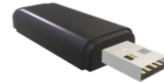


ARIZONA
TELEMEDICINE
PROGRAM



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



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



Protected Health Information

Protected health information (PHI) includes all individually identifiable health information relating to the past, present or future health status, provision of health care, or payment for health care of/for an individual that is created or received by a Covered Entity or Business Associate.

Health information is individually identifiable if it contains any of the following identifiers:

- Names
- Geographic subdivisions smaller than a state
- Dates (except year only) directly related to an individual, including birth date, date of death, admission date, discharge date; and all ages over 89 (except ages may be aggregated into a single category of age 90 or older)
- Telephone and fax numbers
- Email addresses
- Social security numbers (SSN)
- Medical record numbers (MRN)
- Health plan beneficiary numbers
- Account numbers
- Certificate/driver's license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URL)
- Internet Protocol (IP) addresses
- Biometric identifiers (including finger and voice prints)
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code.

Link to new version of this document:

https://research.arizona.edu/sites/default/files/q_is_it_phi.pdf

*A Business Associate Agreement (BAA) is required to be entered into between a Covered Entity and/or Business Associate and any downstream Subcontractor(s) that create, maintain, receive, access or store PHI on behalf of a Covered Entity/Business Associate *prior* to use or disclosure of any PHI.



The Southwest TRC is a subsidiary of



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

Southwest Telehealth Resource Center Blog

Patient Data Breaches: Threat to Health IT & Telemedicine in 2016 and Beyond

By Jared Alfson on Jun 01, 2016



\$363. That's how much a **single stolen patient health record** is worth on the dark market, **according to data from the Ponemon Institute**, making it worth more than any other piece of data from any other industry. In fact, **your medical information is worth 10 times more than your credit card number.**

<https://southwesttrc.org/blog/2016/patient-data-breaches-threat-health-it-telemedicine-2016-and-beyond>

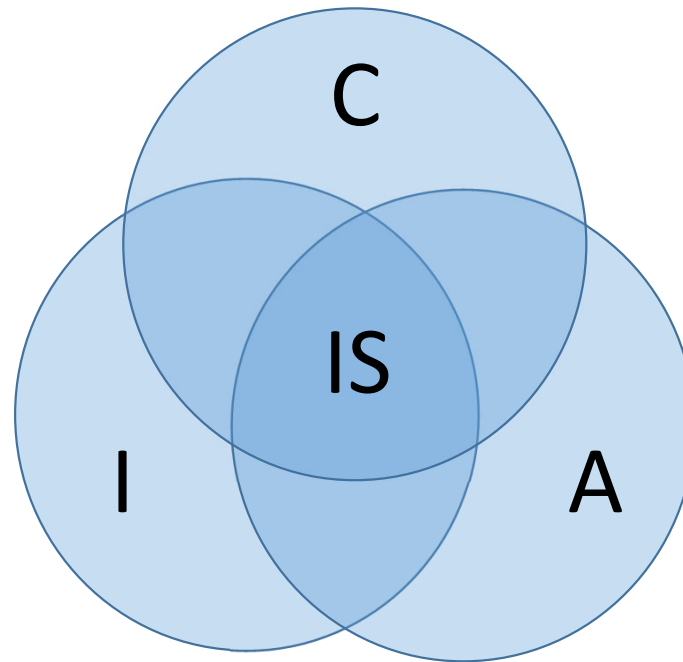


© 2022 ARIZONA TELEMEDICINE PROGRAM



Information Security (IS)

- Confidentiality (C)
- Integrity (I)
- Availability (A)



TRUST and PATIENT SAFETY

Confidentiality | Integrity | Availability

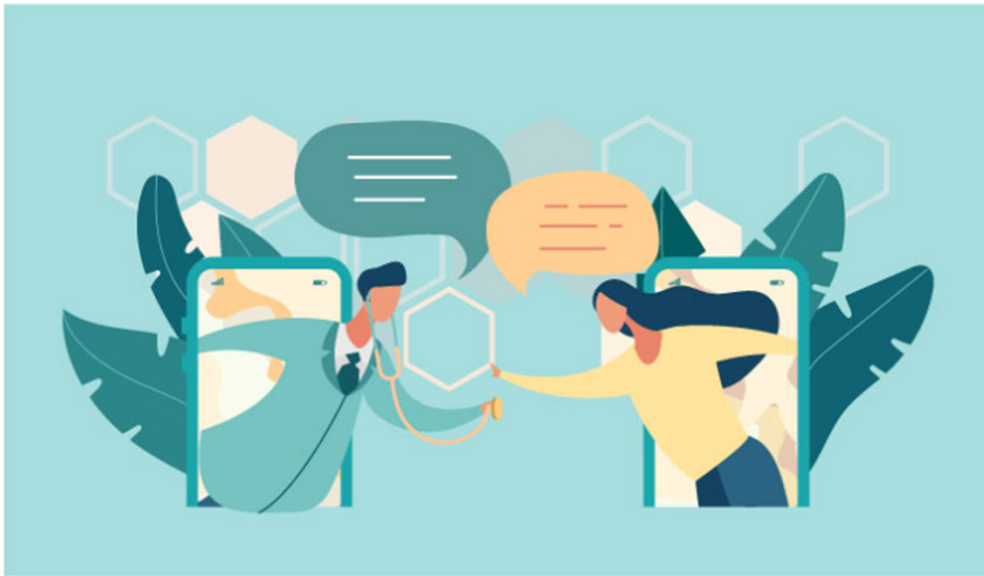
- Confidentiality
 - Only authorized individuals
 - With a legal right and/or business need to know, access and utilize
 - Which have been legally granted permission by appropriate authority
- Integrity
 - Information validity & accuracy is reliably maintained
 - Operates as designed and intended
 -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

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

Managing Telehealth, Remote Patient Monitoring Security Concerns

Industry experts weigh in on how the healthcare sector can manage telehealth and remote patient monitoring security concerns.



Source: Getty Images



Jill McKeon

Assistant Editor

jmckeon@xtelligentmedia.com

“January 27, 2022 - As adoption increases, healthcare organizations, vendors, and providers will continually be tasked with managing telehealth and remote patient monitoring (RPM) security concerns. Although these technologies existed before, the pandemic prompted the need for safe and secure telehealth and RPM solutions that could be deployed on a larger scale.

But that rapid drive toward telehealth naturally comes with security risks. While they may not outweigh the tremendous benefits that telehealth offers to both patients and providers, security concerns must be considered carefully.”

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

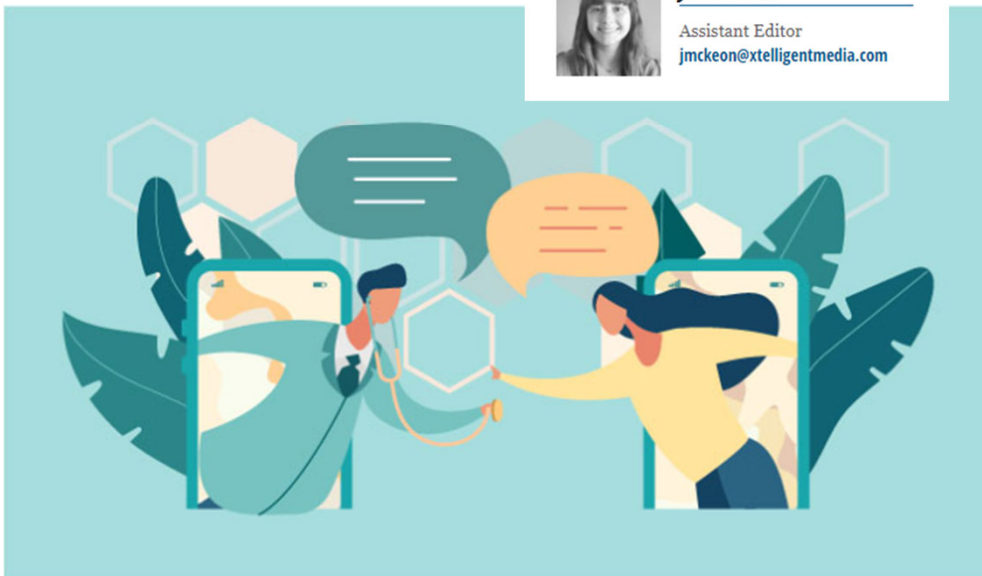
Managing Telehealth, Remote Patient Monitoring Security Concerns

Industry experts weigh in on how the healthcare sector can manage telehealth and remote patient monitoring security concerns.



Jill McKeon

Assistant Editor
jmckeon@xtelligentmedia.com



Source: Getty Images

“A recent survey conducted by Arlington Research and commissioned by Kaspersky found that over 80 percent of surveyed [healthcare providers globally harbor concerns about data security and privacy](#).

More than half of respondents reported experiencing cases where patients refused to participate in telehealth services because they did not trust that the technology would protect their privacy and security.

In addition, 70 percent of respondents said that their practice used outdated legacy operating systems, exposing them to security vulnerabilities. Despite these concerns, respondents largely agreed that telehealth would add the most value to the healthcare sector in the next five years compared to any other technology.

Matthias Wollnik, product marketing manager of security at Jamf, noted that the rapid implementation of telehealth services by many healthcare organizations at the onset of the pandemic also prompted security risks.”

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

Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency

The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) is responsible for enforcing certain regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, to protect the privacy and security of protected health information, namely the HIPAA Privacy, Security and Breach Notification Rules (the HIPAA Rules).

Telehealth Discretion During Coronavirus

During the COVID-19 national emergency, which also constitutes a nationwide public health emergency, covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules.

OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency.

This notification is effective immediately.

<https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>

Under this Notice, however, Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth by covered health care providers.

Covered health care providers that seek additional privacy protections for telehealth while using video communication products should provide such services through technology vendors that are HIPAA compliant and will enter into HIPAA business associate agreements (BAAs) in connection with the provision of their video communication products. The list below includes some vendors that represent that they provide HIPAA-compliant video communication products and that they will enter into a HIPAA BAA.

- Skype for Business / Microsoft Teams
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet
- Cisco Webex Meetings / Webex Teams
- Amazon Chime
- GoToMeeting
- Spruce Health Care Messenger



FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency

9. What may constitute bad faith in the provision of telehealth by a covered health care provider, which would not be covered by the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications?

OCR would consider all facts and circumstances when determining whether a health care provider's use of telehealth services is provided in good faith and thereby covered by the Notice. Some examples of what OCR may consider a bad faith provision of telehealth services that is not covered by this Notice include:

- Conduct or furtherance of a criminal act, such as fraud, identity theft, and intentional invasion of privacy;
- Further uses or disclosures of patient data transmitted during a telehealth communication that are prohibited by the HIPAA Privacy Rule (e.g., sale of the data, or use of the data for marketing without authorization);
- Violations of state licensing laws or professional ethical standards that result in disciplinary actions related to the treatment offered or provided via telehealth (i.e., based on documented findings of a health care licensing or professional ethics board); or
- Use of public-facing remote communication products, such as TikTok, Facebook Live, Twitch, or a public chat room, which OCR has identified in the Notification as unacceptable forms of remote communication for telehealth because they are designed to be open to the public or allow wide or indiscriminate access to the communication.

<https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf>



HOME >> PATIENT-CENTERED CARE

JUL
30
2021

PATIENT-CENTERED CARE

How Telemedicine Requirements and Policies Will Change Post-Pandemic



The public health emergency led to a loosening of telemedicine requirements and an uptick in virtual care use, but are these changes here to stay?



by Jordan Scott 

Jordan Scott is the web editor for *HealthTech*. She is a multimedia journalist with experience in B2B publishing.

Some telehealth restrictions were lifted at the beginning of the pandemic out of necessity, a major factor in the rapid expansion of virtual care services. However, many providers are wondering if those changes are here to stay or if a tightening of telemedicine requirements will lead to a "telehealth cliff."

<https://healthtechmagazine.net/article/2021/07/how-telemedicine-requirements-and-policies-will-change-post-pandemic-perfcon>

DIGITAL

Need for glide path on HIPAA telehealth rules at pandemic's end

JAN 31, 2022



Tanya Albert Henry
Contributing News Writer

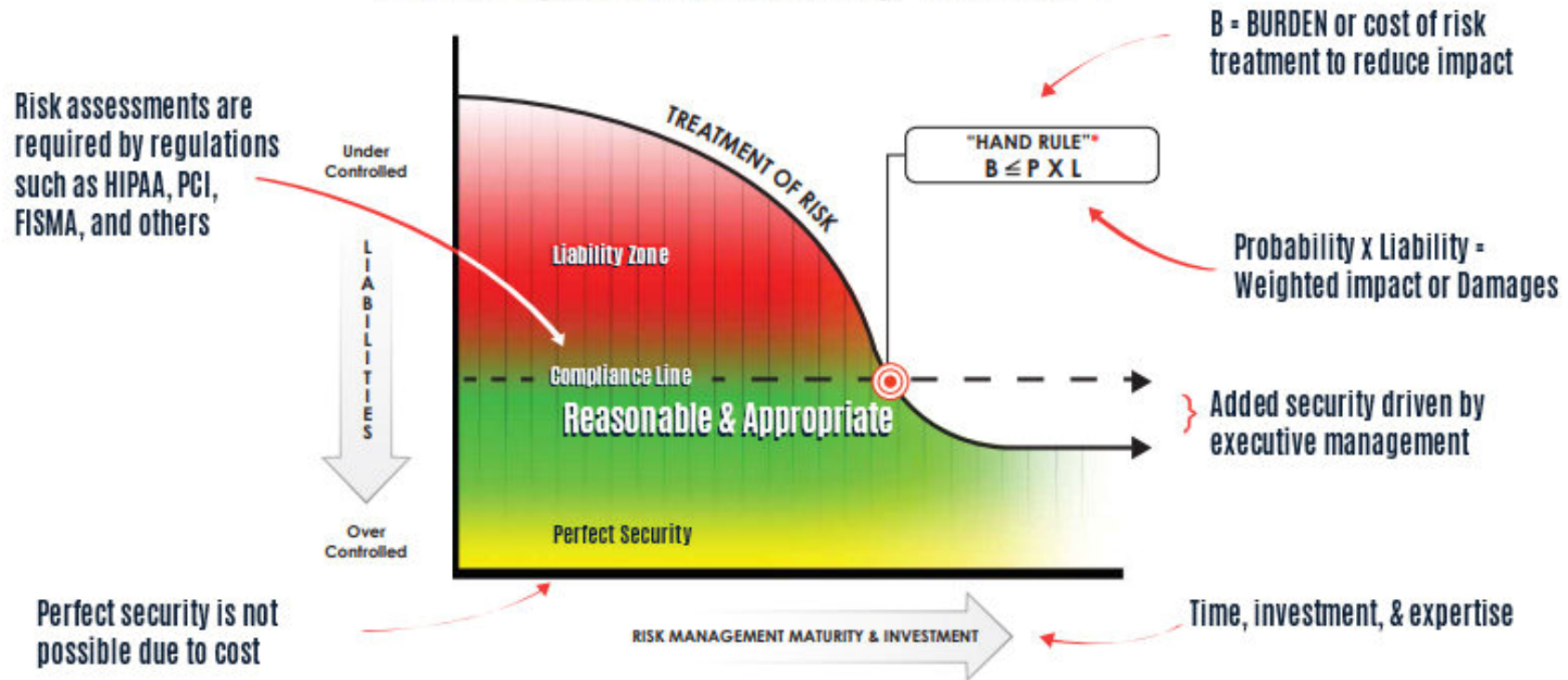


“..The AMA also advised physicians to “enable and activate all available privacy and security features of the platform they selected..”

Though the pandemic's end is nowhere near, when it does arrive the national declaration of a public health emergency will likely soon end along with it. When the public health emergency declaration is eventually ended, the AMA is asking the government to give physicians who quickly pivoted to include telehealth in their practice ample time to meet Health Insurance Portability and Accountability Act (HIPAA) requirements before audits and other enforcement measures ramp up.

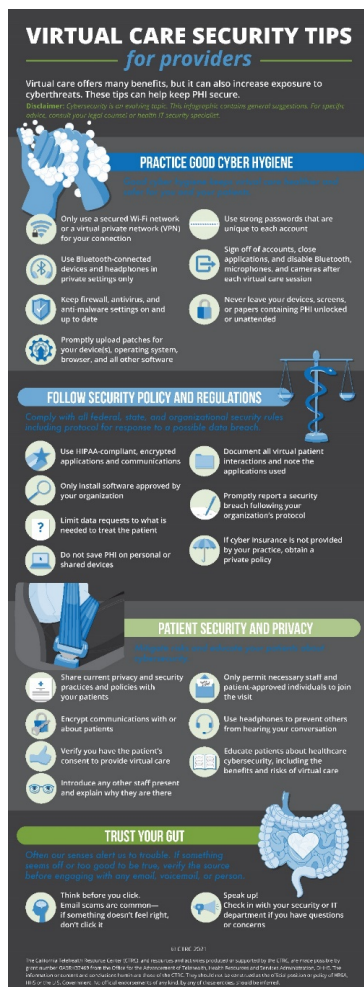
<https://www.ama-assn.org/practice-management/digital/need-glide-path-hipaa-telehealth-rules-pandemic-s-end>

Is Your Organization Exercising "Due Care"?

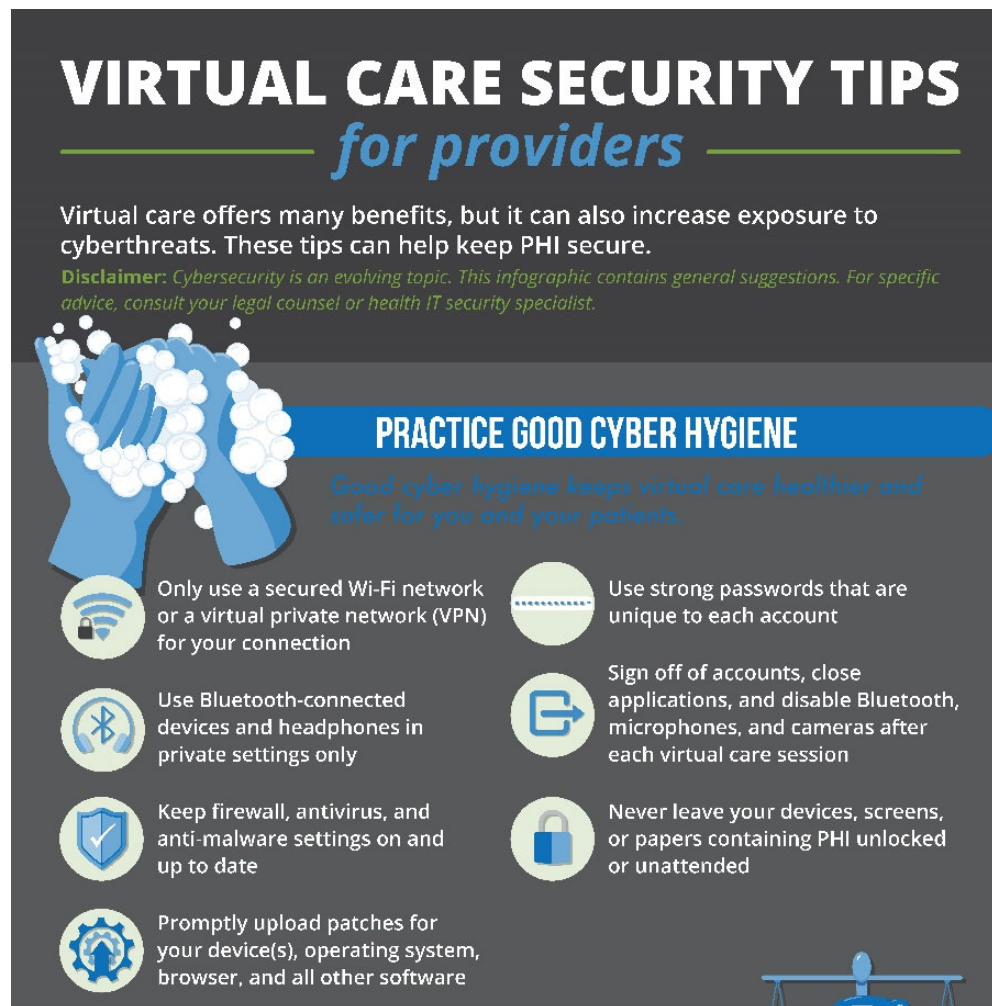


<https://www.halock.com/hand-rule-managing-upper-limits-security-costs/>

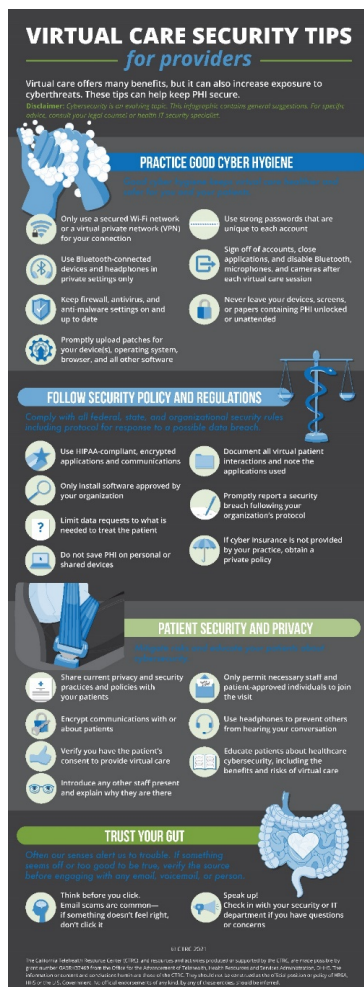
https://en.wikipedia.org/wiki/Learned_Hand



California Telehealth Resource Center, 2021



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

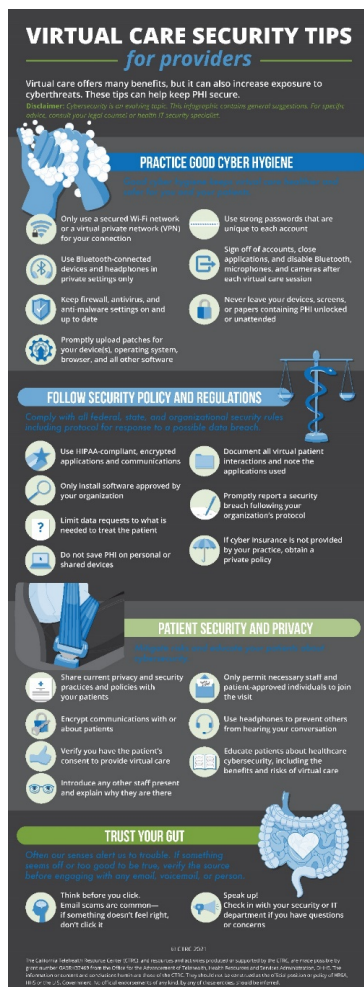


your device(s), operating system, browser, and all other software

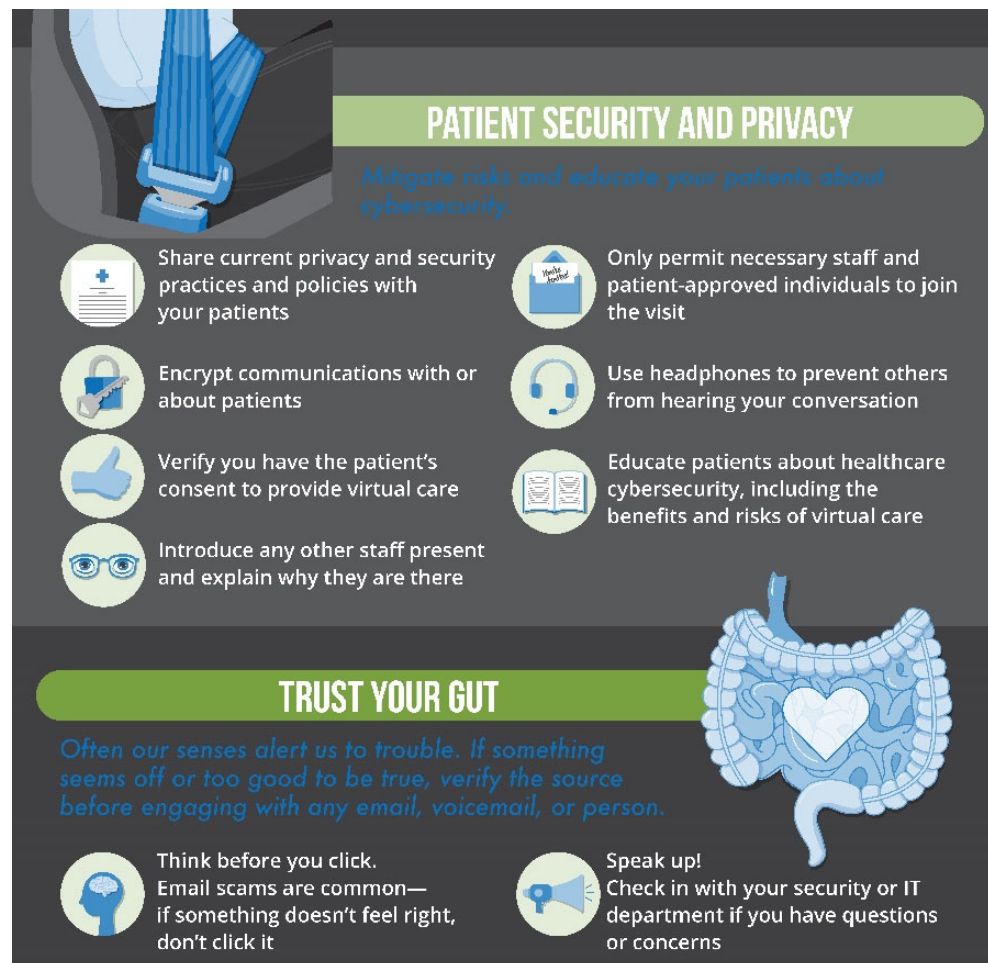
FOLLOW SECURITY POLICY AND REGULATIONS
Comply with all federal, state, and organizational security rules including protocol for response to a possible data breach.

- 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/fact-sheets/virtual-care-security-tips-for-providers/>



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

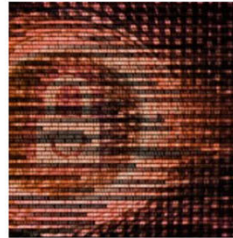


<https://telehealthresourcecenter.org/resources/factsheets/virtual-care-security-tips-for-providers/>

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...

HHS Launches New Website to Align Healthcare Cybersecurity

HHS launched a website for the 405(d) Program, which is comprised of a task force focused on aligning healthcare cybersecurity approaches across the sector.



By **Jill McKeon**

December 06, 2021 - HHS **launched** a new website for its 405(d) Program with the goal of aligning healthcare cybersecurity across the industry. Under the Cybersecurity Act of 2015, HHS established the 405(d) Aligning Health Care Industry Security Approaches Program and the 405(d) Task Group, which is comprised of more than 150 industry and government experts.

The program aims to uphold the motto that “cyber safety is patient safety,” and its website contained resources, videos, products, and tools to help raise awareness and promote cybersecurity best practices, the HHS announcement stated.

“Healthcare professionals understand the importance of hand washing when it comes to mitigating the spread of diseases. Similarly, we know that cybersecurity practices reduce the risk of cyber-attacks and data breaches,” the **website** maintained.

<https://healthitsecurity.com/news/hhs-launches-new-website-to-align-healthcare-cybersecurity>





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

Absence of Cybersecurity is a(n)

Provider **RISK**

The 405(d) Program and Task Group is a collaborative effort between industry and the federal government, which aims to **raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats** to the sector. Please explore our website to learn more about our effort and all products and resources available to our stakeholders.

Subscribe

Contact Us



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)



© 2022 ARIZONA TELEMEDICINE PROGRAM





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](#)

Absence of Cybersecurity is a(n)

Provider **RISK**

The 405(d) Program and Task Group is a collaborative effort between industry and the federal government, which aims to **raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats** to the sector. Please explore our website to learn more about our effort and all products and resources available to our stakeholders.

[Subscribe](#)

[Contact Us](#)

Patient **RISK**

Organization **RISK**

Enterprise **RISK**

0:00 / 4:21

[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)



© 2022 ARIZONA TELEMEDICINE PROGRAM





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)



ARIZONA
TELEMEDICINE
PROGRAM

© 2022 ARIZONA TELEMEDICINE PROGRAM



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 7, 2022 ~875 active
investigations of breaches
involving > 61,000,000 people's
protected health information

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

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

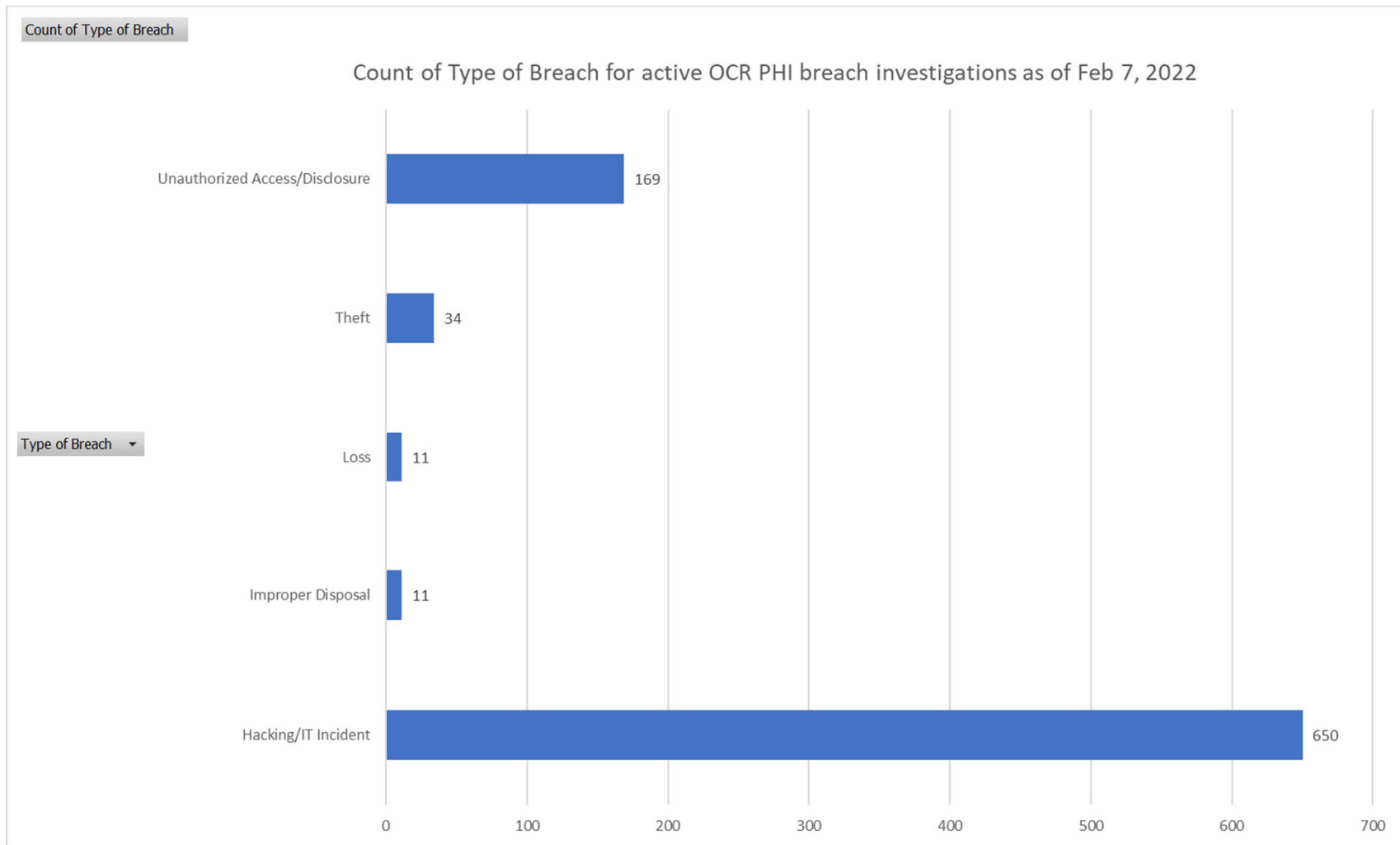
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

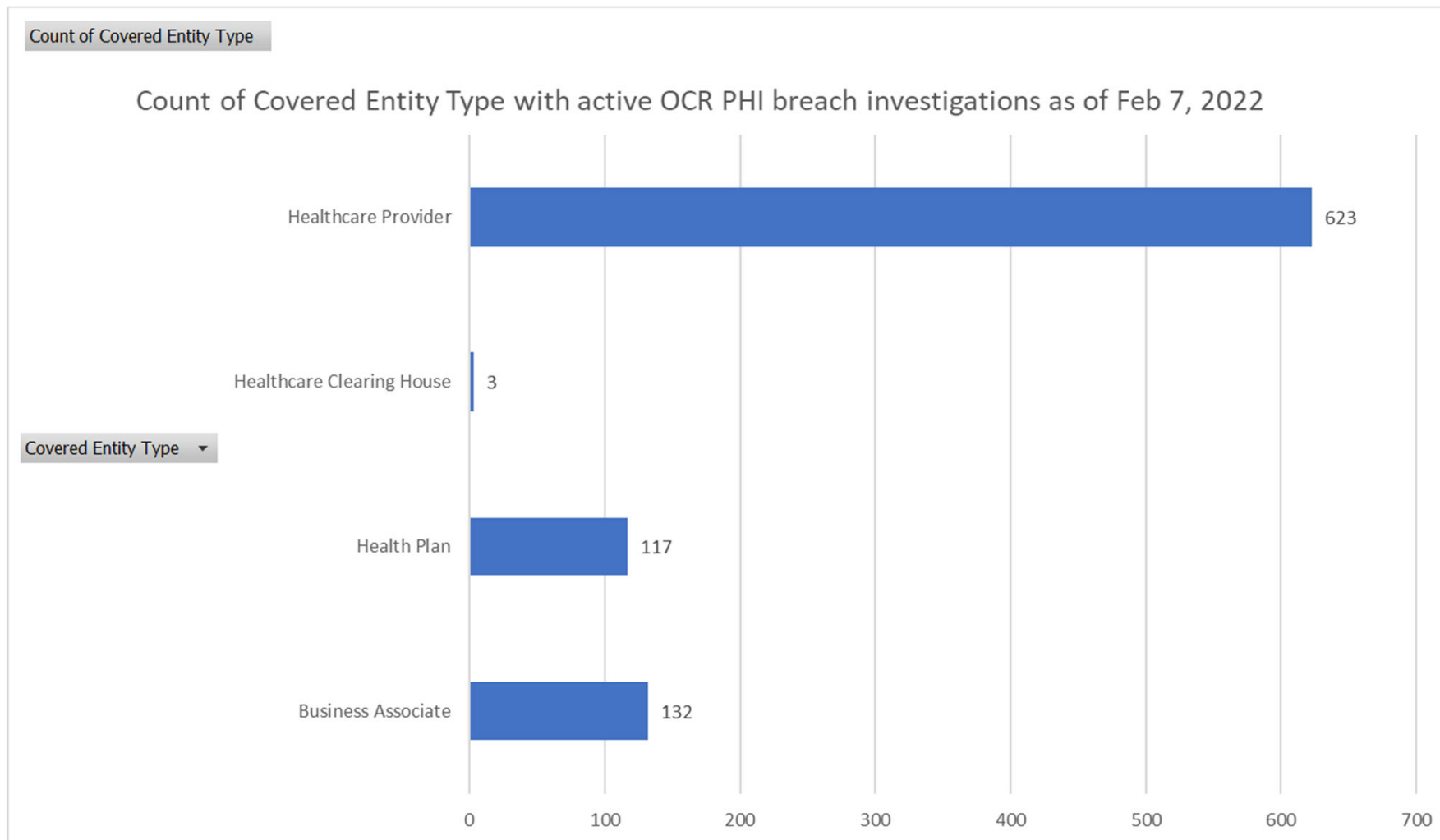
Cases Currently Under Investigation

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

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
⊞	Seneca Family of Agencies	CA	Business Associate	1528	01/22/2022	Hacking/IT Incident	Network Server
⊞	Medical Healthcare Solutions, Inc.	MA	Business Associate	133997	01/22/2022	Hacking/IT Incident	Network Server
⊞	iRise Florida Spine and Joint Institute, LLC	FL	Healthcare Provider	61595	01/21/2022	Hacking/IT Incident	Email
⊞	Independence Blue Cross	PA	Health Plan	591	01/21/2022	Hacking/IT Incident	Network Server
⊞	County of Kings, a political subdivision of the State of California	CA	Healthcare Provider	16590	01/21/2022	Hacking/IT Incident	Network Server
⊞	Walgreen Co.	IL	Healthcare Provider	1471	01/21/2022	Unauthorized Access/Disclosure	Paper/Films
⊞	University of Arkansas for Medical Sciences	AR	Healthcare Provider	518	01/21/2022	Unauthorized Access/Disclosure	Email
⊞	Allegheny Health Network Home Infusion, LLC	PA	Healthcare Provider	7500	01/21/2022	Hacking/IT Incident	Network Server
⊞	Advocates, Inc.	MA	Healthcare Provider	68236	01/21/2022	Hacking/IT Incident	Network Server
⊞	Abington Memorial Hospital (dba Jefferson Abington Hospital)	PA	Healthcare Provider	3475	01/20/2022	Hacking/IT Incident	Network Server
⊞	Thomas Jefferson University Hospital, Inc.	PA	Healthcare Provider	5239	01/20/2022	Hacking/IT Incident	Network Server
⊞	Medical Review Institute of America	UT	Business Associate	2406	01/20/2022	Hacking/IT Incident	Network Server
⊞	Caring Communities	IL	Business Associate	1659	01/20/2022	Hacking/IT Incident	Other
⊞	Colorado Department of Human Services	CO	Healthcare Provider	6132	01/19/2022	Hacking/IT Incident	Network Server
⊞	Golden State Dermatology	CA	Healthcare Provider	1010	01/19/2022	Unauthorized Access/Disclosure	Paper/Films
⊞	Practolytics LLC	SC	Business Associate	1125	01/18/2022	Unauthorized Access/Disclosure	Electronic Medical Record
⊞	Raveco Medical	NY	Healthcare Provider	4897	01/17/2022	Hacking/IT Incident	Network Server
⊞	Volunteers of America Southwest California	CA	Healthcare Provider	1300	01/14/2022	Hacking/IT Incident	Email
⊞	Fiondella, Milone & LaSaracina, LLP	CT	Business Associate	6215	01/14/2022	Hacking/IT Incident	Network Server

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





SCIENCE

HEALTH CARE'S HUGE CYBERSECURITY PROBLEM

Cyberattacks aren't just going after your data

By [Nicole Wettsman](#) | Apr 4, 2019, 9:30am EDT

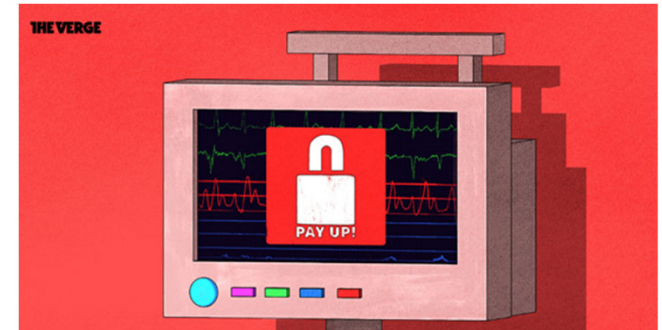
Illustration by Alex Castro / The Verge



SHARE

The patient lying on the emergency room table in front of Paul Pugsley was having a stroke. Time was running out. Pugsley, an emergency medicine resident at Maricopa Medical Center, knew he needed to send the patient for a CT scan.

But when Pugsley looked over at the computer screen at the side of the room, he saw a pop-up message demanding bitcoin payment. A few minutes later, he was told that the same message had shut down the scanner — he'd have to help the patient without knowing whether the stroke was caused by a bleed or a clot, information that's usually vital to the course of treatment.



<https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation>

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/>

A patient has died after ransomware hackers hit a German hospital

This is the first ever case of a fatality being linked to a cyberattack.

by **Patrick Howell O'Neill**

September 18, 2020

<https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/>



PHOTO BY HUSH NAIDOO ON UNSPLASH

Computing / Cybersecurity

Ransomware did not kill a German hospital patient


Still, police warn that it's only a matter of time before hacking hospitals leads to tragic results.

by **Patrick Howell O'Neill**

November 12, 2020

<https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/>

PBS NEWS HOUR Menu



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

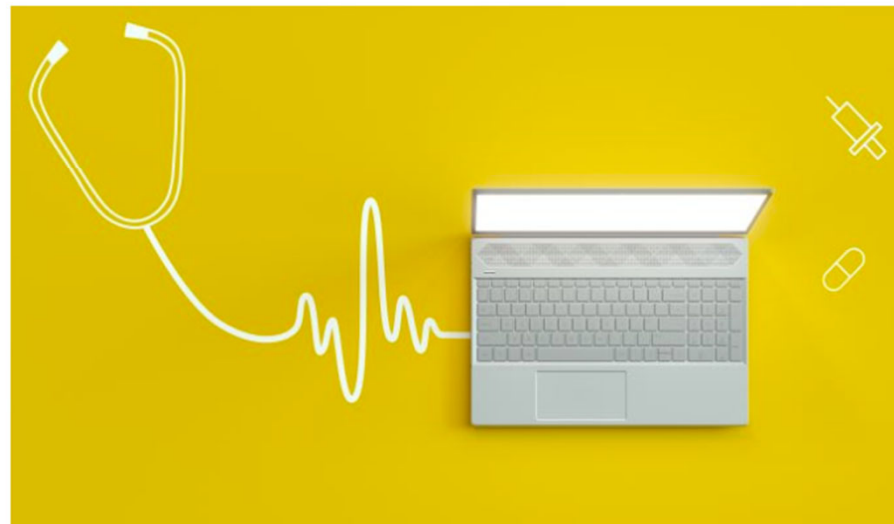
The [ransomware attack](#) that targeted Mobile, Alabama-based Springhill Medical Center in July 2019 knocked the hospital's IT systems offline for more than three weeks, according to the report – necessitating a return to paper charting, disrupting staff communication and compromising visibility of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

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/>

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**
Intelligent 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>





TELEHEALTH AWARENESS WEEK | ABOUT JOIN LOGIN 

Membership News Policy Events Communities Resources

Telehealth Basics Research Practice Guidelines Recorded Content COVID-19



APRIL 30, 2020
TELEHEALTH FUNDAMENTALS
ATA

ATA Urges Health Care Providers New to Telehealth Have Proper Safeguards to Ensure Patient Safety, Data Privacy and Security During COVID-19 Respons

<https://www.americantelemed.org/resources/ata-urges-health-care-providers-new-to-telehealth-have-proper-safeguards-to-ensure-patient-safety-data-privacy-and-security-during-covid-19-respons/>

<https://www.medtechintelligence.com/column/remote-telehealth-driven-world-poses-new-concerns-for-medical-device-security/>

October 28, 2020

MEDdesign

Remote, Telehealth-Driven World Poses New Concerns for Medical Device Security

By Bill Enos

No Comments



Medical device security needs to address the cyber-physical threats, not just patient health information risk.

Increased use of telehealth, forced by the global COVID-19 pandemic, arrived at a time when heightened connectivity of medical devices to computer networks and a convergence of technologies already exposed devices and software applications to a variety of threats. The need to protect patient data from cyberattacks is well understood, but the potential risks from such hacking for clinical care and patient safety haven't been addressed adequately by healthcare organizations, regulators and medical device manufacturers.

The inherent security risk with medical devices is that they can potentially expose both data and control of the device itself to attack. This exposure creates a tension between safety and security, which requires greater stakeholder collaboration to address, particularly in design and regulatory approaches. Put simply, medical device engineering has focused on medical safety for patients but has not sufficiently dealt with cybersecurity for the devices, despite some innovation.

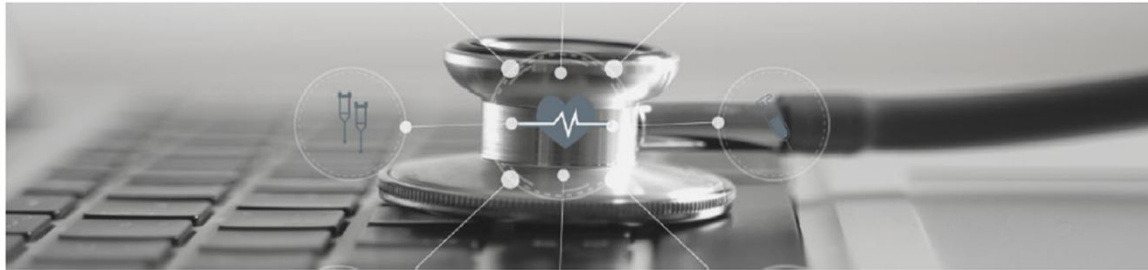
In the age of telemedicine and increased cybersecurity risk, how can healthcare organizations, regulators, medical device manufacturers and consumers ensure their safety?



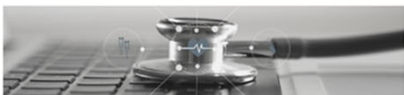
Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY - SECURING TELEHEALTH AND TELEMEDICINE

April 2021



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



What Are the Major Types of Attacks Against Telehealth Systems?

Common threats to and impacts on telehealth systems can include:

Compromise of Confidentiality

- Theft of PHI or PII
- Credential harvesting
- Data exfiltration

Compromise of Integrity

- Exploitation of financial transaction system
- Manipulation of clinical data

Compromise of Availability

- Ransomware
- Denial of Service



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

Telehealth: Extra-Visit Communications and Data

- 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?



COVID-19 Resource Center

Topics ▾

News ▾

Training ▾

Resources ▾

Events ▾

Jobs ▾



Endpoint Security, Governance & Risk Management

Telehealth App Breach Spotlights Privacy, Security Risks

Glitch Briefly Allowed Potential Access to Patient Consultation Recordings

Marianne Kolbasuk McGee (HealthInfoSec) • June 10, 2020

<https://covid19.inforisktoday.com/telehealth-app-breach-spotlights-privacy-security-risks-a-14414>

Why do we need to secure telemedicine technologies and communications?

- Protect patients and business partners
- Good business practice to maintain confidentiality of patient information
 - Patients and business partners may lose trust in a business and potentially take their business to competitors 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 any unauthorized disclosures of PHI
- Information security (InfoSec) is not just about confidentiality.
 - Other important aspects of InfoSec are
 - Availability
 - Integrity



Bruce Schneier - Cyberweek 2018
July 9, 2018

<https://youtu.be/BSsIBuUAVU4?t=302>

Telemedicine Is Growing, But Is Security Lagging Behind?

Bent Philipson - January 11, 2021



Illustration: © IoT For All

When a patient's data is breached, it could snowball into a variety of other scams. Say, for example, one of your patients gets a positive COVID-19 test. You document that information, and, later, someone outside of your network gains access to your facility's patient records. In addition to seeing a positive coronavirus diagnosis, they now have access to that patient's entire history — location, age, contact information, family members' names, etc.

All of this information may be used as part of a cybercriminal's well-thought-out plan. They'll reach out to the patient and their family members, saying they have the cure for the virus and will ask for payment. It may sound ominous, but COVID-19 scams have skyrocketed since the spread of the virus. While older generations and those who aren't as technologically-savvy are the usual victims of such abuse, scam artists have seen success with younger populations.

[https://www.iotforall.com/telemedicine-is-growing-but-is-](https://www.iotforall.com/telemedicine-is-growing-but-is-security-lagging-behind)

[security-lagging-behind](https://www.iotforall.com/telemedicine-is-growing-but-is-security-lagging-behind)



© 2022 ARIZONA TELEMEDICINE PROGRAM



NIST Cybersecurity Framework



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

Telemedicine and Health IT Security: A Team Effort and Product

- Organization C-Suite and Board of Directors
- Information Security Officer
- Privacy Officer
- Information Technology (IT) Director
- Financial Officer
- Organization's entire workforce, not just IT
- Business partners/associates (3rd Parties)
 - Business partners/associates (3rd parties of 3rd parties)
- Technology providers
- Service providers
- Patients

ARIZONA
TELEMEDICINE
PROGRAM



Thank you!

Questions?

mholcomb@telemedicine.arizona.edu



Additional Slides for Reference



LOOKING FORWARD

Technology Considerations for the Rest of 2020

In the months since the United States first declared a public health emergency due to COVID-19, hospitals and physician practices have learned many lessons. Notably, the pandemic quickly increased most Americans' reliance on digital tools, including digital health technologies like telemedicine, which brought increased industry focus on how physicians and hospitals keep patients' protected health information (PHI) private and secure. *Privacy and security are distinct, but closely interrelated. It is not enough for medical practices and hospitals to invest in one but not the other. Fortunately, the concepts are mutually reinforcing, meaning that many actions that are taken to bolster security of patient information will also better protect the privacy of that information.*

The American Medical Association (AMA) and American Hospital Association (AHA) have monitored a variety of technology issues associated with the novel coronavirus and developed a range of resources to assist their members, including our joint resource, [What Physicians Need to Know: Working from home during the COVID-19 pandemic](#). Now, as practices reopen, and hospitals around the country prepare for a second wave of COVID-19 infections coinciding with cold and flu season, our organizations are providing this update on steps physicians should take to prepare for the coming months

Cybersecurity

Risks and Vulnerabilities Update

The COVID-19 pandemic has dramatically changed our way of life and that of the world, including bringing a greater number of people together virtually. However, there is one group that views the pandemic as an opportunity to exploit our virtual community for illicit purposes – cyber criminals.

<https://www.ama-assn.org/system/files/2020-10/ama-aha-technology-considerations.pdf>

LOOKING FORWARD

Technology Considerations for the Rest of 2020

In the months since the United States first declared a public health emergency due to COVID-19, hospitals and physician practices have learned many lessons. Notably, the pandemic quickly increased most Americans' reliance on digital tools, including digital health technologies like telemedicine, which brought increased industry focus on how physicians and hospitals keep patients' protected health information (PHI) private and secure. Privacy and security are distinct, but closely interrelated. It is not enough for medical practices and hospitals to invest in one but not the other. Fortunately, the concepts are mutually reinforcing, meaning that many actions that are taken to bolster security of patient information will also better protect the privacy of that information.

The American Medical Association (AMA) and American Hospital Association (AHA) have monitored a variety of technology issues associated with the novel coronavirus and developed a range of resources to assist their members, including our joint resource, *What Physicians Need to Know: Working from home during the COVID-19 pandemic*. Now, as practices reopen, and hospitals around the country prepare for a second wave of COVID-19 infections coinciding with cold and flu season, our organizations are providing this update on steps physicians should take to prepare for the coming months.

Cybersecurity

Risks and Vulnerabilities Update

The COVID-19 pandemic has dramatically changed our way of life and that of the world, including bringing a greater number of people together virtually. However, there is one group that views the pandemic as an opportunity to exploit our virtual community for illicit purposes – cyber criminals.

We also suggest asking your vendor about their privacy practices, intended data use, and security protocols. Many physicians do not realize that a telemedicine platform or application may be low-cost or free because the vendor's business model is based on aggregating and selling patients' data. If possible, consult with your legal team to clarify how video, audio, and other data are being captured and stored by the vendor and who has access. You can also ask whether the vendor will share results of third-party security audits, including SOC 2 or HITRUST, in addition to the results of their penetration testing.

<https://www.ama-assn.org/system/files/2020-10/ama-aha-technology-considerations.pdf>

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, 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

Data Security: Telehealth's Achilles Heel?

— Cyberattacks on the rise, can only get worse if problems aren't fixed, experts say

by [Ryan Basen](#), Enterprise & Investigative Writer, MedPage Today September 4, 2020

<https://www.medpagetoday.com/practicemanagement/telehealth/8469>



Recently [The Doctors Company](#), a medical malpractice insurance firm, published a report entitled "Your Patient is Logging on Now: The Risks and Benefits of Telehealth in the Future of Healthcare." Among the five "foreseeable major risks" listed in the report: Telehealth "increases cyber liability, especially when providers are seeing patients from a variety of devices in a variety of locations."

In other words, providers are now opening themselves up to cyberattacks on an unprecedented scale.

Recommended For You

Super-Spreading in the Capitol; Provides \$22B to States; 2020 Murder Epidemic

COVID Clot Prevention Evidence Beginning to Bud

Vascular Surgeon Pleads Guilty Blood Vessel Scam

Telemedicine creates big cybersecurity risks, Harvard researchers say

Jackie Drees - Thursday, December 17th, 2020 [Print](#) | [Email](#)



<https://www.beckershospitalreview.com/telehealth/telemedicine-creates-big-cybersecurity-risks-harvard-researchers-say.html>

As hospitals and health systems continue the shift to telemedicine, new issues and risks with cybersecurity have arisen that will require ongoing work to preserve privacy and safe care delivery, Harvard Medical School researchers say.

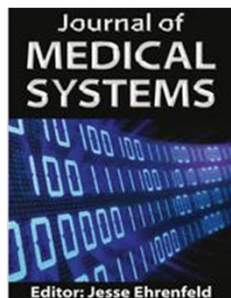
In a Dec. 16 article for the *Journal of Informatics in Health and Medicine*, Mohammad Jalali, PhD, IT professor at Harvard Medical School; Adam Landman, MD, CIO at Brigham and Women's Hospital; and William Gordon, MD, professor at Brigham and Women's Hospital, highlighted security risks of video conferencing apps and the increase in ransomware attacks on healthcare organizations.

Here are five ways they suggest to increase cybersecurity practices for telemedicine:

1. Make awareness the first step. Promote education, employee training and practice simulated cyberattacks, such as sending fake phishing emails to build a culture of security across the organization.
2. Ensure best cybersecurity behaviors are followed, including encrypting data, keeping software updated, running antivirus software, using two-factor authentication and following local cybersecurity regulations.
3. Transition from consumer video-conferencing tools such as FaceTime or Skype to an enterprise healthcare-specific video-conferencing platform. This type of enterprise-grade software may include key security features such as encryption and settings that require a waiting room with every teleconference.
4. Healthcare organizations should partner with telemedicine and cybersecurity vendors to implement tools such as artificial intelligence and blockchain to better prevent and detect cyber threats.
5. While prevention and detection capabilities are critical, organizations should also prepare with incident response plans in the event they do get hit by a cyberattack so they are well prepared and minimize negative consequences.

Non-exhaustive list of some of the best practices to keep health information secure:

- Continually educate all users of a system about cybersecurity threats and about how to use the healthcare information system securely.
- Always follow the rule of least privilege necessary when allowing access to healthcare information
- Always patch security vulnerabilities on an urgent basis.
- Keep your system as simple as possible - more complexity makes it harder to secure and maintain
- Document your policies, procedures, risk assessments and security incidents, etc.
- Maintain frequent backups of your healthcare information system data on air gapped media / systems.
- Disable employee access to healthcare information systems immediately when they leave the organization
- Encrypt healthcare information in transit and at rest
- Make effective use of the security features of the technology that your organization uses
- Use multi-factor authentication for access to healthcare information systems
- Use malware prevention and mitigation technologies, label emails from external sources
- Know where your organization stores its patients' PHI/PII and know the details of how it is communicated.
- At a minimum require involvement of your organization's Chief Information Security Office and HIPAA Privacy Officer in all projects involving healthcare information security.
- Utilize firewalls, intrusion prevention and detection systems



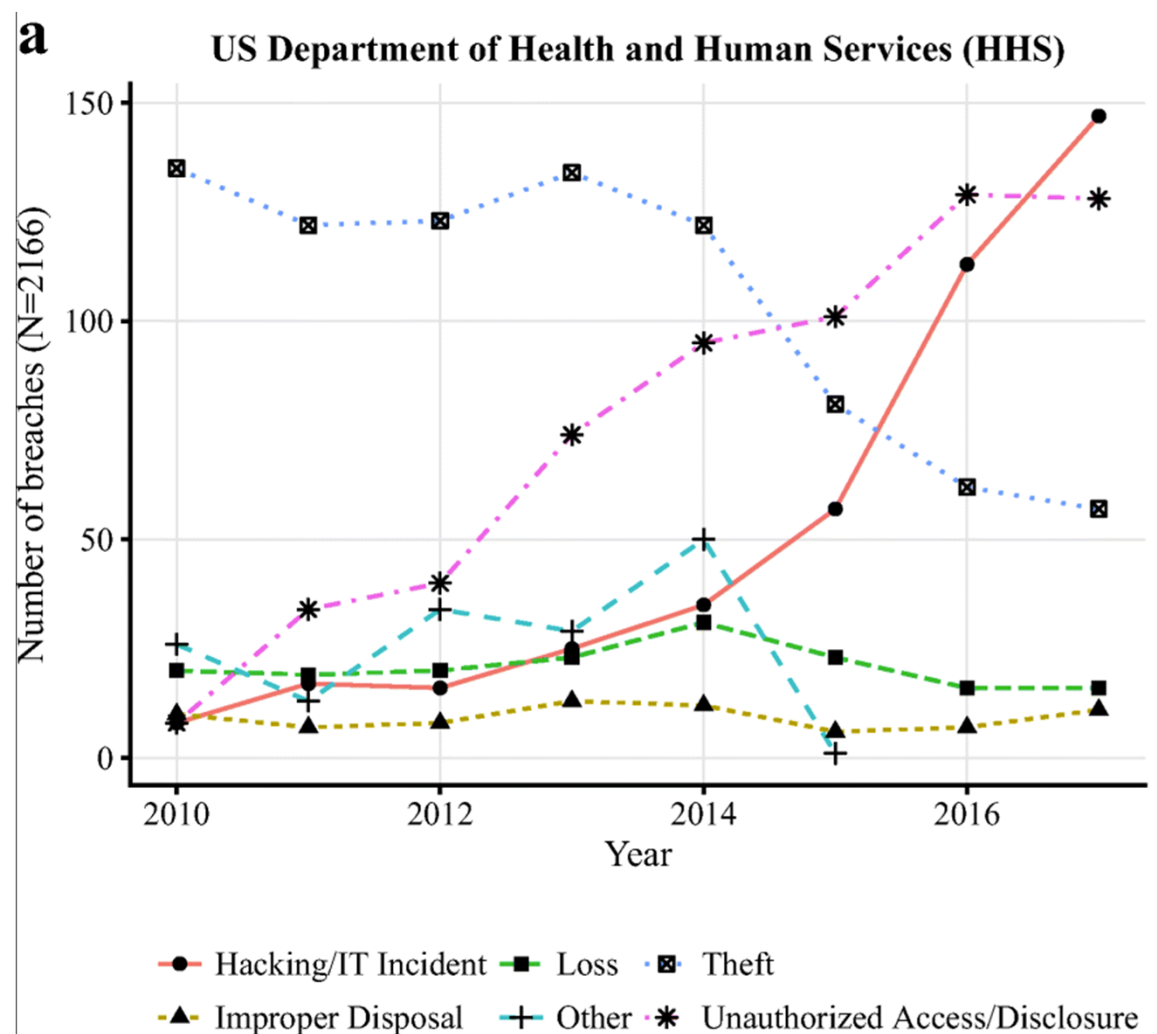
Healthcare Data Breaches: Implications for Digital Forensic Readiness

Chernyshev, M., Zeadally, S. & Baig, Z. J Med Syst (2019) 43: 7.

<https://doi.org/10.1007/s10916-018-1123-2>

Figure 1 part a

Breakdown of healthcare breach types by year based on data provided by the US Department of Health and Human Services (HHS) including archived breaches and breaches under investigation (2010- Apr 2018)





Healthcare Data Breach Statistics

Breaches by Covered Entity Type

Year	Healthcare Provider	Health Plan	Business Associate	Healthcare Clearinghouse	Total
2009	14	1	3	0	18
2010	134	21	44	0	199
2011	134	19	45	1	199
2012	155	23	40	1	219
2013	191	20	64	2	277
2014	196	41	77	0	314
2015	195	61	14	0	270
2016	256	51	22	0	329
2017	285	52	21	0	358
2018	273	53	42	0	368
2019	398	59	53	2	512
2020	497	70	73	2	642
Total	2,728	471	498	8	3,705

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

Health Industry Cybersecurity Practices:

Managing Threats and Protecting Patients

December 28, 2018



Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

In accordance with the CSA, this document sets forth a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes to achieve three core goals:

1. Cost-effectively reduce cybersecurity risks for a range of health care organizations;
2. Support the voluntary adoption and implementation of its recommendations; and
3. Ensure, on an ongoing basis that content is actionable, practical, and relevant to health care stakeholders of every size and resource level.

<https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf>

Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

Table 1. Five Prevailing Cybersecurity Threats to Health Care Organizations

Threat	Potential Impact of Attack
E-mail phishing attack	Malware delivery or credential attacks. Both attacks further compromise the organization.
Ransomware attack	Assets locked and held for monetary ransom (extortion). May result in the permanent loss of patient records.
Loss or theft of equipment or data	Breach of sensitive information. May lead to patient identity theft.
Accidental or intentional data loss	Removal of data from the organization (intentionally or unintentionally). May lead to a breach of sensitive information.
Attacks against connected medical devices that may affect patient safety	Undermined patient safety, treatment, and well-being.



Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

<https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf>

Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

Threat: E-mail Phishing Attack		
Vulnerabilities Lack	Impact	Practices to Consider
of awareness training	Loss of reputation in the community (referrals dry up, patients leave the practice)	Be suspicious of e-mails from unknown senders, e-mails that request sensitive information such as PHI or personal information, or e-mails that include a call to action that stresses urgency or importance (1.S.B)
Lack of IT resource for managing suspicious e-mails	Stolen access credentials used for access to sensitive data	Train staff to recognize suspicious e-mails and to know where to forward them (1.S.B)
Lack of software scanning e-mails for malicious content or bad links	Erosion of trust or brand reputation	Never open e-mail attachments from unknown senders (1.S.B)
Lack of e-mail detection software testing for malicious content	Potential negative impact to the ability to provide timely and quality patient care	Tag external e-mails to make them recognizable to staff (1.S.A)
Lack of e-mail sender and domain validation tools	Patient safety concerns	Implement incident response plays to manage successful phishing attacks (8.M.A)
		Implement advanced technologies for detecting and testing e-mail for malicious content or links (1.L.A)
		Implement multifactor authentication (MFA) (1.S.A, 3.M.D)
		Implement proven and tested response procedures when employees click on phishing e-mails (1.S.C)
		Establish cyber threat information sharing with other health care organizations (8.S.B, 8.M.C)

<https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf>

Table 2. Suggested Practices to Combat E-mail Phishing Attacks

© 2022 ARIZONA TELEMEDICINE PROGRAM

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

Jennifer Cawthra
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Ronnie Daldos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NCCOE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE



2 SCENARIO: REMOTE PATIENT MONITORING AND VIDEO TELEHEALTH

The scenario considered for this project involves RPM equipment deployed to the patient's home [2]. RPM equipment that may be provided to patients includes devices for blood pressure monitoring, heart rate monitoring, BMI/weight measurements, and glucose monitoring. An accompanying application may also be downloaded onto the patient-owned device and synced with the RPM equipment to enable the patient and healthcare provider to share data. Patients may also be able to initiate videoconferencing and/or communicate with the healthcare provider via email, text messaging, chat sessions, or voice communication. Data may be transmitted across the patient's home network and routed across the public internet. Those transmissions may be relayed to a telehealth platform provider that, in turn, routes the communications to the HDO. This process brings the patient and healthcare provider together, allowing for delivery of the needed healthcare services in the comfort of the patient's home.

Project Description: Securing Telehealth Remote Patient Monitoring Ecosystem

5

<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>



IDENTIFY (ID)—*These activities are foundational to developing an organizational understanding to manage risk.*

- **asset management**—includes identification and management of assets on the network and management of the assets to be deployed to equipment. Implementation of this category may vary depending on the parties managing the equipment. However, this category remains relevant as a fundamental component in establishing appropriate cybersecurity practices.
- **governance**—Organizational cybersecurity policy is established and communicated. Governance practices are appropriate for HDOs and their solution partners, including technology providers and those vendors that develop, support, and operate telehealth platforms.
- **risk assessment**—includes the risk management strategy. Risk assessment is a fundamental component for HDOs and their solution partners.
- **supply chain risk management**—The nature of telehealth with RPM is that the system integrates components sourced from disparate vendors and may involve relationships established with multiple suppliers, including cloud services providers.

<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>



PROTECT (PR)—*These activities support the ability to develop and implement appropriate safeguards based on risk.*

- **identity management, authentication, and access control**—includes user account management and remote access
 - controlling (and auditing) user accounts
 - controlling (and auditing) access by external users
 - enforcing least privilege for all (internal and external) users
 - enforcing separation-of-duties policies
 - privileged access management (PAM) with an emphasis on separation of duties
 - enforcing least functionality
- **data security**—includes data confidentiality, integrity, and availability
 - securing and monitoring storage of data—includes data encryption (for data at rest)

<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

Jennifer Cavitt
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Ronnie Dailos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov



(Continued)

PROTECT (PR)—*These activities support the ability to develop and implement appropriate safeguards based on risk.*

- access control on data
- data-at-rest controls should implement some form of a data security manager that would allow for policy application to encrypt data, inclusive of access control policy
- securing distribution of data—includes data encryption (for data in transit) and a data loss prevention mechanism
- controls that promote data integrity
- Cryptographic modules validated as meeting NIST Federal Information Processing Standards (FIPS) 140-2 are preferred.
- **information protection processes and procedures**—include data backup and endpoint protection
- **maintenance**—includes local and remote maintenance
- **protective technology**—host-based intrusion prevention, solutions for malware (malicious-code detection), audit logging, (automated) audit log review, and physical protection

<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

Jennifer Cavitt
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Ronnie Dailos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov



DETECT (DE)—*These activities enable timely discovery of a cybersecurity event.*

- **security continuous monitoring**—monitoring for unauthorized personnel, devices, software, and connections
 - vulnerability management—includes vulnerability scanning and remediation
 - patch management
 - system configuration security settings
 - user account usage (local and remote) and user behavioral analytics
 - security log analysis



<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

Jennifer Cavitt
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Ronnie Dailos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov



RESPOND (RS)—*These activities support development and implementation of actions designed to contain the impact of a detected cybersecurity event.*

- **response planning**—Response processes and procedures are executed and maintained to ensure a response to a detected cybersecurity incident.
- **mitigation**—Activities are performed to prevent expansion of a cybersecurity event, mitigate its effects, and resolve the incident.



<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

Jennifer Cavitt
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Ronnie Dailos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov

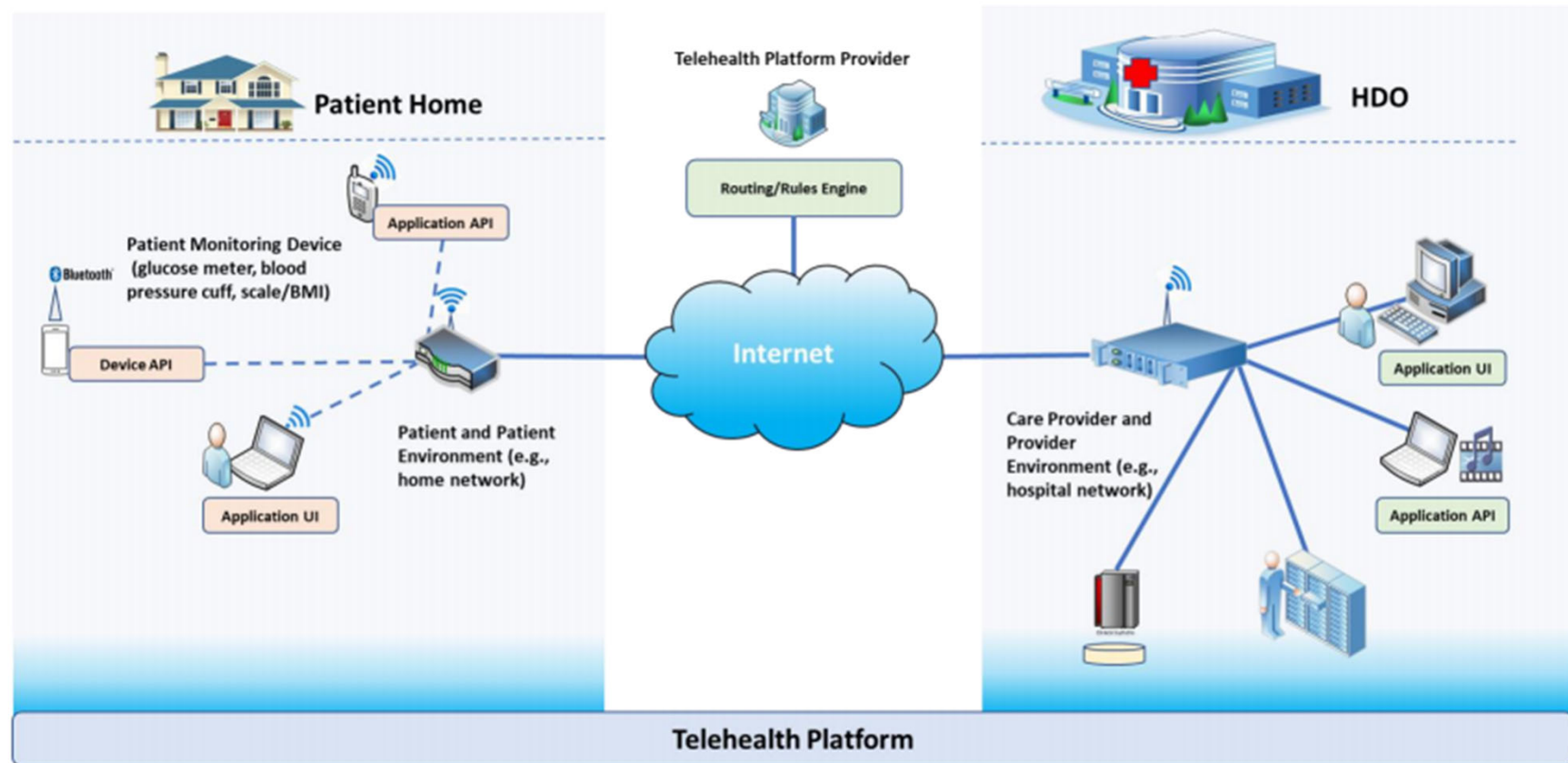


RECOVER (RC)—*These activities support development and implementation of actions for the timely recovery of normal operations after a cybersecurity incident.*

- **recovery planning**—Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
- **communications**—Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, internet service providers, owners of attacking systems, victims, other computer security incident response teams, vendors).

<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>

Figure 3-1: High-Level Architecture



<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>

Health IT Playbook

- The Office of the National Coordinator for Health Information Technology “Health IT Playbook” Section 7 – Privacy and Security
 - <https://www.healthit.gov/playbook/privacy-and-security/#section-7-1>