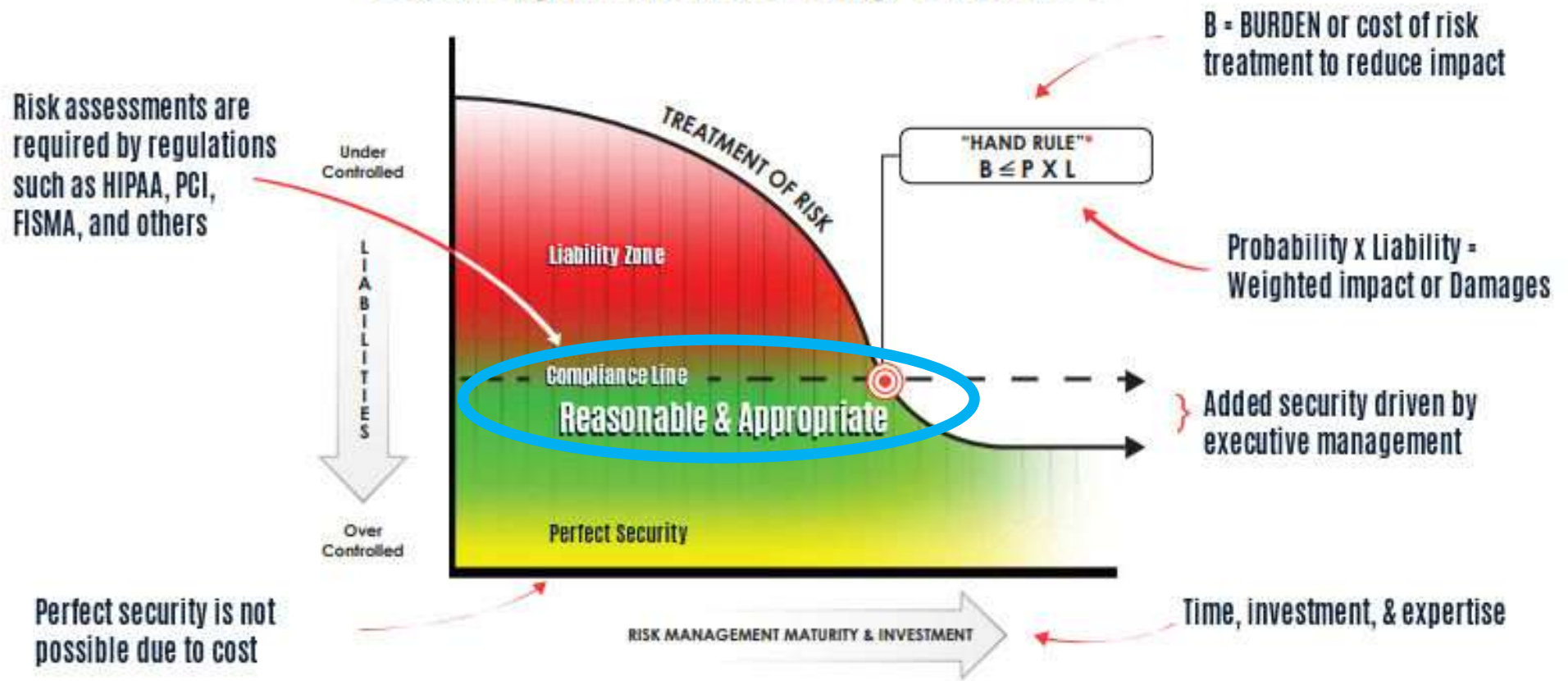
Article



Analyst examines factors that leave industry sectors at risk.

<https://www.medicaleconomics.com/view/health-care-leads-cybersecurity-breaches-for-2022>

Is Your Organization Exercising "Due Care"?



Blog: Halock: Searching for the Meaning of Reasonable Security <https://www.halock.com/hand-rule-managing-upper-limits-security-costs/>

*"Hand Rule" https://en.wikipedia.org/wiki/Calculus_of_negligence

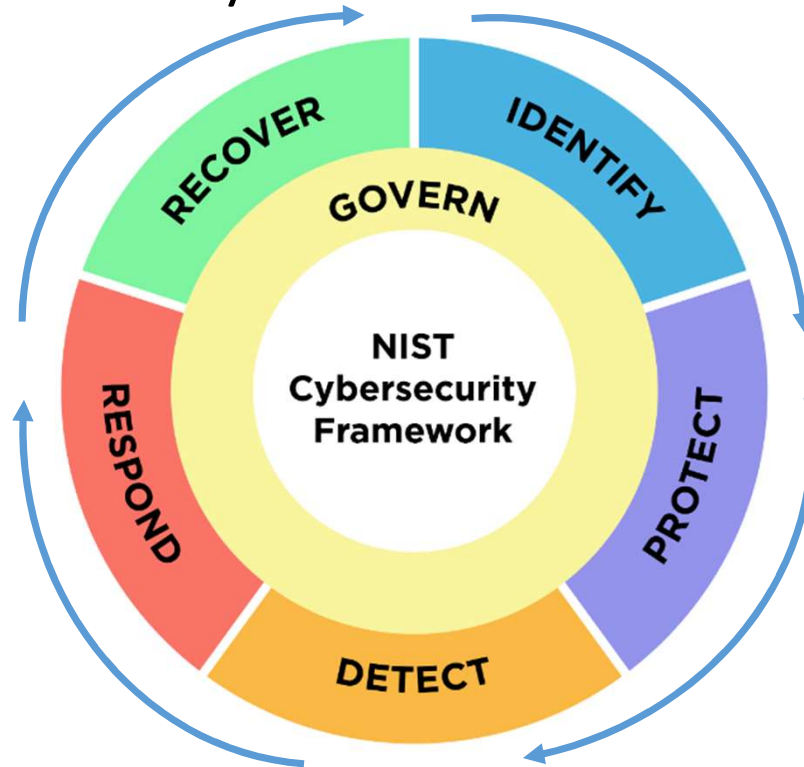
National Institutes of Standards and Technology Cybersecurity Framework



<https://www.nist.gov/cyberframework/online-learning/five-functions>

National Institutes of Standards and Technology Cybersecurity Framework 2.0 (Draft)

“To the five main pillars of a successful cybersecurity program, NIST now has added a sixth, the "govern" function, which emphasizes that cybersecurity is a major source of enterprise risk and a consideration for senior leadership. Credit: N. Hanacek/NIST”



<https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework>

How to build a culture of cybersecurity.

 by Beth Stackpole | Mar 15, 2022

Why It Matters

Technology and training are not enough to safeguard companies against today's litany of cybersecurity attacks. Here's how to infuse safe behavior into corporate culture.

Share 

<https://mitsloan.mit.edu/ideas-made-to-matter/how-to-build-a-culture-cybersecurity>

How to build a culture of cybersecurity

“Make it part of the organization’s fabric”

- Reinforce cybersecurity throughout organizational hierarchy
 - Leadership level
 - Group level
 - Individual level
- Drive culture change with these four steps
 - Make it someone’s job to be the ‘culture owner’
 - Use language that resonates
 - Make cybersecurity part of formal employee evaluation
 - Conduct tabletop exercises and fire drills

<https://mitsloan.mit.edu/ideas-made-to-matter/how-to-build-a-culture-cybersecurity>

Reassessing Your Security Practices

in a Health IT Environment:

A Guide for Small Health Care Practices

TABLE OF CONTENTS

1	INTRODUCTION.....	3
2	INFORMATION SECURITY IN HEALTH CARE.....	4
3	SECURING ELECTRONIC HEALTH INFORMATION IN YOUR HEALTH IT ENVIRONMENT	6
4	RESOURCES.....	9

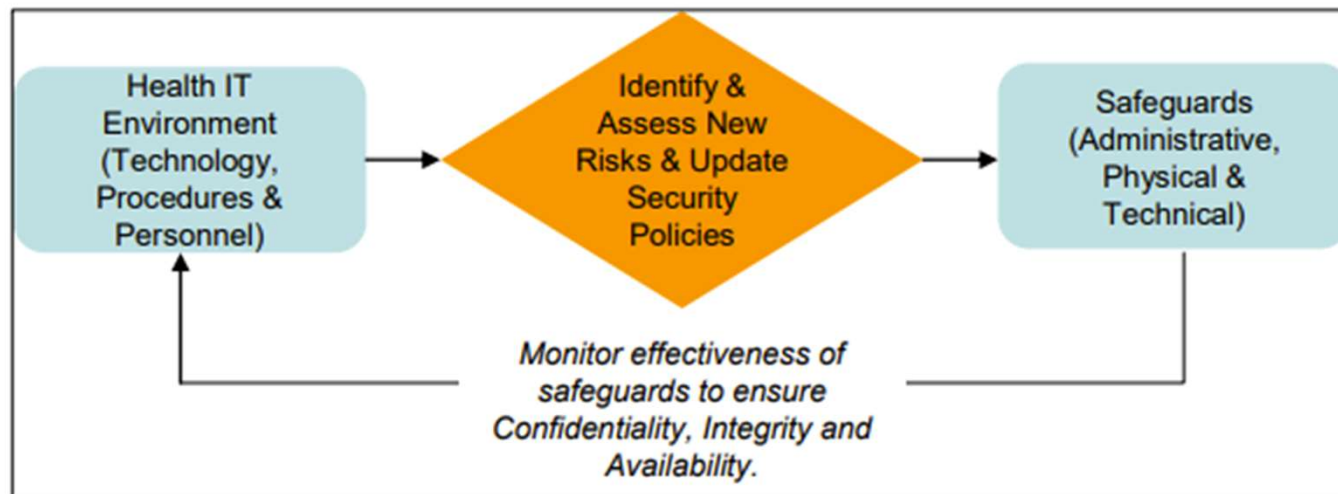


Figure 1: Health Information Security Requires Continual Assessment of Risks to Electronic Health Information

<https://www.hhs.gov/sites/default/files/small-practice-security-guide-1.pdf>



NSA'S Top Ten Cybersecurity Mitigation Strategies

NSA's Top Ten Mitigation Strategies counter a broad range of exploitation techniques used by Advanced Persistent Threat (APT) actors. NSA's mitigations set priorities for enterprise organizations to minimize mission impact. The mitigations also build upon the NIST Cybersecurity Framework functions to manage cybersecurity risk and promote a defense-in-depth security posture. The mitigation strategies are ranked by effectiveness against known APT tactics. Additional strategies and best practices will be required to mitigate the occurrence of new tactics.

The cybersecurity functions are keyed as: ■ Identify, ■ Protect, ■ Detect, ■ Respond, ■ Recover

1. Update and Upgrade Software Immediately

■ Identify, ■ Protect

Apply all available software updates, automate the process to the extent possible, and use an update service provided directly from the vendor. Automation is necessary because threat actors study patches and create exploits, often soon after a patch is released. These "N-day" exploits can be as damaging as a zero-day. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to assure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender's patch cycle.

2. Defend Privileges and Accounts

■ Identify, ■ Protect

Assign privileges based on risk exposure and as required to maintain operations. Use a Privileged Access Management (PAM) solution to automate credential management and fine-grained access control. Another way to manage privilege is through tiered administrative access in which each higher tier provides additional access, but is limited to fewer personnel. Create procedures to securely reset credentials (e.g., passwords, tokens, tickets). Privileged accounts and services must be controlled because threat actors continue to target administrator credentials to access high-value assets, and to move laterally through the network.

3. Enforce Signed Software Execution Policies

■ Protect, ■ Detect

Use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. Maintain a list of trusted certificates to prevent and detect the use and injection of illegitimate executables. Execution policies, when used in conjunction with a secure boot capability, can assure system integrity. Application Whitelisting should be used with signed software execution policies to provide greater control. Allowing unsigned software enables threat actors to gain a foothold and establish persistence through embedded malicious code.

4. Exercise a System Recovery Plan

■ Identify, ■ Respond, ■ Recover

Create, review, and exercise a system recovery plan to ensure the restoration of data as part of a comprehensive disaster recovery strategy. The plan must protect critical data, configurations, and logs to ensure continuity of operations due to unexpected events. For additional protection, backups should be encrypted, stored offsite, offline when possible, and support complete recovery and reconstitution of systems and devices. Perform periodic testing and evaluate the backup plan. Update the plan as necessary to accommodate the ever-changing network environment. A recovery plan is a necessary mitigation for natural disasters as well as malicious threats including ransomware.

5. Actively Manage Systems and Configurations

■ Identify, ■ Protect

Take inventory of network devices and software. Remove unwanted, unneeded or unexpected hardware and software from the network. Starting from a known baseline reduces the attack surface and establishes control of the operational environment. Thereafter, actively manage devices, applications, operating systems, and security configurations. Active enterprise management ensures that systems can adapt to dynamic threat environments while scaling and streamlining administrative operations.

<https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf>



CYBERSECURITY INFORMATION



6. Continuously Hunt for Network Intrusions

■ Detect, ■ Respond, ■ Recover

Take proactive steps to detect, contain, and remove any malicious presence within the network. Enterprise organizations should assume that a compromise has taken place and use dedicated teams to continuously seek out, contain, and remove threat actors within the network. Passive detection mechanisms, such as logs, Security Information and Event Management (SIEM) products, Endpoint Detection and Response (EDR) solutions, and other data analytic capabilities are invaluable tools to find malicious or anomalous behaviors. Active pursuits should also include hunt operations and penetration testing using well documented incident response procedures to address any discovered breaches in security. Establishing proactive steps will transition the organization beyond basic detection methods, enabling real-time threat detection and remediation using a continuous monitoring and mitigation strategy.

7. Leverage Modern Hardware Security Features

■ Identify, ■ Protect

Use hardware security features like Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Platform Module (TPM), and hardware virtualization. Schedule older devices for a hardware refresh. Modern hardware features increase the integrity of the boot process, provide system attestation, and support features for high-risk application containment. Using a modern operating system on outdated hardware results in a reduced ability to protect the system, critical data, and user credentials from threat actors.

8. Segregate Networks Using Application-Aware Defenses

■ Protect, ■ Detect

Segregate critical networks and services. Deploy application-aware network defenses to block improperly formed traffic and restrict content, according to policy and legal authorizations. Traditional intrusion detection based on known-bad signatures is quickly decreasing in effectiveness due to encryption and obfuscation techniques. Threat actors hide malicious actions and remove data over common protocols, making the need for sophisticated, application-aware defensive mechanisms critical for modern network defenses.

9. Integrate Threat Reputation Services

■ Protect, ■ Detect

Leverage multi-sourced threat reputation services for files, DNS, URLs, IPs, and email addresses. Reputation services assist in the detection and prevention of malicious events and allow for rapid global responses to threats, a reduction of exposure from known threats, and provide access to a much larger threat analysis and tipping capability than an organization can provide on its own. Emerging threats, whether targeted or global campaigns, occur faster than most organizations can handle, resulting in poor coverage of new threats. Multi-source reputation and information sharing services can provide a more timely and effective security posture against dynamic threat actors.

10. Transition to Multi-Factor Authentication

■ Identify, ■ Protect

Prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets. Physical token-based authentication systems should be used to supplement knowledge-based factors such as passwords and PINs. Organizations should migrate away from single factor authentication, such as password-based systems, which are subject to poor user choices and susceptible to credential theft, forgery, and reuse across multiple systems.

Disclaimer of Warranties and Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact Information

Client Requirements and General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov

<https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf>



Jill McKeon

Associate Editor
jmckeon@xtelligentmedia.com

Biggest Healthcare Data Breaches Reported This Year, So Far

More than 39 million individuals have been impacted by healthcare data breaches reported in the first half of 2023 alone.

“...CEREBRAL: 3,179,835 INDIVIDUALS IMPACTED

Online mental healthcare platform Cerebral [notified](#) more than 3.1 million users of a data breach that stemmed from its use of tracking pixels. As previously reported, several United States senators sent [letters to telehealth companies](#) in February, including Cerebral, to address concerns over their health data privacy practices.

Specifically, the Senators took issue with [reports](#) that these companies have been tracking their customers’ sensitive health information and sharing it with third-party advertisers [such as Meta](#) and Google...”

<https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far>



Jill McKeon

Associate Editor
jmckeon@xtelligentmedia.com

Biggest Healthcare Data Breaches Reported This Year, So Far

More than 39 million individuals have been impacted by healthcare data breaches reported in the first half of 2023 alone.

“...Cerebral implemented these technologies when it began operations in October 2019 until it launched a review of its data sharing practices a few years later. On January 3, 2023, Cerebral determined that it had disclosed protected health information (PHI) to certain subcontractors “without having obtained HIPAA-required assurances.”

“If an individual created a Cerebral account, the information disclosed may have included name, phone number, email address, date of birth, IP address, Cerebral client ID number, and other demographic or information,” the notice stated.

“If, in addition to creating a Cerebral account, an individual also completed any portion of Cerebral’s online mental health self-assessment, the information disclosed may also have included the service the individual selected, assessment responses, and certain associated health information.”

Other telehealth companies have faced **enforcement actions** from the Federal Trade Commission (FTC), showing that the commission is committed to cracking down on improper health data privacy and security practices...”

<https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far>

FTC fines GoodRx for unauthorized sharing of health data

By FRANK BAJAK February 1, 2023



Click to copy

In a first-of-its-kind enforcement, the Federal Trade Commission has imposed a \$1.5 million penalty on telehealth and prescription drug discount provider GoodRx Holdings Inc. for sharing users' personal health data with Facebook, Google and other third parties without their consent.

<https://apnews.com/article/technology-politics-california-health-prescription-drugs-5934cea79a747ae869c63267a4acb561>



Jill McKeon

Associate Editor
jmckeon@xtelligentmedia.com

How FTC Enforcement Actions Will Impact Telehealth Data Privacy

Recent high-profile settlements against telehealth companies show that the FTC is willing to enforce its Health Breach Notification Rule and hold entities accountable for noncompliance.

“...Both GoodRx and BetterHelp faced allegations of improper health data sharing and agreed to monetary settlements of \$1.5 million and \$7.8 million, respectively. Beyond the monetary settlements and corrective actions ordered by the FTC, these settlements sent a signal to other telehealth providers about what the FTC will and will not tolerate when it comes to health data privacy...”

“...The Health Breach Notification Rule requires vendors of personal health records and other entities to alert the FTC, consumers, and in some cases the media when a personal health record data breach occurs.

The FTC notably specified that a data breach “is not limited to cybersecurity intrusions or nefarious behavior.” Instances of unauthorized access, such as an entity sharing health information without an individual’s permission, also triggers notification obligations...”

<https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy>



HEALTH
IT SECURITY
xtelligent HEALTHCARE MEDIA



Jill McKeon

Associate Editor
jmckeon@xtelligentmedia.com

How FTC Enforcement Actions Will Impact Telehealth Data Privacy

Recent high-profile settlements against telehealth companies show that the FTC is willing to enforce its Health Breach Notification Rule and hold entities accountable for noncompliance.

“...Specifically, GoodRx, a telemedicine and prescription drug discount provider, allegedly “violated the FTC Act by sharing sensitive personal health information for years with advertising companies and platforms—contrary to its privacy promises—and failed to report these unauthorized disclosures,” the FTC stated.

The company allegedly leveraged third-party tracking pixels and “plug and play” software development kits from companies like Facebook, Google, Criteo, Branch, and Twilio that supposedly gathered sensitive data and used it for advertising purposes, the FTC stated...”

<https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy>

FTC and US Department of HHS Office for Civil Rights Joint Letter to ~130 hospital systems July 20, 2023



July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,¹ news reports,² FTC enforcement actions,³ and an OCR bulletin⁴ have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf



[Home](#) / [News and Events](#) / [News](#) / [Press Releases](#)

For Release

FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule

Proposed changes would underscore the rule's applicability to health apps and other evolving technologies

May 18, 2023



<https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule>

Telehealth platform Doxy.me fixing issue that exposed patient data

Katie Adams - Monday, December 13th, 2021



Telehealth platform Doxy.me said it is resolving an issue that gave three third-party companies access to the names of patients' providers, *CyberScoop* reported Dec. 10.

CyberScoop found that Doxy.me, which is used by more than 1 million providers worldwide, was sharing IP addresses and unique device identification numbers with Google, Facebook and marketing software company HubSpot.

When patients clicked the link to enter Doxy.me's virtual waiting room, they were often clicking a link that contained the name of their provider. *CyberScoop's* investigation found that Doxy.me took measures to remove provider names from the URLs it sent to third parties, but the third parties used technical loopholes to view the full URLs.

<https://www.beckershospitalreview.com/cybersecurity/telehealth-platform-doxy-me-fixing-issue-that-exposed-patient-data.html>

Telehealth: Visit Metacommunications and Metadata

- Data communicated about the telehealth visit
 - Email, text or voice messages containing PII such as scheduling messages
 - Direct links to telehealth visit session
 - Is the same link used for more than one patient?
 - Can someone else who has the link intrude on a live telehealth visit?
- Data logged about the telehealth visit
 - PII or PHI such as patient name, email address, ip address, etc.
 - Is the telehealth visit recorded?
 - By provider?
 - By patient?

Breach of Telehealth App Babylon Health Raises Privacy Concerns

While Babylon Health is UK-based, its recent breach that allowed patients to view appointments of other patients raises a host of privacy concerns in light of telehealth expansion in the US.



 By Jessica Davis



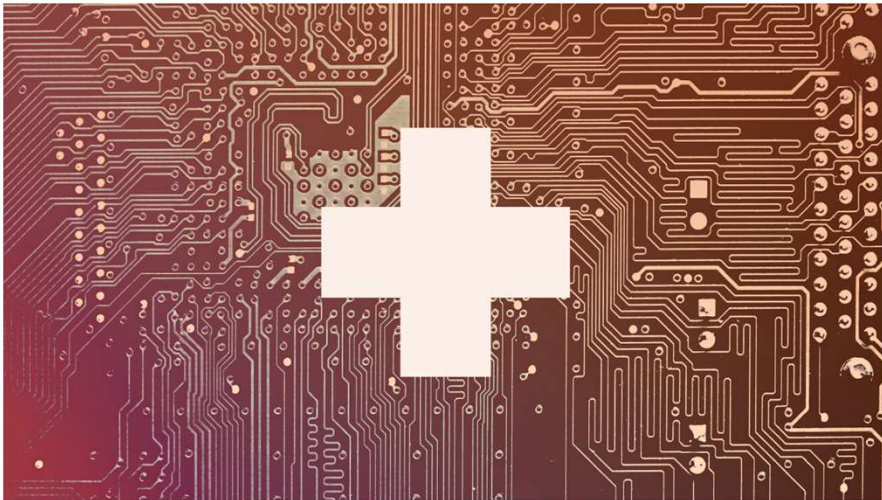
June 11, 2020 - UK-Based telehealth app Babylon Health recently experienced a breach of its general practitioner platform, where users were able to access videos from other patients' appointments, first reported by *the BBC*.

<https://healthitsecurity.com/news/breach-of-telehealth-app-babylon-health-raises-privacy-concerns>



Uncharted Digital Waters: How Private Are Telehealth Platforms?

September 9, 2021 | By Rachael Roth



Since the start of the pandemic, telehealth platforms have been more necessary than ever. But are they a target for cybercriminals?

According to former hacker Alissa Knight, personal health information (PHI) is the most valuable type of data that exists on the dark web. In this study, Knight and Approov looked at 30 mobile healthcare apps to see just how secure they were. Each of them had API vulnerabilities, and all of them were susceptible to Broken Object Level Authorization (BOLA) attacks. This extremely common API vulnerability means that an app does not confirm a user's privileges to protected information, and is very easy for hackers to exploit once discovered.

Obtaining medical records could enable someone to impersonate you and even get treatment or prescription drugs. Not to mention the bevy of information that comes with your MyChart or other accounts that are valuable on the dark web or make you vulnerable to phishing attacks: your birthdate, address, family history, and contact information, to name a few.

<https://blog.dashlane.com/telehealth-platforms-privacy/>

MAY 02 | MORE ON OPERATIONS

ATA2022: Regulatory risk in the business of telehealth

The question becomes, when does data collected from a telemedicine website become patient data?



Susan Morse, Executive Editor



Nathaniel Lacktman, a partner at Foley & Lardner, kicks off a talk on telehealth and regulation Sunday at the ATA2022 conference in Boston.

Photo: Susan Morse/HFN

What can save a company from litigation risk are the fine type cookie policies and terms, Maguregui said. This is critical to mitigating risk.

The best way to obtain a user's agreement is through e-sign or click and sign, he said.

Create a plan. Create a workflow for data. Are health insurers being billed so that HIPAA applies? Collaborate with marketing, legal and other teams. Nail down the purpose of the website.

And don't copy and paste someone else's privacy policy, he said. Create your own.

The question all companies need to ask is, what are you asking the user to do?

"There is definitely regulatory risk," Maguregui said. "The greater risk is public perception."

Also, what works today may not work tomorrow in the changing regulatory environment. Stay on top with audits and reviews.

<https://www.healthcarefinancenews.com/news/ata2022-regulatory-risk-business-telehealth>



https://www.youtube.com/watch?v=vRG4_kDTxTU

TELEHEALTH SECURITY AND PRIVACY TIPS FOR PROVIDERS

While telehealth provides a host of benefits for patient care, it also exposes healthcare delivery organizations (HDOs) to significant cyber risks. Here are some tips for improving the security and privacy of telehealth services for HDOs:

SHARE UPDATED PRIVACY AND SECURITY PRACTICES WITH YOUR PATIENTS.

Communicating privacy and security practices with your patients should be an integral part of your overall patient engagement strategy.

USE HIPAA-COMPLIANT APPLICATIONS to provide telehealth services when practical, and limit the number of applications used to help reduce security and privacy risks.

ENABLE ALL AVAILABLE ENCRYPTION AND PRIVACY MODES when using third-party applications for telehealth services.

MANAGE MOBILE DEVICE ACCESS. Isolate personal mobile devices from HDO applications, networks, and patient data. Corporate-owned devices should be granted the most access to HDO networks and information while personal mobile devices should have the least.

LIMIT NETWORK ACCESS. Apply defense in depth, network segmentation, and the principle of least privilege to prevent unauthorized access to patient information and medical devices.

USE MULTIFACTOR AUTHENTICATION WHENEVER POSSIBLE, especially when it comes to accessing your organization's most sensitive data.

MAINTAIN GOOD CYBER HYGIENE. Healthy habits for your information technology systems and applications will go a long way toward keeping them safe and secure. Run updates for equipment and applications as soon as they are available to take advantage of the latest security capabilities.



- **SHARE UPDATED PRIVACY AND SECURITY PRACTICES WITH YOUR PATIENTS.** Communicating privacy and security practices with your patients should be an integral part of your overall patient engagement strategy.
- **USE HIPAA-COMPLIANT APPLICATIONS** to provide telehealth services when practical, and limit the number of applications used to help reduce security and privacy risks.
- **ENABLE ALL AVAILABLE ENCRYPTION AND PRIVACY MODES** when using third party applications for telehealth services.
- **MANAGE MOBILE DEVICE ACCESS.** Isolate personal mobile devices from HDO applications, networks, and patient data. Corporate-owned devices should be granted the most access to HDO networks and information while personal mobile devices should have the least.

<https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-hdo-tips.pdf>

TELEHEALTH SECURITY AND PRIVACY TIPS FOR PROVIDERS

While telehealth provides a host of benefits for patient care, it also exposes healthcare delivery organizations (HDOs) to significant cyber risks. Here are some tips for improving the security and privacy of telehealth services for HDOs:

SHARE UPDATED PRIVACY AND SECURITY PRACTICES WITH YOUR PATIENTS.

Communicating privacy and security practices with your patients should be an integral part of your overall patient engagement strategy.

USE HIPAA-COMPLIANT APPLICATIONS to provide telehealth services when practical, and limit the number of applications used to help reduce security and privacy risks.

ENABLE ALL AVAILABLE ENCRYPTION AND PRIVACY MODES when using third-party applications for telehealth services.

MANAGE MOBILE DEVICE ACCESS. Isolate personal mobile devices from HDO applications, networks, and patient data. Corporate-owned devices should be granted the most access to HDO networks and information while personal mobile devices should have the least.

LIMIT NETWORK ACCESS. Apply defense in depth, network segmentation, and the principle of least privilege to prevent unauthorized access to patient information and medical devices.

USE MULTIFACTOR AUTHENTICATION WHENEVER POSSIBLE, especially when it comes to accessing your organization's most sensitive data.

MAINTAIN GOOD CYBER HYGIENE. Healthy habits for your information technology systems and applications will go a long way toward keeping them safe and secure. Run updates for equipment and applications as soon as they are available to take advantage of the latest security capabilities.



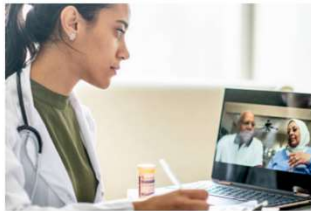
- **LIMIT NETWORK ACCESS.** Apply defense in depth, network segmentation, and the principle of least privilege to prevent unauthorized access to patient information and medical devices.
- **USE MULTIFACTOR AUTHENTICATION WHENEVER POSSIBLE,** especially when it comes to accessing your organization's most sensitive data.
- **MAINTAIN GOOD CYBER HYGIENE.** Healthy habits for your information technology systems and applications will go a long way toward keeping them safe and secure. Run updates for equipment and applications as soon as they are available to take advantage of the latest security capabilities.

<https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-hdo-tips.pdf>

**TELEHEALTH
SECURITY AND
PRIVACY TIPS
FOR PROVIDERS**

During a telehealth visit, ensure your clinicians:

USE A PRIVATE SPACE and limit the number of people who take part in a telehealth session. Allow only personnel directly involved in the patient's care and individuals whom the patient permits to take part in a telehealth visit. Secure the room where you are conducting telehealth sessions (e.g., close the door and post a sign outside the door saying unauthorized individuals should not enter while your session is underway). Use headsets to limit others from hearing your patient and position screens out of the line of sight of others.



LIMIT THE INFORMATION REQUESTED to what is necessary to treat the patient.

SIGN OUT OF ALL APPLICATIONS and turn off all microphones, cameras, and monitors once the telehealth visit has concluded.

ADDITIONAL RESOURCES

Telehealth Security and Privacy Tips for Patients: <https://www.nccoe.nist.gov/patient-tips>

NCCoE Healthcare Sector Cybersecurity Guidance: <https://www.nccoe.nist.gov/healthcare>

NCCoE Mobile Device Security Guidance: <https://www.nccoe.nist.gov/mobile>

NCCoE Data Security Guidance: <https://www.nccoe.nist.gov/projects/building-blocks/data-security>



- **USE A PRIVATE SPACE** and limit the number of people who take part in a telehealth session. Allow only personnel directly involved in the patient's care and individuals whom the patient permits to take part in a telehealth visit. Secure the room where you are conducting telehealth sessions (e.g., close the door and post a sign outside the door saying unauthorized individuals should not enter while your session is underway). Use headsets to limit others from hearing your patient and position screens out of the line of sight of others.
- **LIMIT THE INFORMATION REQUESTED** to what is necessary to treat the patient.
- **SIGN OUT OF ALL APPLICATIONS** and turn off all microphones, cameras, and monitors once the telehealth visit has concluded

<https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-hdo-tips.pdf>



Non-exhaustive list of steps you can take to improve the security of conference calls

- “ ...
- Follow your organization’s policies for virtual meeting security.
 - Limit reuse of access codes; if you’ve used the same code for a while, you’ve probably shared it with more people than you can imagine or recall.
 - If the topic is sensitive, use one-time PINs or meeting identifier codes, and consider multi-factor authentication.
 - Use a “green room” or “waiting room” and don’t allow the meeting to begin until the host joins.
 - Enable notification when attendees join by playing a tone or announcing names. If this is not an option, make sure the meeting host asks new attendees to identify themselves.
 - If available, use a dashboard to monitor attendees – and identify all generic attendees.
 - Don’t record the meeting unless it’s necessary.
 - If it’s a web meeting (with video):
 - Disable features you don’t need (like chat, file sharing, or screen sharing).
 - Consider using a PIN to prevent someone from crashing your meeting by guessing your URL or meeting ID.
 - Limit who can share their screen to avoid any unwanted or unexpected images. And before anyone shares their screen, remind them not to share sensitive information inadvertently...”

<https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings>

VIRTUAL CARE SECURITY TIPS for providers

Virtual care offers many benefits, but it can also increase exposure to cyberthreats. These tips can help keep PHI secure.

Disclaimer: Cybersecurity is an evolving topic. This infographic contains general suggestions. For specific advice, consult your legal counsel or health IT security specialist.

PRACTICE GOOD CYBER HYGIENE

Good cyber hygiene keeps virtual care healthier and safer for you and your patients.

- Only use a secured Wi-Fi network or a virtual private network (VPN) for your connection
- Use strong passwords that are unique to each account
- Use Bluetooth-connected devices and headphones in private settings only
- Sign off of accounts, close applications, and disable Bluetooth, microphones, and cameras after each virtual care session
- Keep firewall, antivirus, and anti-malware settings on and up to date
- Never leave your devices, screens, or papers containing PHI unlocked or unattended
- Promptly upload patches for your device(s), operating system, browser, and all other software

FOLLOW SECURITY POLICY AND REGULATIONS

Comply with all federal, state, and organizational security rules including protocols for response to a possible data breach.

- Use HIPAA-compliant, encrypted applications and communications
- Document all virtual patient interactions and trace the applications used
- Only install software approved by your organization
- Promptly report a security breach following your organization's protocol
- Limit data requests to what is needed to treat the patient
- If cyber insurance is not provided by your practice, obtain a private policy
- Do not save PHI on personal or shared devices

PATIENT SECURITY AND PRIVACY

Share your privacy and security practices and policies with your patients.

- Only permit necessary staff and patient-approved individuals to join the visit
- Encrypt communications with or about patients
- Use headphones to prevent others from hearing your conversation
- Verify you have the patient's consent to provide virtual care
- Educate patients about healthcare cybersecurity, including the benefits and risks of virtual care
- Introduce any other staff present and explain why they are there

TRUST YOUR GUT

Often our senses alert us to trouble. If something doesn't feel right, stop. If something feels suspicious, investigate.

- Think before you click. Small scams are common—if something doesn't feel right, don't click it.
- Speak up! Check in with your security or IT department if you have questions or concerns.

© 2021 Telehealth Resource Center. All rights reserved. This infographic is a work of the U.S. Government and is in the public domain in the United States of America. It is not subject to copyright protection under 17 USC 101. It is not to be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the Telehealth Resource Center. This infographic is provided as a service to the public and is not intended to constitute an offer of any financial product or service. It is not to be used as a substitute for professional advice. For more information, visit telehealthresourcecenter.org.

VIRTUAL CARE SECURITY TIPS for providers

Virtual care offers many benefits, but it can also increase exposure to cyberthreats. These tips can help keep PHI secure.

Disclaimer: Cybersecurity is an evolving topic. This infographic contains general suggestions. For specific advice, consult your legal counsel or health IT security specialist.

PRACTICE GOOD CYBER HYGIENE

Good cyber hygiene keeps virtual care healthier and safer for you and your patients.

- Only use a secured Wi-Fi network or a virtual private network (VPN) for your connection
- Use strong passwords that are unique to each account
- Use Bluetooth-connected devices and headphones in private settings only
- Sign off of accounts, close applications, and disable Bluetooth, microphones, and cameras after each virtual care session
- Keep firewall, antivirus, and anti-malware settings on and up to date
- Never leave your devices, screens, or papers containing PHI unlocked or unattended
- Promptly upload patches for your device(s), operating system, browser, and all other software

VIRTUAL CARE SECURITY TIPS for providers

Virtual care offers many benefits, but it can also increase exposure to cyberthreats. These tips can help keep PHI secure.

Disclaimer: This document is for informational purposes only. It does not constitute a legal opinion. For specific advice, consult your legal counsel or health IT security specialist.

PRACTICE GOOD CYBER HYGIENE

Keep your devices secure and up to date

- Only use a secured Wi-Fi network or a virtual private network (VPN) for your connection
- Use Bluetooth-connected devices and headphones in private settings only
- Keep firewall, antivirus, and anti-malware settings on and up to date
- Promptly upload patches for your devices (operating system, browser, and all other software)
- Use strong passwords that are unique to each account
- Sign off of accounts, close applications, and disable Bluetooth, microphones, and camera after each virtual care session
- Never leave your devices, screens, or papers containing PHI unlocked or unattended

FOLLOW SECURITY POLICY AND REGULATIONS

Comply with all federal, state, and organizational security rules including protocol for response to a possible data breach.

- Use HIPAA-compliant, encrypted applications and communications
- Only install software approved by your organization
- Limit data requests to what is needed to treat the patient
- Do not save PHI on personal or shared devices
- Document all virtual patient interactions and note the applications used
- Promptly report a security breach following your organization's protocol
- If cyber insurance is not provided by your practice, obtain a private policy

PATIENT SECURITY AND PRIVACY

Share your care securely, from wherever you're working

- Share current privacy and security practices and policies with your patients
- Encrypt communications with or about patients
- Verify you have the patient's consent to provide virtual care
- Introduce any other staff present and explain why they are there
- Only permit necessary staff and patient-approved individuals to join the visit
- Use headphones to prevent others from hearing your conversation
- Educate patients about healthcare cybersecurity, including the benefits and risks of virtual care

TRUST YOUR GUT

Often our senses alert us to trouble. If something doesn't feel right, stop. If something doesn't feel right, stop. If something doesn't feel right, stop.

- Think before you click—small scams are common—if something doesn't feel right, don't click it
- Speak up! Check in with your security or IT department if you have questions or concerns

© 2021 Telehealth Resource Center. All rights reserved. This document is for informational purposes only. It does not constitute a legal opinion. For specific advice, consult your legal counsel or health IT security specialist.

FOLLOW SECURITY POLICY AND REGULATIONS

Comply with all federal, state, and organizational security rules including protocol for response to a possible data breach.

- Use HIPAA-compliant, encrypted applications and communications
- Only install software approved by your organization
- Limit data requests to what is needed to treat the patient
- Do not save PHI on personal or shared devices
- Document all virtual patient interactions and note the applications used
- Promptly report a security breach following your organization's protocol
- If cyber insurance is not provided by your practice, obtain a private policy

<https://telehealthresourcecenter.org/resources/factsheets/virtual-care-security-tips-for-providers/>

VIRTUAL CARE SECURITY TIPS *for providers*

Virtual care offers many benefits, but it can also increase exposure to cyberthreats. These tips can help keep PHI secure. Guidelines developed by the American Psychiatric Association. Always consult your legal counsel or health IT security specialist.

PRACTICE GOOD CYBER HYGIENE

- Only use a secured Wi-Fi network or a virtual private network (VPN) for your connection.
- Use Bluetooth-connected devices and headphones in private settings only.
- Keep firewall, antivirus, and anti-malware settings on and up to date.
- Promptly upload patches for your devices (operating system, browser, and all other software).
- Use strong passwords that are unique to each account.
- Sign off of accounts, close applications, and disable Bluetooth, microphones, and camera after each virtual care session.
- Never leave your devices, screens, or papers containing PHI unlocked or unattended.

FOLLOW SECURITY POLICY AND REGULATIONS

Comply with all federal, state, and organizational security rules, including protocols for response to a possible data breach.

- Use HIPAA-compliant, encrypted applications and communications.
- Only install software approved by your organization.
- Limit data requests to what is needed to treat the patient.
- Do not save PHI on personal or shared devices.
- Document all virtual patient interactions and trace the applications used.
- Promptly report a security breach following your organization's protocol.
- If cyber insurance is not provided by your practice, obtain a private policy.

PATIENT SECURITY AND PRIVACY

Mitigate risks and educate your patients about cybersecurity.

- Share current privacy and security practices and policies with your patients.
- Encrypt communications with or about patients.
- Verify you have the patient's consent to provide virtual care.
- Introduce any other staff present and explain why they are there.
- Only permit necessary staff and patient-approved individuals to join the visit.
- Use headphones to prevent others from hearing your conversation.
- Educate patients about healthcare cybersecurity, including the benefits and risks of virtual care.

TRUST YOUR GUT

Often our senses alert us to trouble. If something seems off or too good to be true, verify the source before engaging with any email, voicemail, or person.

- Think before you click. Email scams are common—if something doesn't feel right, don't click it.
- Speak up! Check in with your security or IT department if you have questions or concerns.

© 2021 DHHS

California Telehealth Resource Center, 2021
 Made possible by grant number GA5RH37469 from the
 Office for the Advancement of Telehealth, Health Resources
 and Services Administration, DHHS

PATIENT SECURITY AND PRIVACY

Mitigate risks and educate your patients about cybersecurity.

- Share current privacy and security practices and policies with your patients.
- Encrypt communications with or about patients.
- Verify you have the patient's consent to provide virtual care.
- Introduce any other staff present and explain why they are there.
- Only permit necessary staff and patient-approved individuals to join the visit.
- Use headphones to prevent others from hearing your conversation.
- Educate patients about healthcare cybersecurity, including the benefits and risks of virtual care.

TRUST YOUR GUT

Often our senses alert us to trouble. If something seems off or too good to be true, verify the source before engaging with any email, voicemail, or person.

- Think before you click. Email scams are common—if something doesn't feel right, don't click it.
- Speak up! Check in with your security or IT department if you have questions or concerns.

<https://telehealthresourcecenter.org/resources/factsheets/virtual-care-security-tips-for-providers/>

TELEHEALTH SECURITY AND PRIVACY TIPS FOR PATIENTS

Demand for telehealth services skyrocketed in 2020 in response to social distancing recommendations from the COVID-19 pandemic, and is continuing its ascent into 2021 and beyond. While telehealth is convenient, it can also unexpectedly add cybersecurity risk and impact the privacy of patient information.

Here are some basic tips for improving the security and privacy of your telehealth visits:

BE AWARE OF UPDATED PRIVACY AND SECURITY PRACTICES FROM YOUR HEALTHCARE PROVIDER. Contact your healthcare provider with any questions or concerns you have about the privacy and security of the information shared during your telehealth session.

ALWAYS ASK YOUR PROVIDER IF YOUR TELEHEALTH SESSION IS PROTECTED AND SECURE. Unauthorized parties should not be able to listen in on the communication. Communication between you and your healthcare provider should be encrypted.

PICK A PRIVATE LOCATION FOR YOUR VISIT. Hold your telehealth session in a location away from others, such as a room with a door, so that you can control who hears your conversation.

BE AWARE OF SCAMS. Know how and when you will be contacted for your telehealth visit or any follow-up information. If you receive a suspicious call or email about your telehealth visit, contact your healthcare provider. Better safe than sorry.

BE AWARE OF WHAT'S BEHIND YOU. Be aware of what will be displayed in the background during a video call and remove any identifying information you do not want to share.

KEEP YOUR COMPUTER OR MOBILE DEVICE PATCHED AND UPDATED. Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.

AVOID USING PUBLIC WI-FI NETWORKS FOR YOUR TELEHEALTH APPOINTMENT. Use private Wi-Fi networks whenever possible when exchanging any kind of sensitive information with your healthcare provider.

TURN OFF NEARBY DEVICES THAT MAY CAPTURE YOUR CONVERSATION. Remove or turn off nearby items such as home security cameras, voice assistants, or other devices you are not using to contact your healthcare provider to make sure they do not capture potentially sensitive information.

LOG OUT OF YOUR TELEHEALTH SESSION WHEN YOU ARE DONE.



- **BE AWARE OF UPDATED PRIVACY AND SECURITY PRACTICES FROM YOUR HEALTHCARE PROVIDER.** Contact your healthcare provider with any questions or concerns you have about the privacy and security of the information shared during your telehealth session.
- **ALWAYS ASK YOUR PROVIDER IF YOUR TELEHEALTH SESSION IS PROTECTED AND SECURE.** Unauthorized parties should not be able to listen in on the communication. Communication between you and your healthcare provider should be encrypted.
- **PICK A PRIVATE LOCATION FOR YOUR VISIT.** Hold your telehealth session in a location away from others, such as a room with a door, so that you can control who hears your conversation.
- **BE AWARE OF SCAMS.** Know how and when you will be contacted for your telehealth visit or any follow-up information. If you receive a suspicious call or email about your telehealth visit, contact your healthcare provider. Better safe than sorry.

<https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-patient-tips.pdf>

TELEHEALTH SECURITY AND PRIVACY TIPS FOR PATIENTS

Demand for telehealth services skyrocketed in 2020 in response to social distancing recommendations from the COVID-19 pandemic, and is continuing its ascent into 2021 and beyond. While telehealth is convenient, it can also unexpectedly add cybersecurity risk and impact the privacy of patient information.

Here are some basic tips for improving the security and privacy of your telehealth visits:

BE AWARE OF UPDATED PRIVACY AND SECURITY PRACTICES FROM YOUR HEALTHCARE PROVIDER. Contact your healthcare provider with any questions or concerns you have about the privacy and security of the information shared during your telehealth session.

ALWAYS ASK YOUR PROVIDER IF YOUR TELEHEALTH SESSION IS PROTECTED AND SECURE. Unauthorized parties should not be able to listen in on the communication. Communication between you and your healthcare provider should be encrypted.

PICK A PRIVATE LOCATION FOR YOUR VISIT. Hold your telehealth session in a location away from others, such as a room with a door, so that you can control who hears your conversation.

BE AWARE OF SCAMS. Know how and when you will be contacted for your telehealth visit or any follow-up information. If you receive a suspicious call or email about your telehealth visit, contact your healthcare provider. Better safe than sorry.

BE AWARE OF WHAT'S BEHIND YOU. Be aware of what will be displayed in the background during a video call and remove any identifying information you do not want to share.

KEEP YOUR COMPUTER OR MOBILE DEVICE PATCHED AND UPDATED. Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.

AVOID USING PUBLIC WI-FI NETWORKS FOR YOUR TELEHEALTH APPOINTMENT. Use private Wi-Fi networks whenever possible when exchanging any kind of sensitive information with your healthcare provider.

TURN OFF NEARBY DEVICES THAT MAY CAPTURE YOUR CONVERSATION. Remove or turn off nearby items such as home security cameras, voice assistants, or other devices you are not using to contact your healthcare provider to make sure they do not capture potentially sensitive information.

LOG OUT OF YOUR TELEHEALTH SESSION WHEN YOU ARE DONE.



- **BE AWARE OF WHAT'S BEHIND YOU.** Be aware of what will be displayed in the background during a video call and remove any identifying information you do not want to share.
- **KEEP YOUR COMPUTER OR MOBILE DEVICE PATCHED AND UPDATED.** Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.
- **AVOID USING PUBLIC Wi-Fi NETWORKS FOR YOUR TELEHEALTH APPOINTMENT.** Use private Wi-Fi networks whenever possible when exchanging any kind of sensitive information with your healthcare provider.
- **TURN OFF NEARBY DEVICES THAT MAY CAPTURE YOUR CONVERSATION.** Remove or turn off nearby items such as home security cameras, voice assistants, or other devices you are not using to contact your healthcare provider to make sure they do not capture potentially sensitive information.


<https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-patient-tips.pdf>

VIRTUAL CARE SECURITY TIPS

for patients






Virtual care offers patients convenience, flexibility, and reduced costs. To ensure your information is secure, consider the following safeguards.

Disclaimer: Cybersecurity is an evolving topic. This infographic contains general suggestions. For specific advice, consult your legal counsel or health IT security specialist.



PRACTICE GOOD CYBER HYGIENE

What is cyber hygiene? Like washing your hands and getting enough sleep, good cyber hygiene is a set of best practices for keeping your digital information healthy and safe.

- **Use strong passwords**
A strong password uses 12 or more characters, is unique to each account, and mixes uppercase letters, lowercase letters, and symbols.
- **Use security software on your device**
Firewall, antivirus, and anti-malware software help protect your network and devices from harmful activity.
- **Use a secure router**
If using a wireless internet connection, check that the router is secure and password-protected with a password set by you.
- **Stay Up to Date**
Install current software updates to provide security patches for:
 - Operating systems on phones, tablets, and computers
 - Internet browsers
 - Routers and modems
- **Close the Loop**
Sign out of your accounts, close applications, and turn off Bluetooth, microphone, and camera once the virtual care session is complete.

California Telehealth
Resource Center, 2021

<https://caltrc.org/wp-content/uploads/2021/08/Virtual-Care-Security-Tips-for-Patients-2.pdf>

VIRTUAL CARE SECURITY TIPS

for patients

PRIVACY PLEASE

When you engage in virtual care, it is critical to know who can see your screen and hear your conversations.



Find the right location

Pick a private place for viewing personal health information and virtual visits.



Use a secure connection

Do not use public Wi-Fi for virtual care or accessing any sensitive information.



Use Bluetooth wisely

Only use Bluetooth connected devices or headphones for virtual care in private settings.



Invitation only

Ask your provider to identify anyone else who is in room with them or within earshot. In turn, let your provider know if people in the room with you have permission to be there.



Inventory your surroundings

Turn off recording devices and remove anything that displays personal information not necessary for your virtual visit.

PLEASE
Do Not
Disturb



READ UP ON POLICIES

Federal, state, and clinic-level policy provides you some privacy and security protections, but they may not apply to all digital tools related to your care. Request policies and ask questions if you are unsure.



From your health care provider

Read the updated privacy and security practices from your healthcare provider.



From your apps and devices

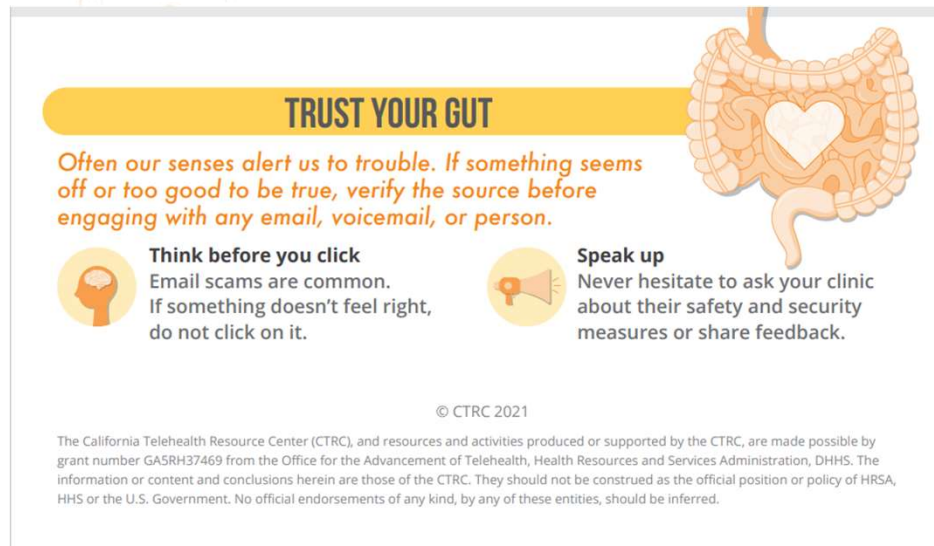
Don't assume all mHealth apps and digital tools are protected by HIPAA regulations.

VIRTUAL CARE SECURITY TIPS

for patients

Virtual care offers patients convenience, flexibility, and reduced costs. To ensure your information is secure, consider the following safeguards.

Disclaimer: Cybersecurity is an evolving topic. This infographic contains general suggestions. For specific advice, consult your legal counsel or health IT security specialist.



TRUST YOUR GUT

Often our senses alert us to trouble. If something seems off or too good to be true, verify the source before engaging with any email, voicemail, or person.

Think before you click
Email scams are common. If something doesn't feel right, do not click on it.

Speak up
Never hesitate to ask your clinic about their safety and security measures or share feedback.

© CTRC 2021

The California Telehealth Resource Center (CTRC), and resources and activities produced or supported by the CTRC, are made possible by grant number GA5RH37469 from the Office for the Advancement of Telehealth, Health Resources and Services Administration, DHHS. The information or content and conclusions herein are those of the CTRC. They should not be construed as the official position or policy of HRSA, HHS or the U.S. Government. No official endorsements of any kind, by any of these entities, should be inferred.

California Telehealth
Resource Center, 2021

<https://caltrc.org/wp-content/uploads/2021/08/Virtual-Care-Security-Tips-for-Patients-2.pdf>

The screenshot shows the NIST website page for 'Securing Telehealth Remote Patient Monitoring Ecosystem'. At the top left is the NIST logo. Below it is a breadcrumb trail: Home > Security Guidance > Securing Telehealth Remote Patient Monitoring Ecosystem. The NCCoE logo (National Cybersecurity Center of Excellence) is on the left. A navigation bar contains 'SECURITY GUIDANCE', 'OUR APPROACH', 'NEWS & INSIGHTS', 'GET INVOLVED', and a search icon. The main title is 'Securing Telehealth Remote Patient Monitoring Ecosystem'. Below the title is a paragraph of introductory text. To the right is a circular image of a person in a blue lab coat holding a smartwatch. At the bottom left, a text box says 'A distributed solution that enables health delivery organizations to better secure their remote patient monitoring ecosystem'. At the bottom right, a blue box indicates 'STATUS: FINALIZED PRACTICE GUIDE' and 'NIST SP 1800-30: Complete Guide (PDF)' with a PDF icon.

<https://www.nccoe.nist.gov/healthcare/securing-telehealth-remote-patient-monitoring-ecosystem>

TechTarget | HEALTH IT SECURITY | xtelligent HEALTHCARE MEDIA

Jill McKeon
Associate Editor
jmckeon@xtelligentmedia.com

NIST Issues Final Guidance on RPM, Telehealth Security

The National Cybersecurity Center of Excellence (NCCoE) released NIST’s final guidance on RPM and telehealth security.

February 24, 2022

“...The publication is aimed at healthcare professionals who are implementing RPM ecosystems using third-party telehealth platform providers. Since the telehealth platform provider manages devices and collects biometric data, the guide stressed the criticality of **third-party risk assessments** and **proper security controls**...”

<https://healthitsecurity.com/news/nist-issues-final-guidance-on-rpm-telehealth-security>

Managing Telehealth, Remote Patient Monitoring Security Concerns

January 27, 2022



Jill McKeon

Assistant Editor
jmckeon@xtelligentmedia.com



TELEHEALTH SECURITY CONCERNS

“If you're in a hospital, all the technology that is used to monitor you and take care of you is all within the confines of the hospital's firewall. It's a tightly controlled technology IT environment, and all the equipment inside can be very tightly secured,” Shah explained.

“The minute you take some part of that technology and send it home with the patient, suddenly you have to open up holes in your defense system so that the technology from the home can send data to the central systems where the clinicians can actually provide the care.”

Because data is being transmitted back and forth, and network security often cannot be guaranteed, cybercriminals may be able to attack healthcare organizations via the home or hospital environment. The increasing number of access points expands the surface and scope for cyberattacks and provides an unsuspecting entry point for hackers.

<https://healthitsecurity.com/features/managing-telehealth-remote-patient-monitoring-security-concerns>

Managing Telehealth, Remote Patient Monitoring Security Concerns

January 27, 2022

MITIGATING RISK AND MANAGING CONCERNS

“Healthcare organizations should always make sure that the tools they use to communicate are as protected as they can be, even when on an untrusted device,” Wollnik suggested.

Maintaining [endpoint security](#) and [BYOD policies](#) across the organization’s network is crucial to overall cybersecurity and telehealth security. Identity management and [zero trust tactics](#) can also contribute to a comprehensive cybersecurity program.

In addition to implementing key technical safeguards, Wollnik recommended that healthcare organizations [evaluate telehealth vendors carefully and have frequent discussions about data privacy and security](#).

“When evaluating a vendor, one of the primary questions becomes data handling,” Wollnik continued.

Healthcare organizations should ensure that they know how third-party vendors are interacting with and storing their data. Those conversations will naturally come up as organizations go through the process of creating and signing a [business associate agreement](#), (BAA) which requires business associates handling [protected health information](#) (PHI) to adhere to HIPAA regulations.

“Vendors need to recognize that yes, the customer is the healthcare provider, but it is patients whose data they’re actually holding,” Wollnik emphasized.

“And they are the ultimate beneficiaries and potential victims if anything goes sideways.”

Regular patching by vendors, technical safeguard implementation by healthcare organizations, and proper cyber hygiene by providers can ensure that telehealth and RPM technologies are secure.

<https://healthitsecurity.com/features/managing-telehealth-remote-patient-monitoring-security-concerns>



Jill McKeon

Assistant Editor
jmckeon@xtelligentmedia.com





Jill McKeon

Associate Editor
jmckeon@xtelligentmedia.com

HIMSS Healthcare Cybersecurity Forum: Understanding, Tackling Top Cyber Threats

Top risks to healthcare cybersecurity include notorious ransomware groups, unpatched vulnerabilities, and the sector's reliance on technology.

September 08, 2023 - *BOSTON, Mass.*

<https://healthitsecurity.com/news/himss-healthcare-cybersecurity-forum-understanding-tackling-top-cyber-threats>



Jill McKeon

Associate Editor
jmckeon@xtelligentmedia.com

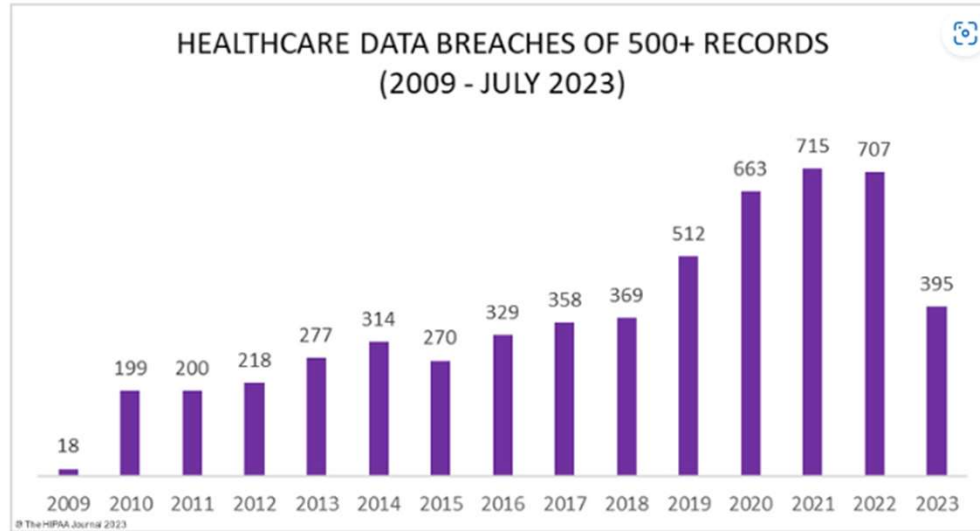
78% of Surveyed Healthcare Organizations Experienced a Cybersecurity Incident in Last Year

More than 60 percent of respondents reported a moderate or substantial impact on care delivery due to a cybersecurity incident, Claroty found.

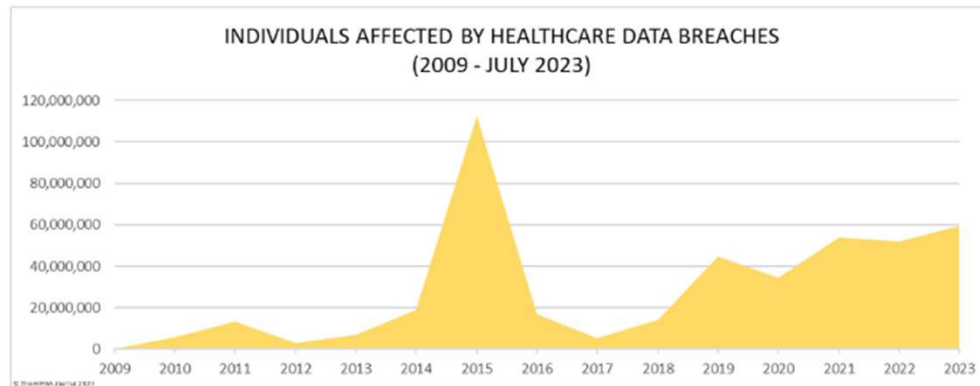
August 29, 2023 - More than three-quarters of surveyed healthcare professionals reported experiencing at least one cybersecurity incident at their organizations in the last year, Claroty **revealed** in its “Global Healthcare Cybersecurity Study 2023.”

<https://healthitsecurity.com/news/78-of-surveyed-healthcare-organizations-experienced-a-cybersecurity-incident-in-last-year>

<https://www.hipaajournal.com/healthcare-data-breach-statistics/>



Healthcare Records Exposed by Year



Krebs on Security

In-depth security news and investigation



HOME

ABOUT THE AUTHOR

ADVERTISING/SPEAKING

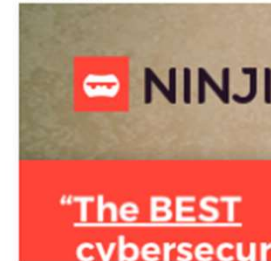
New Ransom Payment Schemes Target Executives, Telemedicine

December 8, 2022

7 Comments

Ransomware groups are constantly devising new methods for infecting victims and convincing them to pay up, but a couple of strategies tested recently seem especially devious. The first centers on targeting healthcare organizations that offer consultations over the Internet and sending them booby-trapped medical records for the “patient.” The other involves carefully editing email inboxes of public company executives to make it appear that some were involved in insider trading.

Advertisement



<https://krebsonsecurity.com/2022/12/new-ransom-payment-schemes-target-executives-telemedicine/>

OCR Quarter 1 2022 Cybersecurity Newsletter

Defending Against Common Cyber-Attacks



“ ... Phishing

One of the most common attack vectors is phishing. Phishing is a type of cyber-attack used to trick individuals into divulging sensitive information via electronic communication, such as email, by impersonating a trustworthy source.⁴ A recent report noted that 42% of ransomware attacks in Q2 2021 involved phishing.⁵ All regulated entities' workforce members should understand they have an important role in protecting the ePHI their organization holds from cyber-attacks. Part of that role ...

Exploiting Known Vulnerabilities

Hackers can penetrate a regulated entity's network and gain access to ePHI by exploiting known vulnerabilities. A known vulnerability is a vulnerability whose existence is publicly known. The National Institute of Standards and Technology (NIST) maintains the National Vulnerability Database (NVD),¹² which provides information about known vulnerabilities. Exploitable vulnerabilities can exist in many ...

Weak Cybersecurity Practices

A regulated entity that has weak cybersecurity practices makes itself an attractive soft target. Weak authentication requirements are frequent targets of successful cyber-attacks (over 80% of breaches due to hacking involved compromised or brute-forced credentials).²¹ Weak password rules and single factor authentication are among the practices that can contribute to successful attacks. Once inside an ...

availability of their ePHI. Further, HHS is collaborating with its industry partners, through the [HHS 405\(d\) Aligning Health Care Industry Security Approaches Program](#), to provide the HPH sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices, to combat cybersecurity threats common. ...”

<https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html>

Sentinel Event Alert

A complimentary publication of The Joint Commission

Issue 67, Aug. 15, 2023

Preserving patient safety after a cyberattack



“...It’s critical that healthcare organizations do all they can to prevent a cyberattack, such as decreasing access points for penetration, removing devices with old or obsolete operating systems, and training and testing staff to decrease vulnerability to phishing. There is abundant guidance for healthcare and IT professionals on how to prevent cyberattacks; therefore, this Sentinel Event Alert focuses on the safety risks associated with such events and provides tips on what organizations can do to prepare to deliver safe patient care in the event of a cyberattack...”

<https://www.jointcommission.org/-/media/tjc/newsletters/sea-67-cybersecurity-7-26-23-final.pdf>



HHS 405(d) Aligning Health Care Industry Security Approaches

Task Group Member Portal

- Home
- Why Care About Cybersecurity
- Protect Patients & Organizations
- News & Awareness Resources
- Get Involved
- Resources
- About Us
- Disclaimer

Video Transcript:

“Imagine this:

You're sitting around the table eating dinner with your friends and family, when all of a sudden you see a family friend grasp their chest.

Out of instinct, you immediately call 911 and the paramedics arrive, revealing that your friend's artificial heart valve is malfunctioning.

On the way to the hospital, the paramedics are diverted to a hospital thirty-five minutes away

Your initial instinct is to blame the hospital, because you're confused as to how they could have no room for your friend. However, this is not the case.

In fact, you soon discover the hospital's patient and data system was being held for ransom as result of a cyber-attacker; thus the hospital was unable to accept incoming patients...”



Download the script to the video above

<https://405d.hhs.gov/public/navigation/home>



U.S. Department of Health & Human Services

405(d) Program, Office of Information Security (OIS)



© 2023 ARIZONA TELEMEDICINE PROGRAM



CRITICAL CONDITION —

Hospitals hamstrung by ransomware are turning away patients

The ransomware epidemic continues to grow.

DAN GOODIN - 8/16/2021, 12:26 PM



health.mil

Enlarge

176



Dozens of hospitals and clinics in West Virginia and Ohio are canceling surgeries and diverting ambulances following a ransomware attack that has knocked out staff access to IT systems across virtually all of their operations.

The facilities are owned by **Memorial Health System**, which represents 64 clinics, including hospitals Marietta Memorial, Selby General, and Sistersville General in the Marietta-Parkersburg metropolitan area in West Virginia and Ohio. Early on Sunday, the chain experienced a ransomware attack that hampered the three hospitals' ability to operate normally.

<https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/>

Latest Health Data Breaches News

<https://healthitsecurity.com/topic/latest-health-data-breaches>

Third-Party Data Breaches, Unauthorized Email Access Cause PHI Exposure



February 4, 2022 - Third-party data breaches, unauthorized email access, and cyberattacks aimed at small outpatient facilities continue to impact the healthcare sector. Threat actors are increasingly leveraging Ransomware-as-a-Service (RaaS) models, software vulnerability exploits, and double extortion over traditional data encryption, a recent Abnormal Security report found. Healthcare organizations...

Healthcare Ransomware Outages: Scripps, Ireland HSE, and NZ Hospitals

May 18, 2021 by Jessica Davis

Healthcare remains a key target for ransomware hacking groups, as seen in recent research data and multiple hospital system outages. Scripps Health is continuing recovery efforts two weeks after an attack, while Ireland's health...

Scripps Health EHR, Patient Portal Still Down After Ransomware Attack

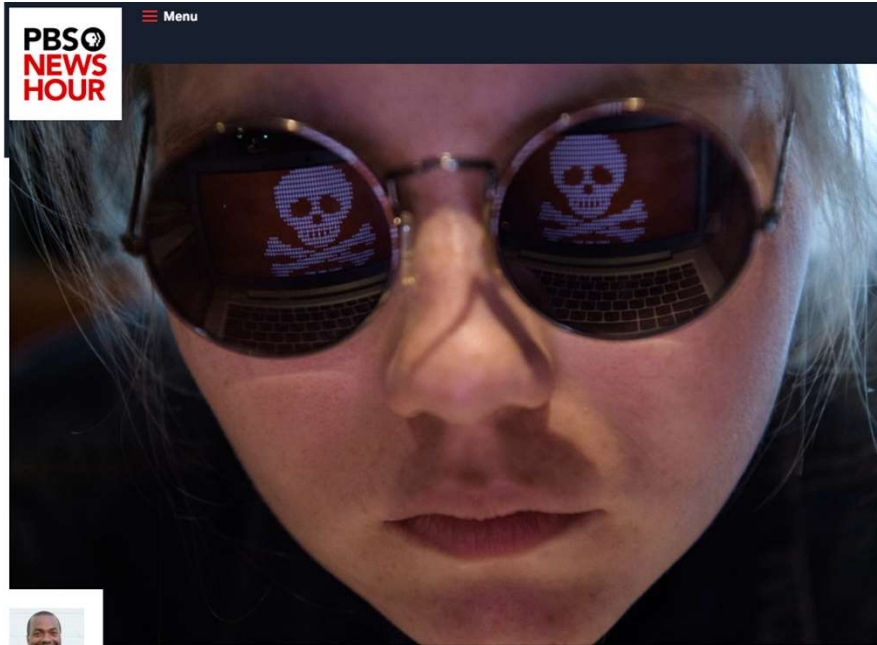
May 10, 2021 by Jessica Davis

Scripps Health is continuing to operate under EHR downtime procedures and its website and patient portal remain offline, nine days after a ransomware attack struck its servers. The California Department of Health (CDPH) has since confirmed...

Ransomware Hits Scripps Health, Disrupting Critical Care, Online Portal

May 03, 2021 by Jessica Davis

Scripps Health in San Diego was hit by a ransomware attack over the weekend, forcing the health system into EHR downtime. Some critical care patients were diverted and the online patient portal has been taken offline, according to...



By —
**Nsikan
Akpan**

Leave a
comment

Share

f t

Ransomware and data breaches linked to uptick in fatal heart attacks

Science Oct 24, 2019 9:15 AM EST

Imagine a scenario where you have a medical emergency, you head to the hospital, and it is shut down. On a Friday morning in September, this hypothetical became a reality for a community in northeast Wyoming.

<https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks>

Hospital ransomware attack led to infant's death, lawsuit alleges

The 2019 incident, which disabled Springhill Medical Center's EHR and patient monitors for days, obscured access to critical information that could have allowed for a lifesaving C-section, the baby's mother says.

By [Mike Miliard](#) | October 01, 2021 | 01:31 PM



A new report in [The Wall Street Journal](#) details a cyberattack that may, a lawsuit alleges, have caused the first fatality linked to ransomware in the U.S.

WHY IT MATTERS

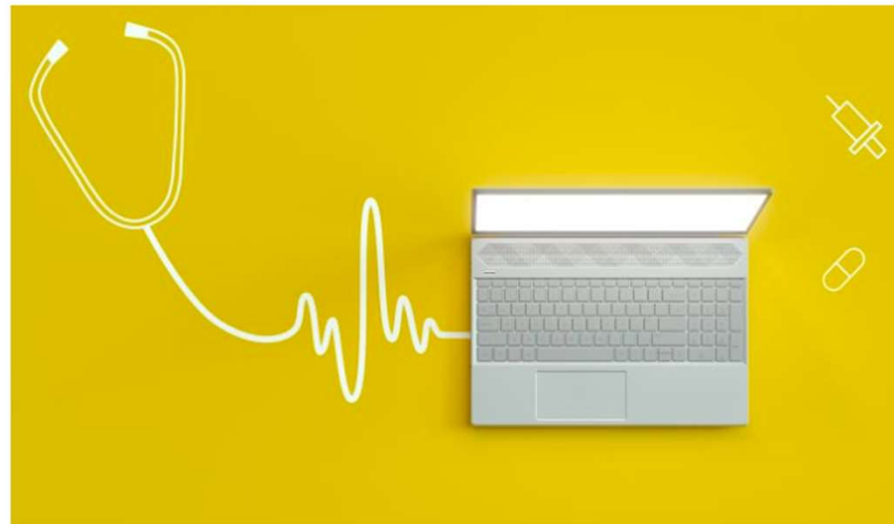
The [ransomware attack](#) that targeted Mobile, Alabama-based Springhill Medical Center in July 2019 knocked the hospital's IT systems offline for more than three weeks, according to the report – necessitating a return to paper charting, disrupting staff communication and compromising visibility of fetal heartbeat monitors in the labor and delivery ward.

In the [lawsuit](#), Teiranni Kidd alleges that she was not informed that the hospital was in the midst of fending off the cyberattack when she arrived for a scheduled labor induction.

<https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges>

AZ Ransomware Attack Leads to Unrecoverable EHRs, Data Loss

An Arizona medical center will have to rebuild thousands of patient records after a ransomware attack resulted in corrupted EHRs and data loss.



Source: Getty Images



By Jill McKeon



<https://healthitsecurity.com/news/az-ransomware-attack-leads-to-unrecoverable-ehrs-data-loss>

Physician accused of HIPAA breach after exiting practice for telehealth startup

Laura Dyrda (Twitter) - Friday, July 15th, 2022



Washington, D.C.-based Foxhall OB/GYN Associates accused Sharon Malone, MD, a former owner and physician at the practice, of taking patient information with her when she exited the practice to join telehealth startup Alloy, *The Washington Examiner* reported July 14.

Dr. Malone left Foxhall on Dec. 31, 2020, to join Alloy as its medical director. Foxhall sent a letter to patients in June accusing Dr. Malone of giving Alloy the names, phone numbers, email addresses and insurance information of former patients earlier this year, which is a HIPAA violation. The letter states Alloy sent emails to some of the patients.

At least one of the patients who received an email from Alloy complained to Foxhall, which is how the practice said it learned Dr. Malone had taken patient information with her.

<https://www.beckershospitalreview.com/cybersecurity/physician-accused-of-hipaa-breach-after-exiting-practice-for-telehealth-startup.html>

How An Independent Practice Recovered From a Third-Party Ransomware Attack

A NC-based family physician shares lessons learned after his independent practice was collateral damage in a third-party ransomware attack originating at a cloud provider.



Source: Getty Images January 24, 2023

<https://healthitsecurity.com/features/how-an-independent-practice-recovered-from-a-third-party-ransomware-attack>



Jill McKeon

Assistant Editor
jmckeon@xtelligentmedia.com

The New Resource for Life Sciences
News and Research

Stay up to date on
pathology, genomics,
medical devices,
and more at...

TechTarget | LIFESCIENCES
INTELLIGENCE
INTEGRATING HEALTHCARE MEDIA

Visit Now >

Newsletter Signup

- HIPAA, Cybersecurity and Ransomware
- IT Infrastructure
- Analytics, AI and Blockchain
- Pharma/BioMed
- Life Sciences

corporate email address

I agree to TechTarget's [Terms of Use](#), [Privacy Policy](#), and the transfer of my information to the United States for processing to provide me with relevant information as described in our Privacy Policy.

NCTRC Webinar – Ransomware In Health

BY SOUTHWEST TELEHEALTH RESOURCE CENTER • OCTOBER 14, 2021



Hosted by: Southwest Telehealth Resource Center

Outcome Objectives:

- Describe the basics of ransomware and why it poses cybersecurity and other risks.
- Determine weaknesses in healthcare systems.
- Identify methods to counteract ransomware in medical settings.

Speakers:

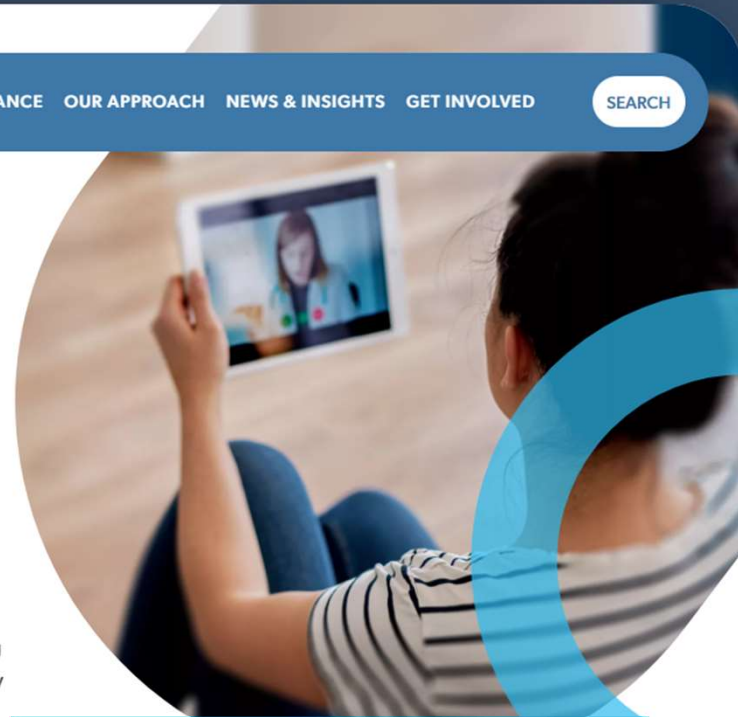
- Jeanne E. Varner Powell, JD, Senior Legal Risk Management Consultant, MICA
- David Shelley, President, BVA Inc.

Moderator: Michael J Holcomb, Associate Director, Information Technology, Southwest Telehealth Resource Center, Arizona Telemedicine Program

<https://telehealthresourcecenter.org/resources/webinars/nctrc-webinar-ransomware-in-health/>

Mitigating Cybersecurity Risk in Telehealth Smart Home Integration

Consumers now use smart home devices as an interface into the telehealth ecosystem. Smart home devices offer enhanced, multi-sensory user experiences that allow individuals to converse with technology naturally. While the user experience may be improved, practitioners may find challenges associated with deploying mitigating controls that limit cybersecurity and privacy risk given that devices may use proprietary or purpose-built operating systems that do not allow engineers to add protective software.



 STATUS: SEEKING COLLABORATORS

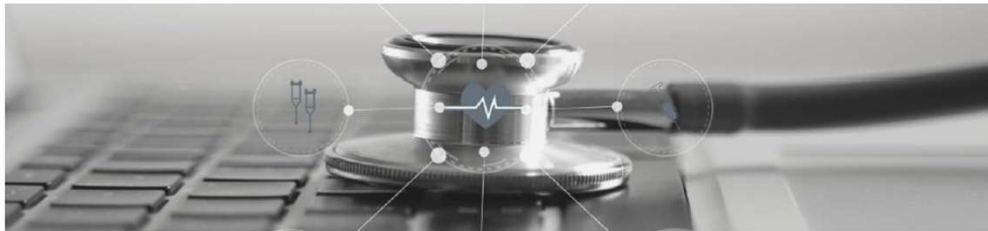
<https://www.nccoe.nist.gov/healthcare/mitigating-cybersecurity-risk-telehealth-smart-home-integration>



Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY - SECURING TELEHEALTH AND TELEMEDICINE

April 2021



The Health Sector Coordinating Council (HSCC) has developed this white paper, the “Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)” guide,- for the benefit of health care systems, clinicians, vendors and service providers, and patients. All of these stakeholders share responsibility for ensuring that telehealth services achieve their optimum benefit with minimal risk to the privacy and security of the data, the consultations, and the systems hosting them.

<https://www.aha.org/guidesreports/2021-04-20-healthcare-and-public-health-sector-coordinating-councils-public-private>



Privacy, Security, and HIPAA ▾

Educational Videos

Security Risk Assessment Tool ▾

Security Risk Assessment Videos

Top 10 Myths of Security Risk Analysis

HIPAA Basics >

Privacy & Security Resources & Tools >

Model Privacy Notice (MPN)

How APIs in Health Care can Support Access to Health Information: Learning Module

Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, visit the Office for Civil Rights' official guidance.

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

Need Help?

Please leave any questions, comments, or feedback about the SRA Tool using our Health IT Feedback Form. This includes any trouble in using the tool or problems/bugs with the application itself. Also, please feel free to leave any suggestions on how we could improve the tool in the future.

You may also leave a message with our Help Desk by contacting 734-302-4717

Submit Questions Or Feedback

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

ARIZONA
TELEMEDICINE
PROGRAM



Thank you!

Questions?

mholcomb@telemedicine.arizona.edu

