

ARIZONA
TELEMEDICINE
PROGRAM



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



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



Why do we need to secure telemedicine technologies and communications?

- Protect patients, business, and business partners
- Good business practice to maintain confidentiality of patient information
 - Patients and business partners may lose trust in a healthcare provider if their information is compromised
- Laws such as Health Insurance Privacy and Accountability Act (HIPAA) require implementation of security measures to protect protected health information (PHI)
 - To guard against breaches of and unauthorized disclosures of PHI
- Securing telehealth is not just about privacy and maintaining confidentiality.
 - Also important:
 - Availability of data and technology to conduct telehealth operations
 - Integrity of data used to make patient care decisions via telehealth

Example Types of Telemedicine and Telehealth Communications (selected)

- Video conferencing
 - Face to face
 - provider to patient, provider to provider, multiple provider to patient, provider to multiple patients
 - Real-time medical imaging applications
- Audio only phone calls
- 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
- Diagnostic review of medical/health 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

What specific security measures are needed for telemedicine?

- The techniques used to secure telemedicine services are not, in general, unique to telemedicine
- HIPAA, for example, does not specify specific information security technologies
 - Technology is always advancing
 - Hackers are always looking for vulnerabilities
 - Organizations must implement reasonable and appropriate administrative, technical and physical controls to safeguard PHI
- Cybersecurity is all about controlling access to prevent unauthorized access to computers, mobile devices, networks and data while allowing authorized access for those that need it.
- When allowing business associates to work with your organization's patients' healthcare information, Verify Their Security Practices



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



© 2023 ARIZONA TELEMEDICINE PROGRAM



Social Determinants of Health Virtual Summit Featured
PATIENT ENGAGEMENT HIT [REGISTER NOW](#) Housing & Transport
Improving Health Outco

The Telehealth Security Impact: Now and Beyond the COVID-19 Pandemic

IEEE and Impact Advisor leaders share best practice policies for encryption, risk remediation, and security reviews to reduce possible telehealth security impacts beyond COVID-19.

“Regulatory enforcement pertaining to telehealth was eased somewhat during the pandemic, but this easing will not last forever.”

But Garzone predicts there will be additional stringency for how telehealth is used.

<https://healthitsecurity.com/news/the-telehealth-security-impact-now-and-beyond-the-covid-19-pandemic>

Report: COVID-19 Telehealth Risks and Best Practice Privacy, Security

A report published in JAMIA spotlights both the cybersecurity risks associated with telehealth use amid COVID-19 and best practice privacy and security measures needed in response.



By Jessica Davis



December 17, 2020 - Highlighting the risks posed by **lifted** restrictions on communication apps amid the COVID-19 pandemic, new research published in the *Journal of the American Medical Informatics Association* urged healthcare organizations to take steps to bolster telehealth privacy and cybersecurity measures.

In light of these threats, the researchers released a number of recommended best practice privacy and security measures needed to ensure the security of the healthcare infrastructure.

To start, healthcare organizations should ensure they have the right processes in place to drive awareness across the enterprise, including education, training, and even simulated cyberattacks.

Hospitals may also consider reducing the number of announcements sent to employees, as research shows that employees' workload has the biggest effect on the rate of clicking malicious links.

Administrators should ensure they've implemented best practice security measures, including data encryption, prompt software updates, antivirus software, two-factor authentication, and employing local cybersecurity recommendations or regulations.

Further, while it may have been necessary to leverage consumer-based video conferencing tools at the start of the pandemic response, covered entities should transition to an enterprise-grade, healthcare-specific product as soon as they're able as the platforms will typically offer better security features.

"Protection against these threats to secure telemedicine platforms is complex, and requires a multi-disciplinary, multi-stakeholder approach," researchers explained. "Healthcare organizations need to enhance (if not revolutionize) their cybersecurity infrastructure by developing stronger prevention and detection protocols, both administrative and technological."

"Executives need to be willing to invest fully in cybersecurity throughout the organization," they added. "Emerging fields, such as AI, IoT, and blockchain can also be employed as prevention and detection tools to combat cyber threats more effectively."

HEALTH
IT SECURITY
xtelligent HEALTHCARE MEDIA

Home News Features In

HIPAA and Compliance Cybersecurity Cloud Mobile Patient Privacy Data Breaches

<https://healthitsecurity.com/news/report-covid-19-telehealth-risks-and-best-practice-privacy-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



Global Cyberattacks Increased By 38% Last Year, Healthcare Hit Hard

Healthcare, education, and government were the three industries most impacted by cyberattacks in 2022, new data from Check Point Research suggests.



Source: Getty Images



By Jill McKeon



January 11, 2023 - Global cyberattacks increased by 38 percent in 2022 compared to 2021, new **data** from Check Point Research revealed. Healthcare was one of the three most attacked industries in 2022 according to Check Point Research data, along with the government and education sectors.

KrebsonSecurity

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/>

COMPUTING

2021 has broken the record for zero-day hacking attacks

But the reasons why are complicated—and not all bad news.

By Patrick Howell O'Neill

September 23, 2021

<https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/>

A zero-day exploit—a way to launch a cyberattack via a previously unknown vulnerability—is just about the most valuable thing a hacker can possess. These exploits can carry price tags north of \$1 million on the open market.

And this year, cybersecurity defenders have caught the highest number ever, according to multiple databases, researchers, and cybersecurity companies who spoke to MIT Technology Review. At least 66 zero-days have been found in use this year, according to databases such as the 0-day tracking project—almost double the total for 2020, and more than in any other year on record.

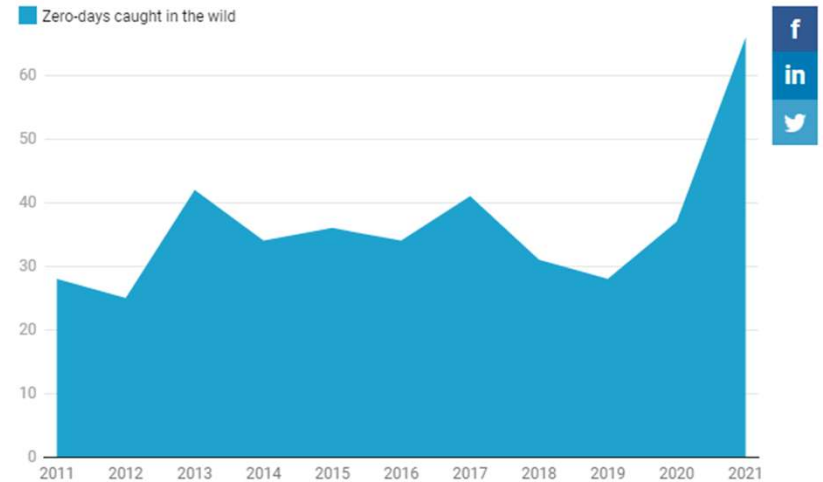


Chart: Patrick Howell O'Neill • Source: Zero-day tracking project • Get the data • Created with Datawrapper

MODEL BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT (the “BAA”) is made and entered into as of _____ by and between _____, a _____ organized under the laws of the _____ (“Covered Entity”) and _____, a _____ organized under the laws of _____ (“Business Associate”, in accordance with the meaning given to those terms at 45 CFR §164.501). In this BAA, Covered Entity and Business Associate are each a “Party” and, collectively, are the “Parties”.

- 3. Safeguards Against Misuse of PHI.** Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided by the Agreement or this BAA and Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate agrees to take reasonable steps, including providing adequate training to its employees to ensure compliance with this BAA and to ensure that the actions or omissions of its employees or agents do not cause Business Associate to breach the terms of this BAA.
- 4. Reporting Disclosures of PHI and Security Incidents.** Business Associate will report to Covered Entity in writing any use or disclosure of PHI not provided for by this BAA of which it becomes aware and Business Associate agrees to report to Covered Entity any Security Incident affecting Electronic PHI of Covered Entity of which it becomes aware. Business Associate agrees to report any such event within five business days of becoming aware of the event.
- 5. Reporting Breaches of Unsecured PHI.** Business Associate will notify Covered Entity in writing promptly upon the discovery of any Breach of Unsecured PHI in accordance with the requirements set forth in 45 CFR §164.410, but in no case later than 30 calendar days after discovery of a Breach. Business Associate will reimburse Covered Entity for any costs incurred by it in complying with the requirements of Subpart D of 45 CFR §164 that are imposed on Covered Entity as a result of a Breach committed by Business Associate.

<https://www.hhs.gov/sites/default/files/model-business-associate-agreement.pdf>

OCR Cyber Awareness Newsletters

In 2019, OCR moved to quarterly cybersecurity newsletters. The purpose of the newsletters remains unchanged: to help HIPAA covered entities and business associates remain in compliance with the HIPAA Security Rule by identifying emerging or prevalent issues, and highlighting best practices to safeguard PHI. [Visit our Cybersecurity Newsletter Archive page to view previous newsletters from 2016.](#)

- [October 2022 OCR Cybersecurity Newsletter: HIPAA Security Rule Security Incident Procedures](#)
- [Quarter 1 2022 OCR Cybersecurity Newsletter: Defending Against Common Cyber-Attacks](#)
- [Fall 2021 OCR Cybersecurity Newsletter: Securing Your Legacy \[System Security\]](#)
- [Summer 2021 OCR Cybersecurity Newsletter: Controlling Access to ePHI: For Whose Eyes Only?](#)
- [Summer 2020 OCR Cybersecurity Newsletter: HIPAA and IT Asset Inventories](#)
- [Summer 2019 OCR Cybersecurity Newsletter: Managing Malicious Insider Threats](#)
- [Spring 2019 OCR Cybersecurity Newsletter: Advanced Persistent Threats and Zero Day Vulnerabilities](#)
- [Fall 2019 OCR Cybersecurity Newsletter: What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware](#)

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

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>



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



U.S. Department of Health and Human Services Office for Civil Rights

Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Breach Report Results



Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
▶	Benefit Administrative Systems, LLC (BAS)	IL	Business Associate	6465	01/27/2023	Hacking/IT Incident	Network Server
▶	Cedar Oaks Surgery Center	MO	Healthcare Provider	794	01/27/2023	Hacking/IT Incident	Email
▶	Hayward Sisters Hospital d/b/a St. Rose Hospital	CA	Healthcare Provider	501	01/27/2023	Hacking/IT Incident	Network Server
▶	Howard Memorial Hospital	AR	Healthcare Provider	53668	01/27/2023	Hacking/IT Incident	Network Server
▶	AppleCare, LLC	GA	Healthcare Provider	512	01/23/2023	Unauthorized Access/Disclosure	Paper/Films
▶	City of Cleveland	OH	Health Plan	15206	01/20/2023	Unauthorized Access/Disclosure	Other
▶	DCH Health System	AL	Healthcare Provider	2530	01/20/2023	Unauthorized Access/Disclosure	Desktop Computer
▶	Chico Immediate Care Medical Center, Inc.	CA	Healthcare Provider	3780	01/19/2023	Unauthorized Access/Disclosure	Electronic Medical Record

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

**U.S. Department of Health and Human Services
Office for Civil Rights**

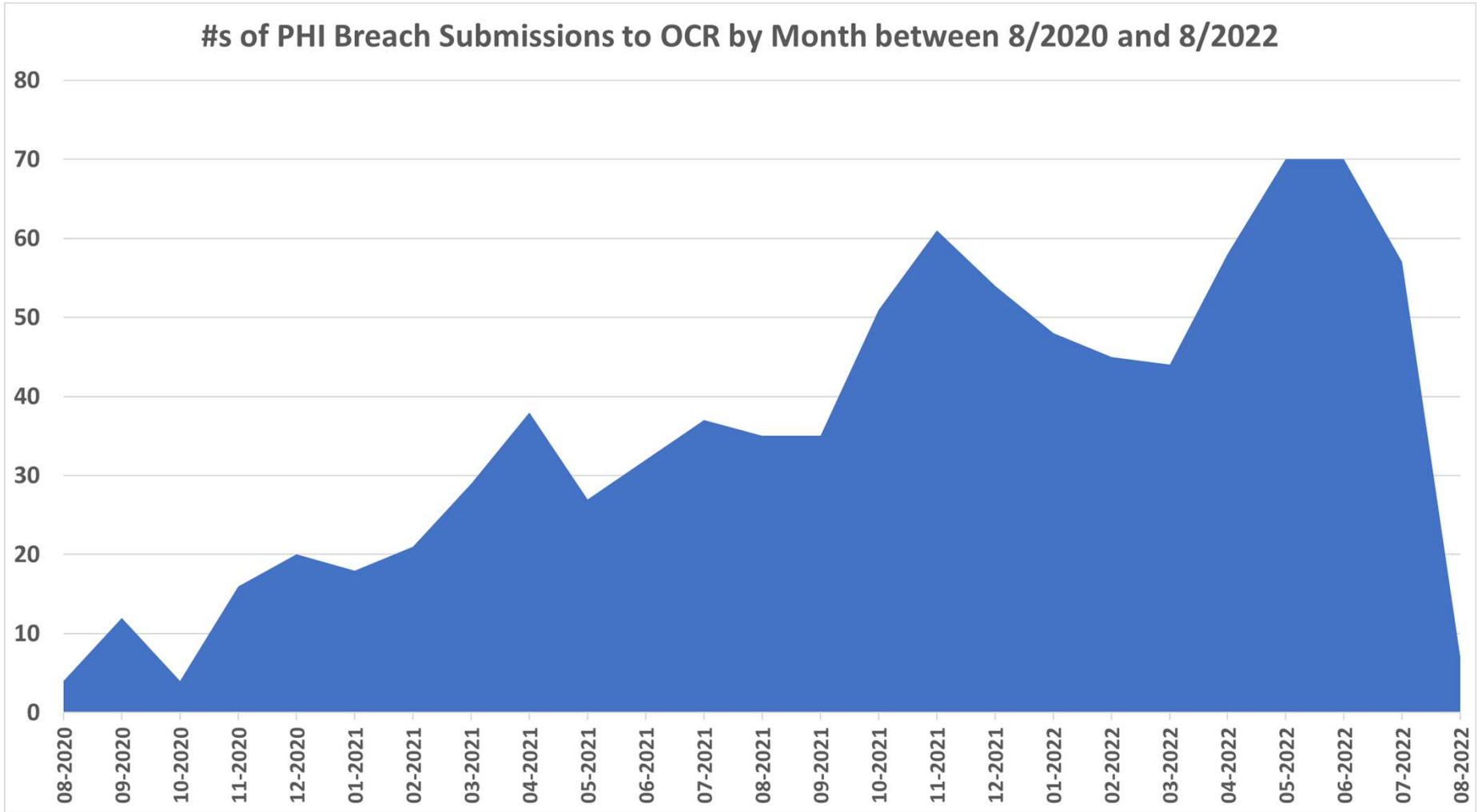
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Cases Currently Under Investigation

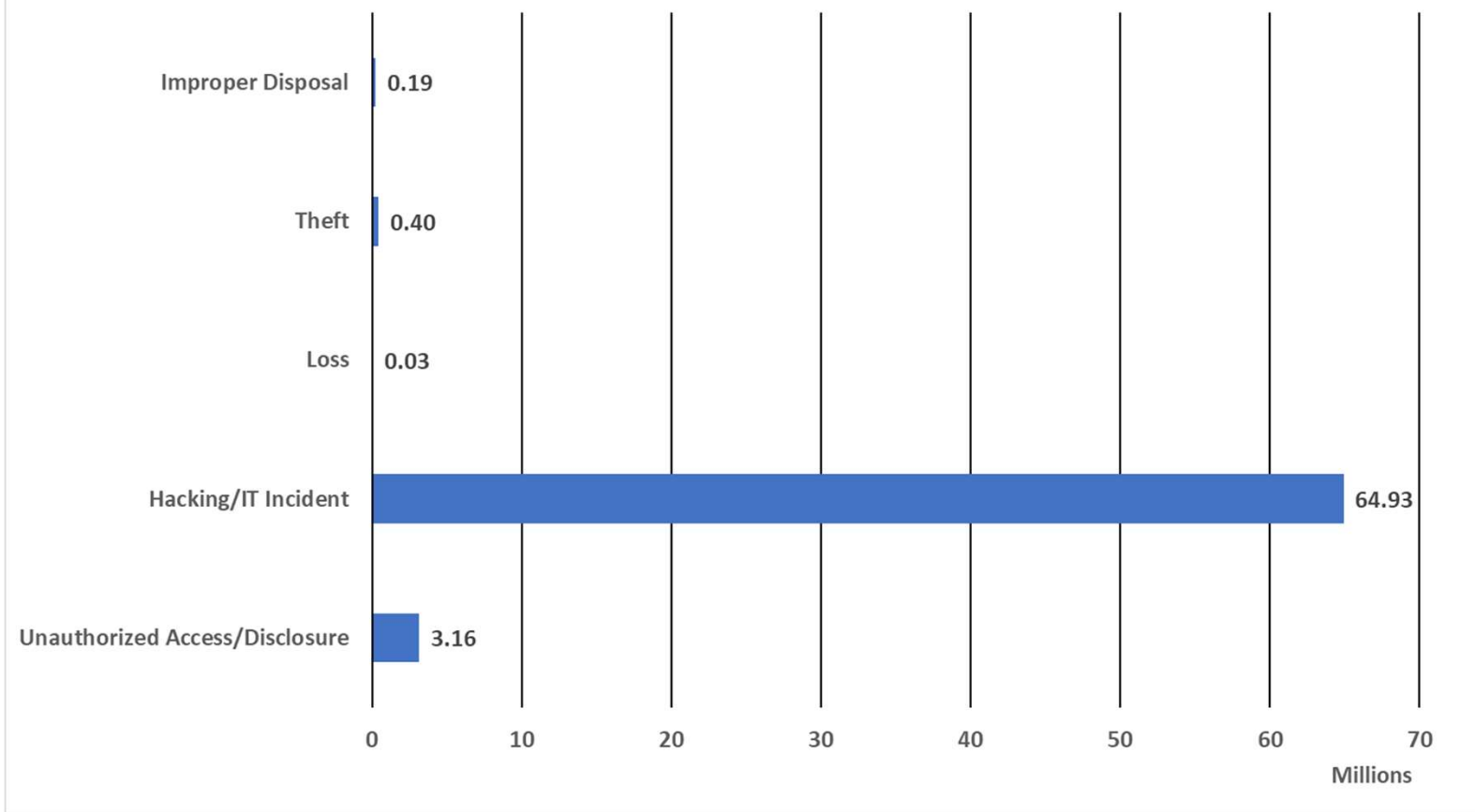
This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

As of Feb 6, 2023 ~876 active investigations of breaches involving > 75,900,000 people's protected health information (PHI). An additional ~4300 previous investigations are now in archive status.

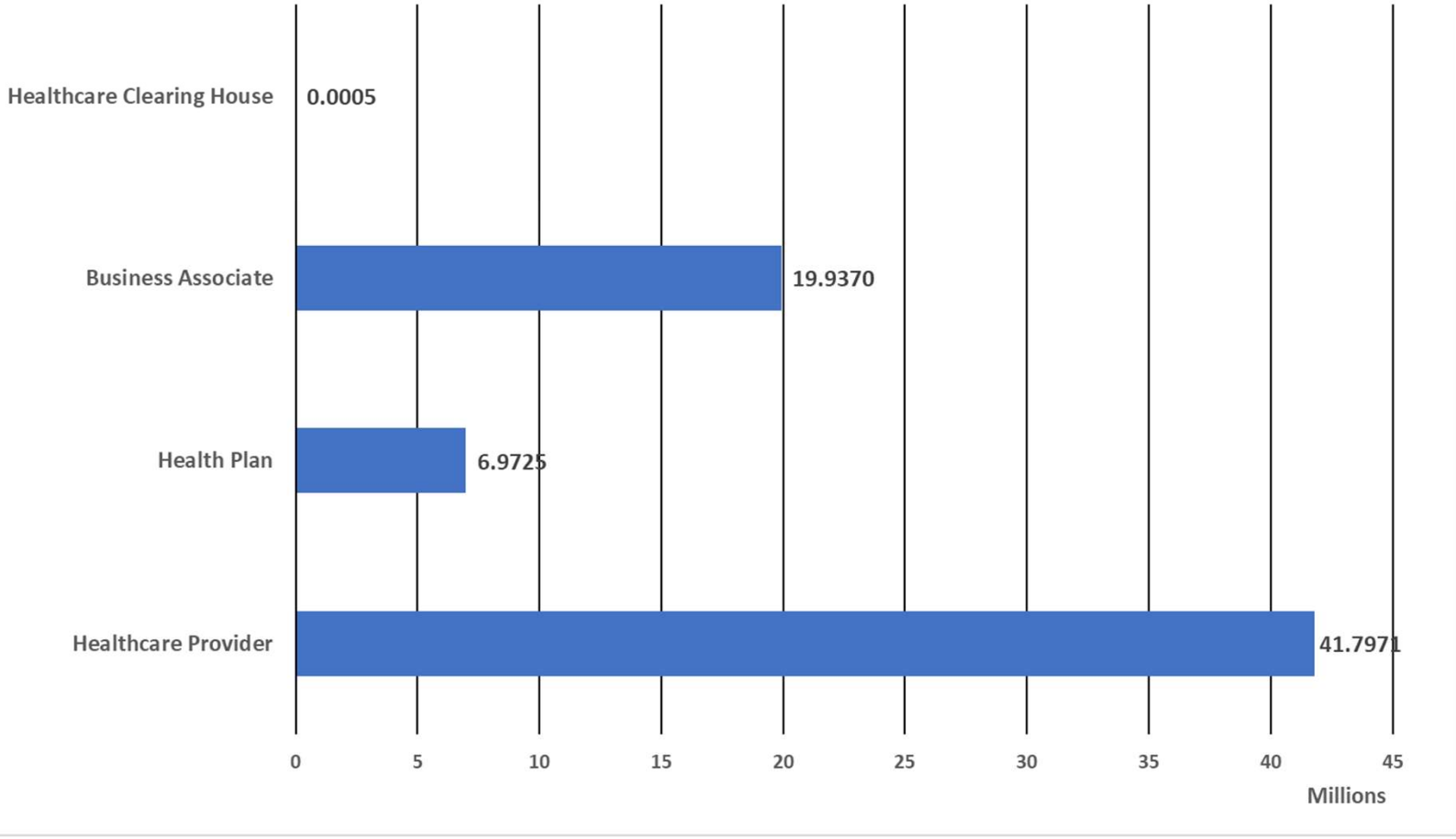
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf



Individuals Affected in Active OCR PHI Breach Investigations as of 8/14/2022 Grouped by Type for Breach



Individuals Affected in Active OCR PHI Breach Investigations as of 8/14/2022
Grouped by Covered Entity Type Responsible for Breach



**Individuals Affected
in Active OCR PHI
Breach Investigations
as of 8/14/2022
Grouped by Location
of Breached
Information**

Location of Breached Information	Individuals Affected
Network Server	53,926,154
Email	9,762,944
Other	1,754,876
Electronic Medical Record	1,011,331
Desktop Computer, Laptop, Network Server	500,000
Electronic Medical Record, Network Server	470,219
Paper/Films	408,856
Email, Other	212,509
Desktop Computer	160,597
Other Portable Electronic Device	143,541
Electronic Medical Record, Other	59,960
Network Server, Other	46,954
Laptop, Other, Other Portable Electronic Device	37,636
Email, Network Server	36,974
Laptop	33,032
Desktop Computer, Electronic Medical Record, Laptop, Network Server	29,227
Email, Laptop	28,332
Desktop Computer, Network Server	25,555
Laptop, Other	24,000
Desktop Computer, Electronic Medical Record, Network Server	13,530
Desktop Computer, Electronic Medical Record, Laptop, Other Portable Electronic Device	3,300
Other, Other Portable Electronic Device	2,869
Laptop, Network Server	2,716
Desktop Computer, Electronic Medical Record	2,371
Desktop Computer, Other Portable Electronic Device	2,287
Network Server, Paper/Films	2,000
Electronic Medical Record, Email, Paper/Films	1,748
Desktop Computer, Laptop, Other Portable Electronic Device	1,580
Electronic Medical Record, Laptop, Network Server	823
Desktop Computer, Electronic Medical Record, Laptop	601
Desktop Computer, Electronic Medical Record, Email, Network Server, Paper/Films	500

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?



Office of the Chair

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

STATEMENT OF THE COMMISSION
On Breaches by Health Apps and Other Connected Devices

September 15, 2021

In recognition of the proliferation of apps and connected devices that capture sensitive health data, the Federal Trade Commission is providing this Policy Statement to offer guidance on the scope of the FTC's Health Breach Notification Rule, 16 C.F.R. Part 318 ("the Rule").¹

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>

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>

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.

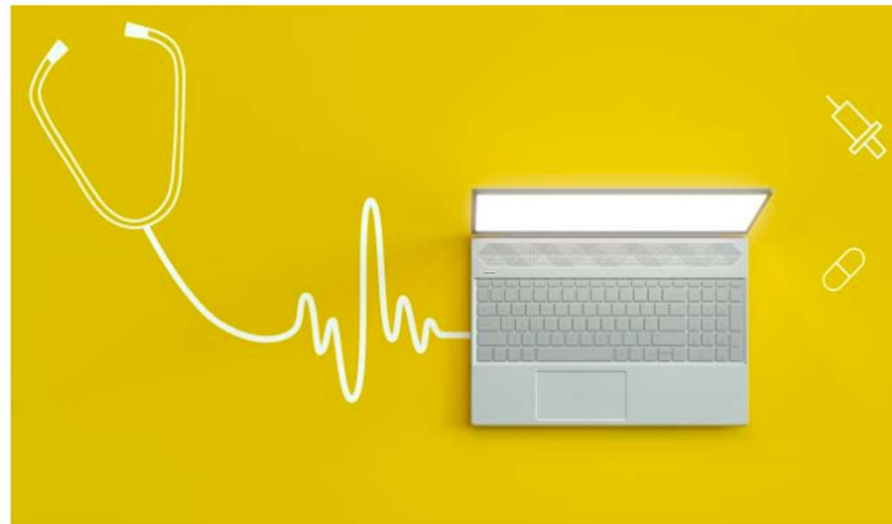
CyberScoop found that Doxy.me, which is used by more than 1 million providers worldwide, was sharing IP addresses and unique device identification numbers with Google, Facebook and marketing software company HubSpot.

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>

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>

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>

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

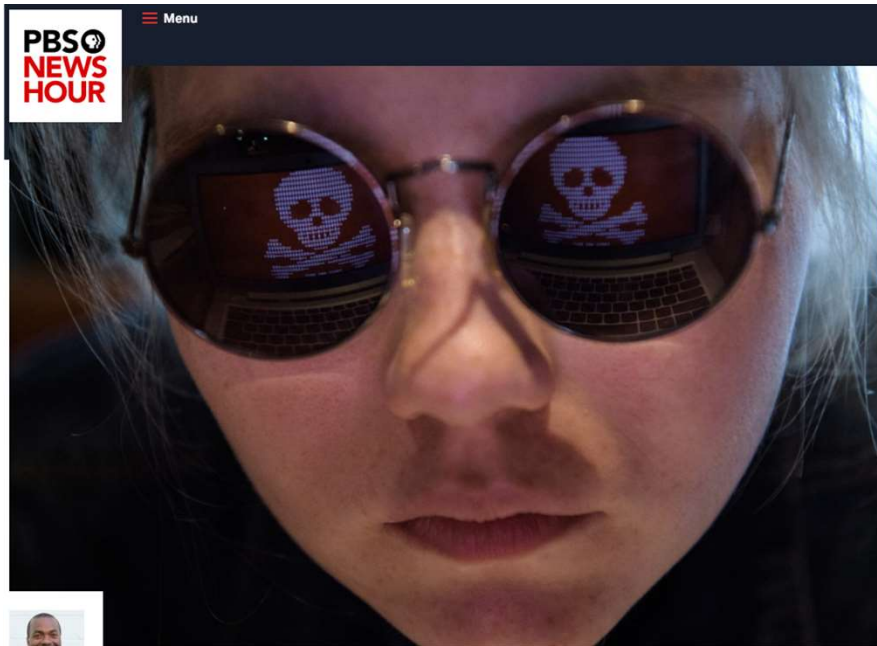
May 10, 2021 by Jessica Davis

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**



Share ...



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>

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.

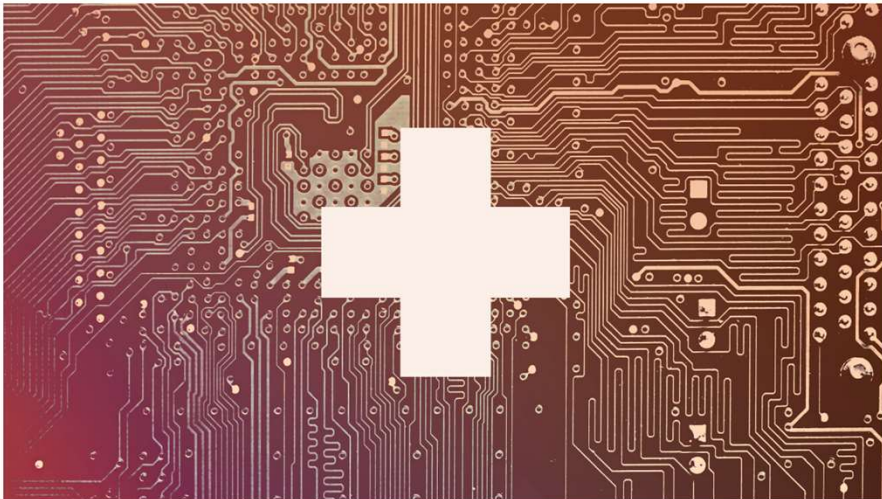
The facilities are owned by **Memorial Health System**, which represents 64 clinics, including hospitals Marietta Memorial, Selby General, and Sistersville General in the Marietta-Parkersburg metropolitan area in West Virginia and Ohio. Early on Sunday, the chain experienced a ransomware attack that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

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



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/>

What is the value of a patient health record on the dark market?



HOSPITALS

Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web

By Paul Nadrag, Capsule Technologies • Jan 26, 2021 01:55pm

Why? Stolen records sell for as much as **\$1,000 each**, according to credit rating agency Experian. Cybersecurity firm Trustwave pegged the black-market value of medical records at **\$250 (PDF)** each. Credit card numbers, on the other hand, sell for around \$5 each on the dark web, according to both sources, while Social Security numbers can be purchased for as little as \$1 each.

<https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web>

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>

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

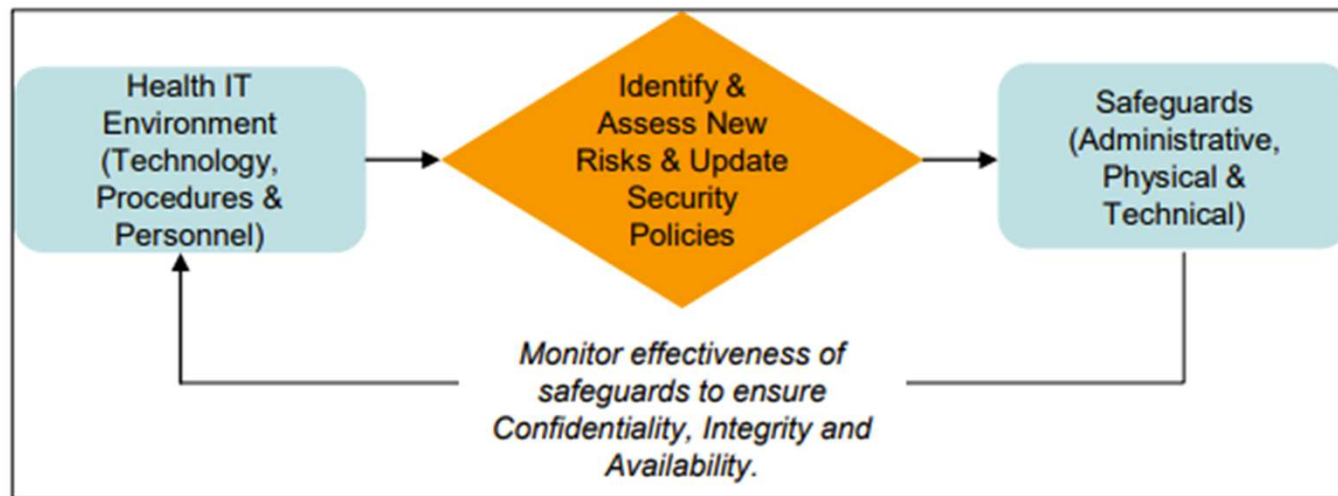
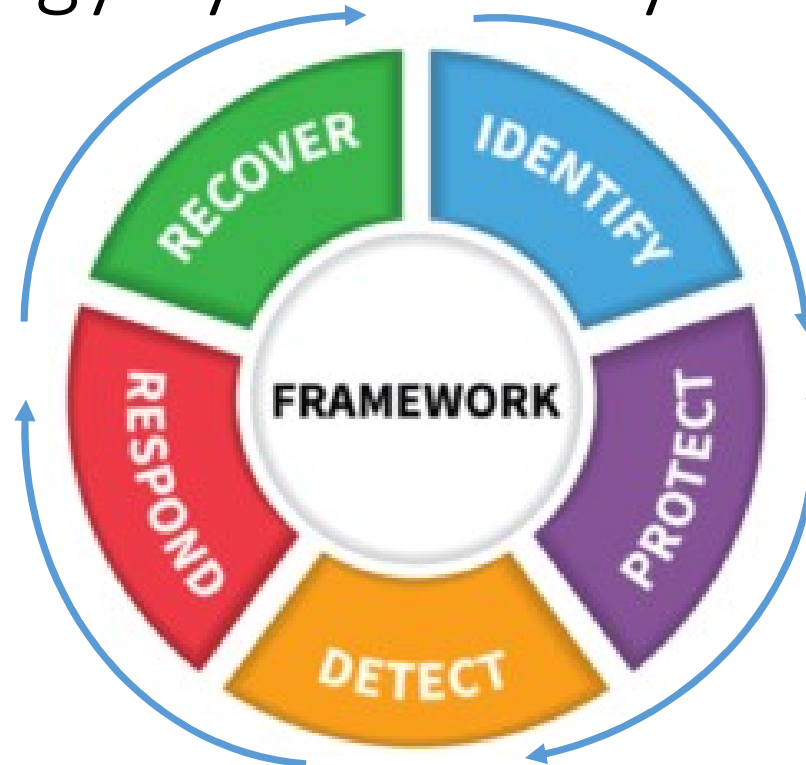


Figure 1: Health Information Security Requires Continual Assessment of Risks to Electronic Health Information

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

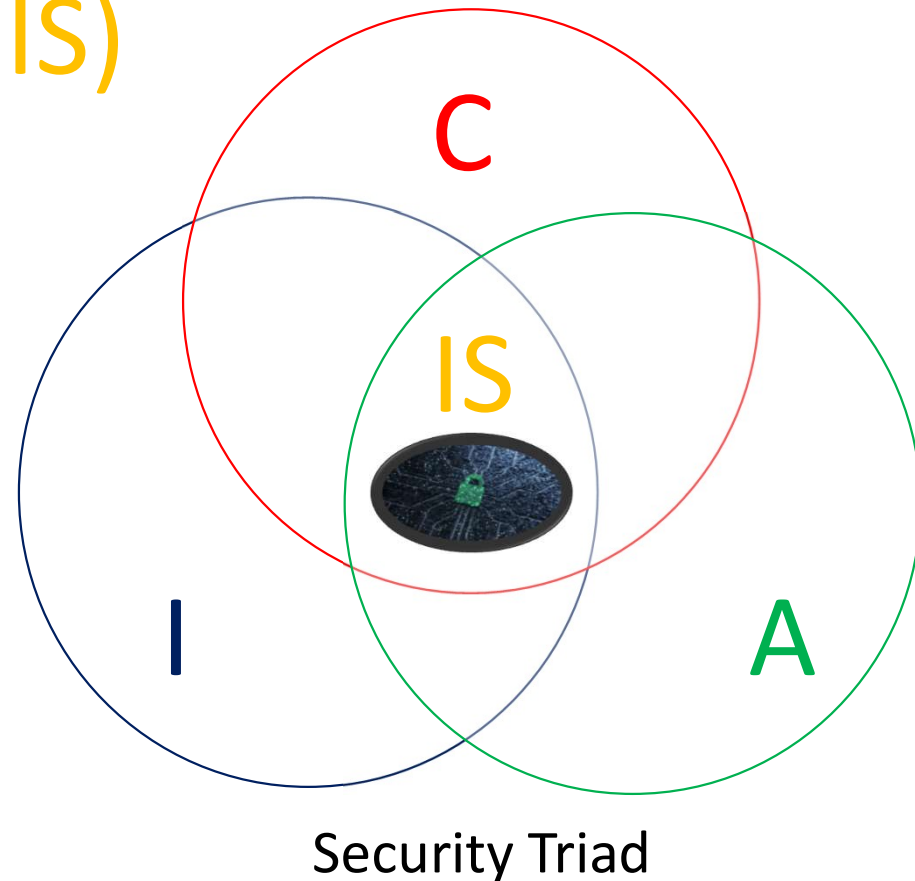
National Institutes of Standards and Technology Cybersecurity Framework



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

Information Security (IS)

- Confidentiality (C)
 - Strict limits on who can access information
- Integrity (I)
 - Protections from improper changes to information
- Availability (A)
 - Access to information is timely and reliable

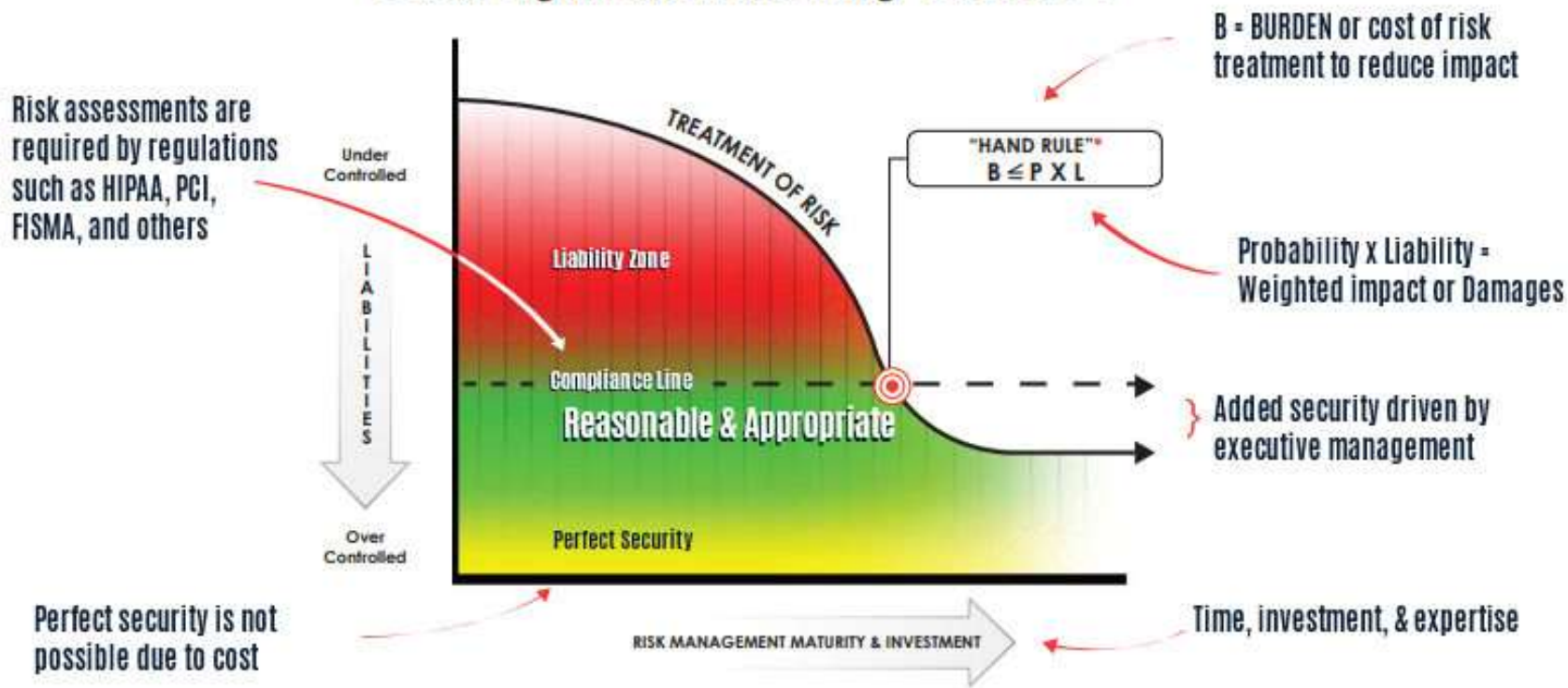


TRUST and PATIENT SAFETY

Confidentiality | Integrity | Availability

- Confidentiality
 - Only authorized individuals
 - With a legal right and/or business need to know, access and utilize
 - Which have been legally granted permission by appropriate authority
- Integrity
 - Information validity & accuracy is reliably maintained
 - Operates as designed and intended
 - Change logs
- Availability
 - Accessible and usable as designed and on demand commensurate with service requirements

Is Your Organization Exercising "Due Care"?



<https://www.halock.com/hand-rule-managing-upper-limits-security-costs/>

https://en.wikipedia.org/wiki/Learned_Hand

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/>

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, don't click it.

- 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 supported by the U.S. Department of Health and Human Services. It is the intellectual property of the Telehealth Resource Center. This document is for informational purposes only and is not intended to constitute an offer of any financial product or service.

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

California Telehealth Resource Center, 2021

<https://telehealthresourcecenter.org/resources/fact-sheets/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.

Disclaimer: This document is for informational purposes only. It does not constitute an offer of insurance, financial product, investment, or any other financial product. For specific information, contact 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 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 Camera 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 devices (operating system, browser, and all other software)

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
- Document all virtual patient interactions and note 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 care securely, from wherever you're working

- Share current 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 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 an offer of insurance, financial product, investment, or any other financial product. For specific information, contact 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
- Document all virtual patient interactions and note 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

<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. © 2021 California Telehealth Resource Center. All rights reserved. For more information, contact the legal counsel or health IT security specialist.

PRACTICE GOOD CYBER HYGIENE

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

- 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 cameras 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

Minimize 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 California Telehealth Resource Center. All rights reserved. For more information, contact the legal counsel or health IT security specialist.

PATIENT SECURITY AND PRIVACY

Minimize 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.

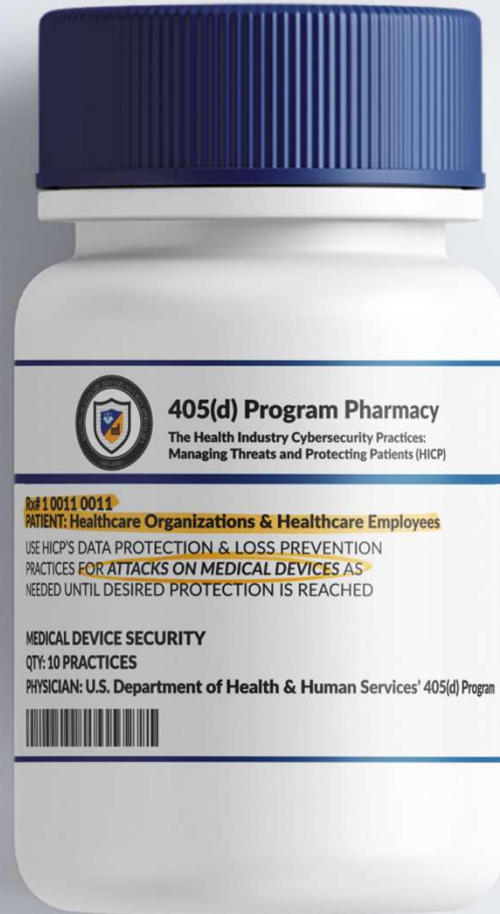
- Think before you click. Email scams are common—if something doesn't feel right, don't click it
- Speak up! Check in with your security or IT department if you have questions or concerns

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

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



HHS 405(d) Aligning Health Care Industry Security Approaches



PRESCRIPTION: Medical Device Security

Medical devices are essential to diagnostic, therapeutic and treatment practices. These devices deliver significant benefits and are successful in the treatment of many diseases. As with all technologies, medical device benefits are accompanied by cybersecurity challenges. Cybersecurity vulnerabilities are introduced when medical devices are connected to a network or computer to process required updates, therefore in order to protect patients it is important to protect these devices. Medical devices are a specialized type of Internet of Things (IoT) device and rather than recreating cybersecurity practices for them, healthcare organizations are encouraged to extend the relevant cybersecurity practices from each of the other prescriptions, and implement them appropriately for medical device management.

Protect yourself and your patients by following the course of treatment below:

For Organizations of All Sizes:

- Establish Endpoint Protection Controls. As with other endpoints, medical devices should follow similar protocols such as installing local firewalls, providing routine patching, network segmentation, and changing default passwords
- Implement Identity and Access Management Policies. Just like endpoints, medical devices security should include authentication measures and remote access controls like multifactor authentication
- Institute asset Management procedures. It is important to follow your asset management procedures for medical devices just as you would for endpoints. Keep an updated list of inventory and software updates to ensure your devices are accounted for and are up to date.
- Create a Vulnerability Management Program that can consume Medical Device Management disclosures and always respond accordingly when received.
- Add security terms to Medical Device Management contracts that enable you to hold device manufacturers accountable.

For more Medical Device Security practices, please visit www.405d.hhs.gov to download a copy of the HICP technical volume for your organization. Check out the available resources 405(d) has to offer by visiting our social media pages @ask405d on Facebook, Twitter, and Instagram!

<https://405d.hhs.gov/protect>

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>

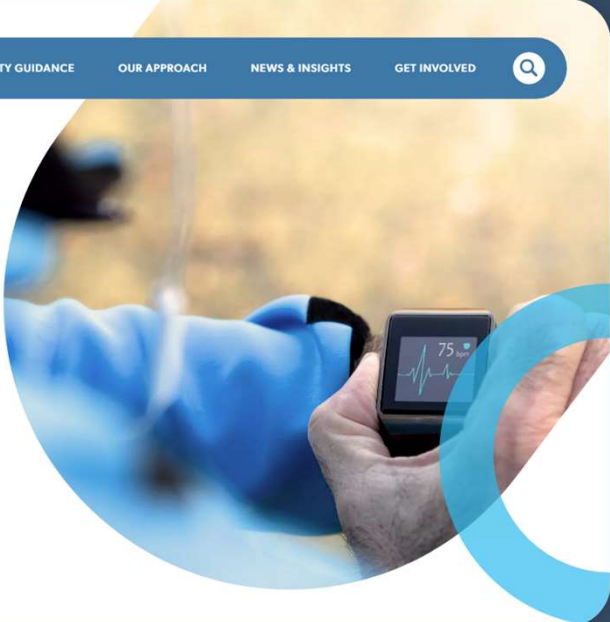
< NIST

Home > Security Guidance > Securing Telehealth Remote Patient Monitoring Ecosystem

 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE


SECURITY GUIDANCE OUR APPROACH NEWS & INSIGHTS GET INVOLVED 


Securing Telehealth Remote Patient Monitoring Ecosystem



Traditionally, patient monitoring systems have been deployed in healthcare facilities, in controlled environments. Remote patient monitoring (RPM), however, is different in that monitoring equipment is deployed in the patient's home. These new capabilities can involve third-party platform providers utilizing videoconferencing capabilities, and may leverage cloud and internet technologies coupled with RPM devices. As the use of these capabilities continues to grow, it is important to ensure the infrastructure supporting them can maintain the confidentiality, integrity, and availability of patient data.

A distributed solution that enables health delivery organizations to better secure their remote patient monitoring ecosystem

 STATUS: FINALIZED PRACTICE GUIDE

 NIST SP 1800-30: Complete Guide (PDF)

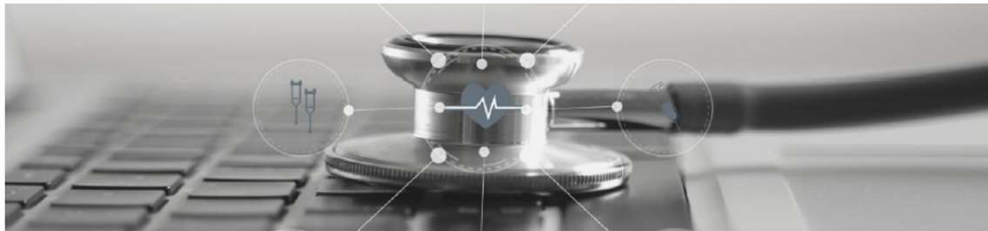
<https://www.nccoe.nist.gov/healthcare/securing-telehealth-remote-patient-monitoring-ecosystem>



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>

ARIZONA
TELEMEDICINE
PROGRAM



Thank you!

Questions?

mholcomb@telemedicine.arizona.edu

