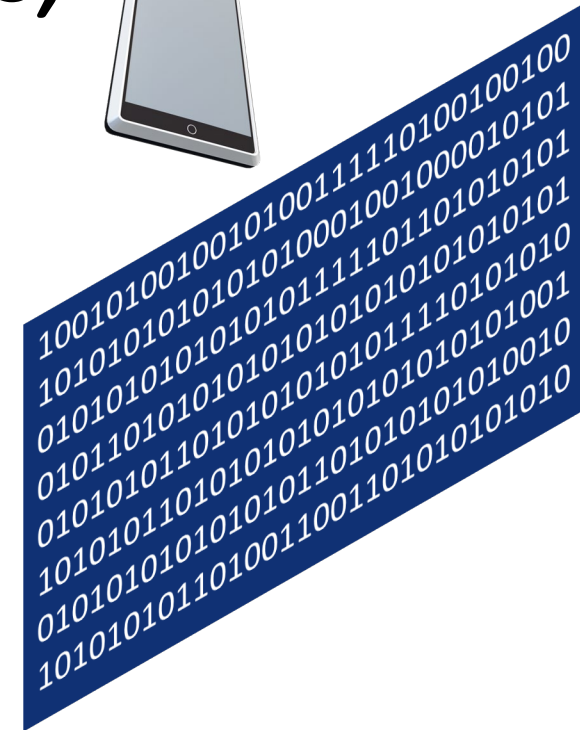
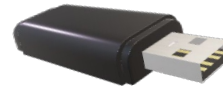


ARIZONA
TELEMEDICINE
PROGRAM



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



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



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

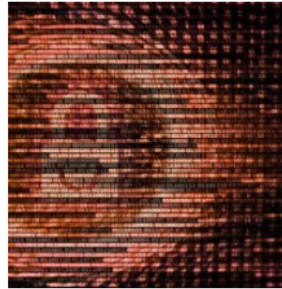


<https://healthitsecurity.com/news/az-ransomware-attack-leads-to-unrecoverable-ehrs-data-loss>

Latest Health Data Breaches News

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

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



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

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

May 18, 2021 by [Jessica Davis](#)

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

Scripps Health EHR, Patient Portal Still Down After Ransomware Attack

May 10, 2021 by [Jessica Davis](#)

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

Ransomware Hits Scripps Health, Disrupting Critical Care, Online Portal

May 03, 2021 by [Jessica Davis](#)

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



By -
Nsikan
Akpan

Leave a
comment

Share ...



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>

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.

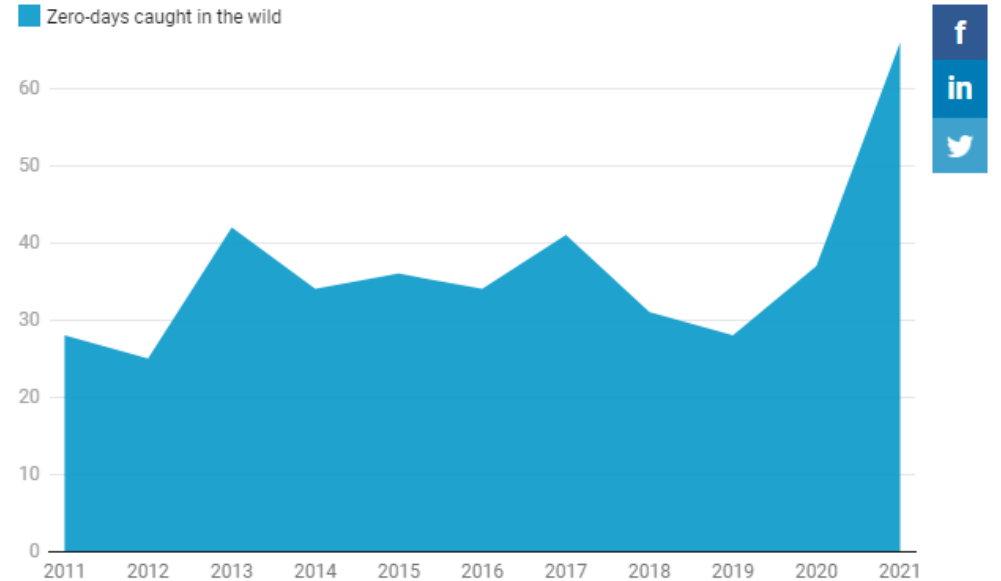


Chart: Patrick Howell O'Neill • Source: [Zero-day tracking project](#) • [Get the data](#) • Created with [Datawrapper](#)

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/>

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>

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 May 9, 2022 ~835 active investigations of breaches involving > 63,000,000 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

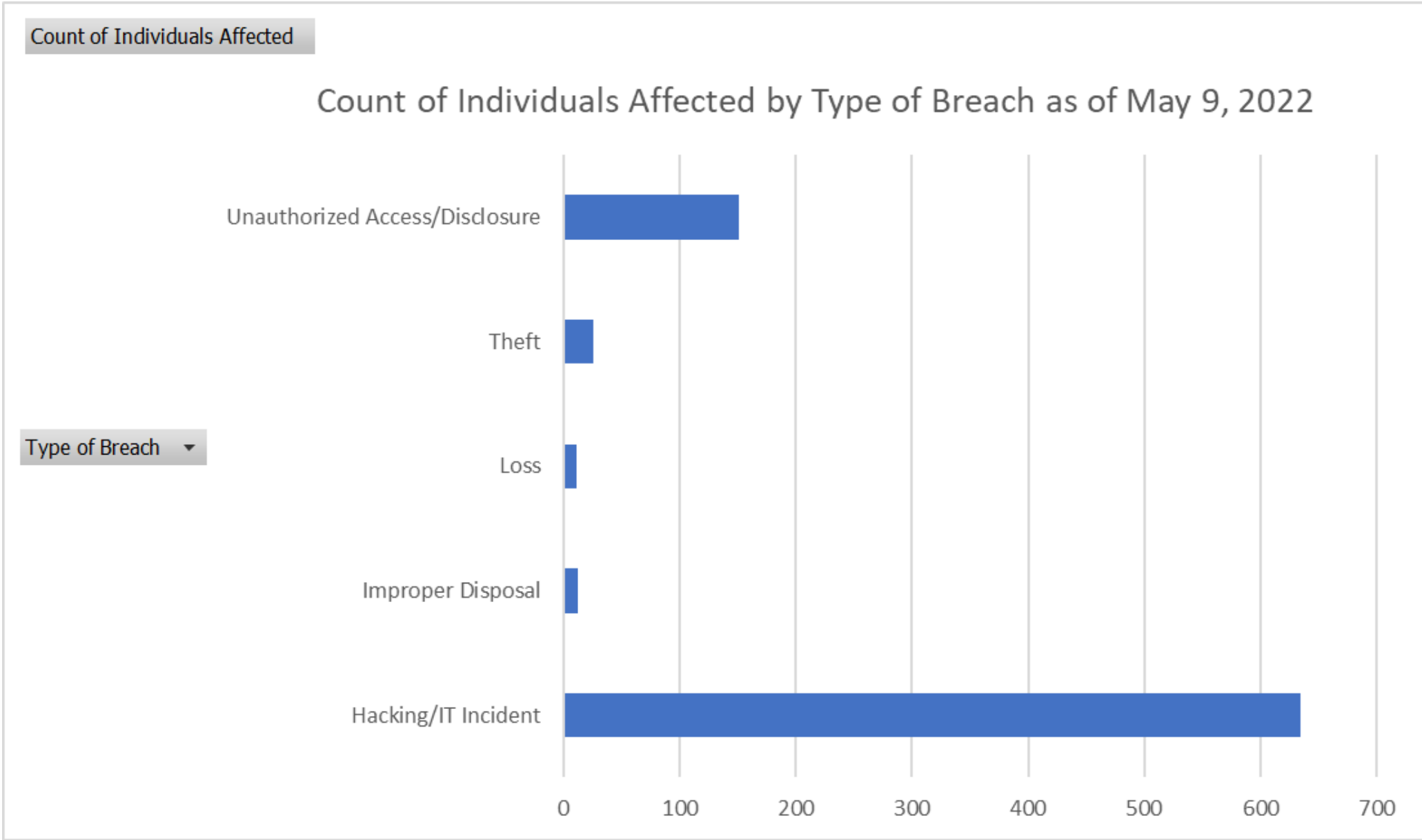
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

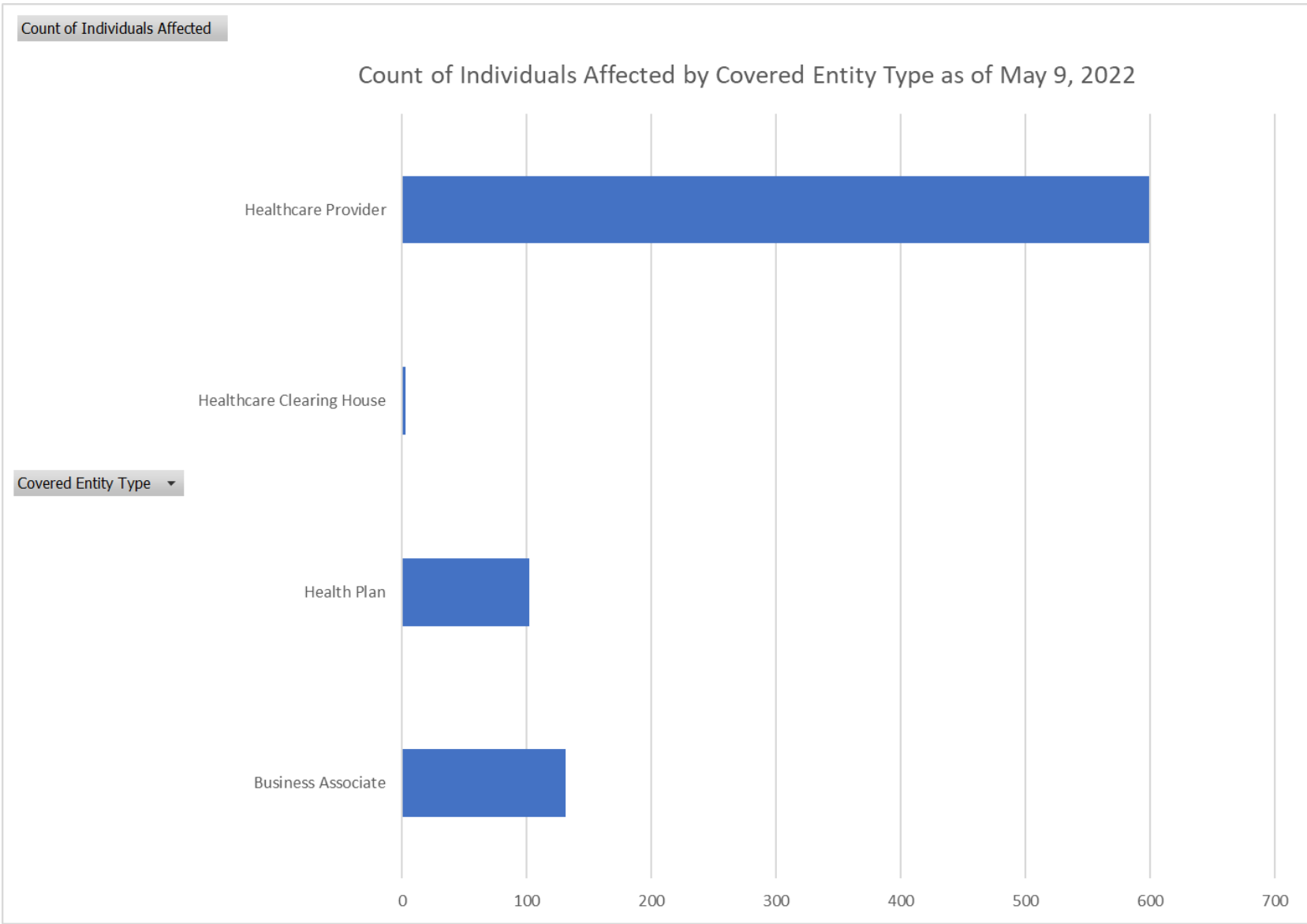
Cases Currently Under Investigation

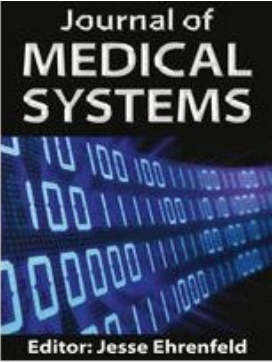
This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

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
0	National Imaging Associates, Inc.	MD	Business Associate	744	05/02/2022	Unauthorized Access/Disclosure	Laptop
0	Select Benefits Group, LLC dba Dental Select	UT	Business Associate	1035	04/26/2022	Hacking/IT Incident	Email
0	ARcare	AR	Healthcare Provider	345353	04/25/2022	Hacking/IT Incident	Network Server
0	King County Public Hospital District No. 2 d/b/a EvergreenHealth	WA	Healthcare Provider	20533	04/22/2022	Hacking/IT Incident	Network Server
0	Montefiore Medical Center	NY	Healthcare Provider	3717	04/22/2022	Unauthorized Access/Disclosure	Electronic Medical Record
0	The Mental Health Center of Greater Manchester	NH	Healthcare Provider	1322	04/22/2022	Hacking/IT Incident	Network Server
0	Illinois Gastroenterology Group, PLLC	IL	Healthcare Provider	227943	04/22/2022	Hacking/IT Incident	Network Server
0	National Imaging Associates, Inc.	MD	Business Associate	616	04/22/2022	Unauthorized Access/Disclosure	Laptop
0	The Energy Cooperative Group Benefits Plan	OH	Health Plan	875	04/21/2022	Hacking/IT Incident	Network Server
0	County of Los Angeles Department of Mental Health	CA	Healthcare Provider	5129	04/20/2022	Hacking/IT Incident	Email
0	Healthplex, Inc.	NY	Health Plan	89955	04/20/2022	Hacking/IT Incident	Email
0	La Casa de Salud	NY	Healthcare Provider	9969	04/20/2022	Hacking/IT Incident	Email
0	Wayne Family Practice Associates, PC	GA	Healthcare Provider	5944	04/19/2022	Hacking/IT Incident	Network Server
0	Fairfield County Implants and Periodontics, LLC	CT	Healthcare Provider	10502	04/19/2022	Hacking/IT Incident	Email
0	Optima Dermatology Holdings, LLC	NH	Healthcare Provider	59872	04/18/2022	Hacking/IT Incident	Email
0	HealthActions, P.A.	AL	Healthcare Provider	2369	04/18/2022	Hacking/IT Incident	Email
0	Canon Business Process Services Inc	NY	Business Associate	1625	04/15/2022	Unauthorized Access/Disclosure	Paper/Films
0	Canon Business Process Services Inc	NY	Business Associate	745	04/15/2022	Unauthorized Access/Disclosure	Paper/Films
0	Canon Business Process Services Inc	NY	Business Associate	8015	04/15/2022	Unauthorized Access/Disclosure	Paper/Films
0	Spectrum Health System	MI	Healthcare Provider	794	04/15/2022	Unauthorized Access/Disclosure	Electronic Medical Record
0	Central Florida Cardiology Group	FL	Healthcare Provider	1186	04/14/2022	Hacking/IT Incident	Other
0	New Creation Counseling Center	OH	Healthcare Provider	24029	04/14/2022	Hacking/IT Incident	Network Server, Other
0	Newman Regional Health	KS	Healthcare Provider	52224	04/14/2022	Hacking/IT Incident	Email
0	Mountain Area Health Education Center dba MAHEC	NC	Healthcare Provider	1115	04/14/2022	Improper Disposal	Paper/Films
0	Onehome Health Solutions	FL	Healthcare Provider	15401	04/13/2022	Theft	Laptop
0	Lutheran Services Carolinas	NC	Business Associate	1226	04/12/2022	Hacking/IT Incident	Network Server
0	Adaptive Health Integrations	ND	Healthcare Provider	510574	04/11/2022	Hacking/IT Incident	Network Server

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



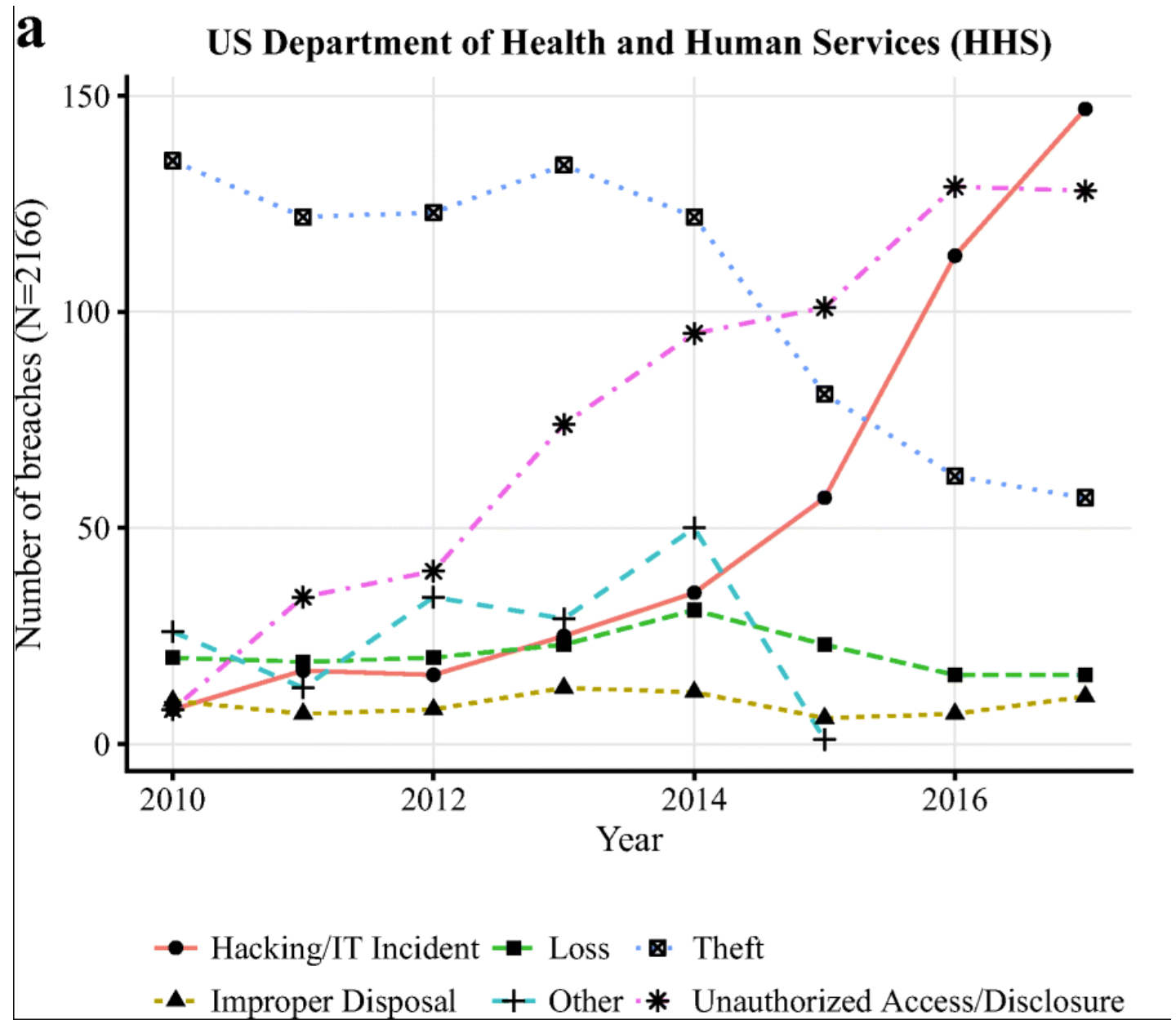




Healthcare Data Breaches: Implications for Digital Forensic Readiness

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)



Individually identifiable health information in the records of health care providers, health insurers and healthcare clearinghouses used for treatment, payment or healthcare operations (in medical records or medical insurance records but not in personnel or student records, for instance) is "Protected Health Information" (PHI) and is regulated by HIPAA.

The following data elements of the individual or of relatives, employers, or household members of the individual, are considered identifiers that make the PHI individually identifiable:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
 - a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code unless the re-identification key is maintained by the covered entity and is not decipherable or disclosed to the data recipient.

HPP Use Only:
HIPAA Privacy Program
v. 2015

Additional information about PHI and de-identification standards:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html>

Page 1 of 1

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



Renewal of Determination That A Public Health Emergency Exists

Public Health Emergency Declaration

Declarations of a Public Health Emergency

As a result of the continued consequences of the Coronavirus Disease 2019 (COVID-19) pandemic, on this date and after consultation with public health officials as necessary, I, Xavier Becerra, Secretary of Health and Human Services, pursuant to the authority vested in me under section 319 of the Public Health Service Act, **do hereby renew, effective April 16, 2022,** the January 31, 2020, determination by former Secretary Alex M. Azar II, that he previously renewed on April 21, 2020, July 23, 2020, October 2, 2020, and January 7, 2021, and that I renewed on April 15, 2021, July 19, 2021, October 15, 2021, and January 14, 2022, that a public health emergency exists and has existed since January 27, 2020, nationwide.

April 12, 2022

/s/

Date

Xavier Becerra

<https://aspr.hhs.gov/legal/PHE/Pages/COVID19-12Apr2022.aspx>

I'm looking for...



A-Z Index



HIPAA for
Individuals



Filing a
Complaint



HIPAA for
Professionals



Newsroom

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Special Topics](#) > [Emergency Response](#) > Notification of Enforcement Discretion for Telehealth

HIPAA for Professionals

Regulatory Initiatives

Privacy



Text Resize A A A

Print

Share



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

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>



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>

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

Social Determinants of Health Virtual Summit Featured
Housing & Transporta
Improving Health Outco

PATIENT ENGAGEMENT HIT

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.

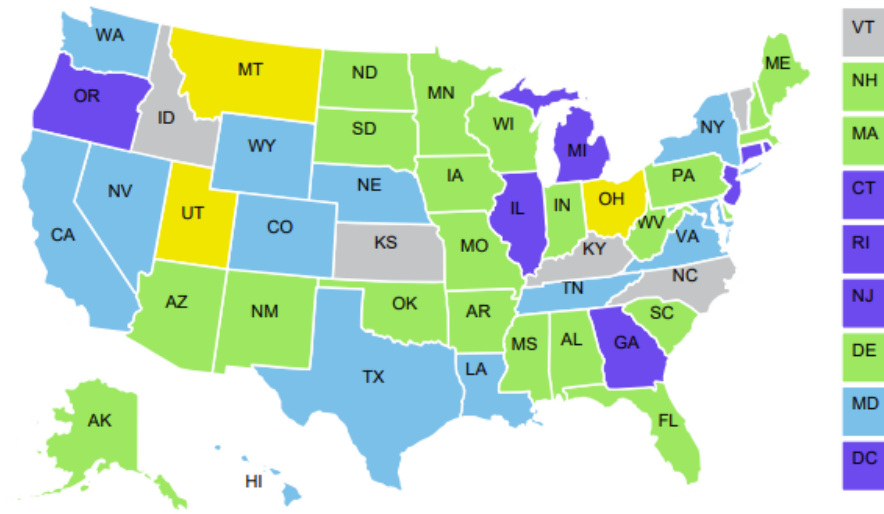
<https://healthitsecurity.com/news/the-telehealth-security-impact-now-and-beyond-the-covid-19-pandemic>

Individual Access to Medical Records: 50 State Comparison

Arizona

Preempted by HIPAA

A.R.S. § 32-3211: A health professional must establish procedures for providing a patient their medical record in a "timely" manner, but a specific time period is not provided under the law.



State Medical Record Access Requirements Compared to HIPAA

- Stronger than HIPAA
- Same as HIPAA

A project of the George Washington University's Hirsh Health Law and Policy Program and the Robert Wood Johnson Foundation

<http://www.healthinfolaw.org>

Individual Access to Medical Records: 50 State Comparison

- Preempted by HIPAA
- No law specifically granting individual access right; HIPAA applies
- HIPAA applies to covered entities, and state has additional requirements for entities not covered by HIPAA

<http://www.healthinfolaw.org/pdf/print/individual-access-medical-records-50-state-comparison>

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



HHS 405(d) Aligning Health Care Industry Security Approaches

ProtectThreats

What is Email Phishing?

An attempt to use email to trick you into giving out personal information or clicking on infected links which give hackers access to all of your patients' data.



Real-World Scenario:

Your employees receive a fraudulent e-mail from a cyber-attacker disguised as an IT support person from your patient billing company. The e-mail instructs your employees to click on a link to change their billing software passwords. An employee who clicks the link is directed to a fake login page, which collects that employee's login credentials and transmits this information to the attackers. The attacker then uses the employee's login credentials to access your organization's financial and patient data.

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



HHS 405(d) Aligning Health Care Industry Security Approaches

What is Ransomware?

An attack that occurs when hackers gain control of data or a computer system and hold it hostage until a ransom is paid. This can put your patients in danger and prevent you from delivering care in a timely fashion.



Real-World Scenario:

Through an e-mail that appears to have originated from a credit card company, a user is directed to a fake website and tricked into downloading a security update. The so-called security update is actually a malicious program designed to find and encrypt data, rendering them inaccessible. The program then instructs the user to pay a ransom to unlock or unencrypt the data.

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



HHS 405(d) Aligning Health Care Industry Security Approaches

What is Loss or Theft of Equipment?

Did you know? Everyday devices such as laptops, smart phones, and USB/thumb drives are often lost or stolen and could end up in the hands of hackers. Make sure that you: never leave your laptop or computer unattended, always encrypt sensitive data that is on your device as a second line of defense, notify your supervisor or IT professional immediately if your equipment is lost or stolen.



Real-World Scenario:

A physician stops at a coffee shop for a coffee and to use the public Wi-Fi to review radiology reports. As the physician leaves the table momentarily to pick up his coffee, a thief steals the laptop. The doctor return to the table to find the laptop is gone.

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



HHS 405(d) Aligning Health Care Industry Security Approaches

What is Insider, Accidental, or Intentional Data Loss?

Insider threats exist within every organization where employees, contractors, or other users access the organization's technology infrastructure, network, or databases.



Real-World Scenario:

An attacker impersonating a staff member of a physical therapy center contacts a hospital employee and asks to verify patient data. Pretending to be hospital staff, the imposter acquires the entire patient health record.

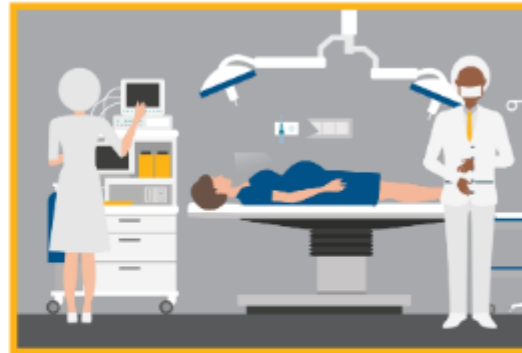
<https://405d.hhs.gov/protect>



HHS 405(d) Aligning Health Care Industry Security Approaches

What are Attacks Against Connected Medical Devices?

Consider this: Your organization is afflicted by a phishing attack that affects a file server that's connected to multiple heart monitors. The attack gives the hacker complete control to power them off and on as they please.



Real-World Scenario:

A cyber attacker gains access to a care provider's computer network through an e-mail phishing attack and takes command of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot) of all heart monitors in the ICU, putting multiple patients at risk.

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

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

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>

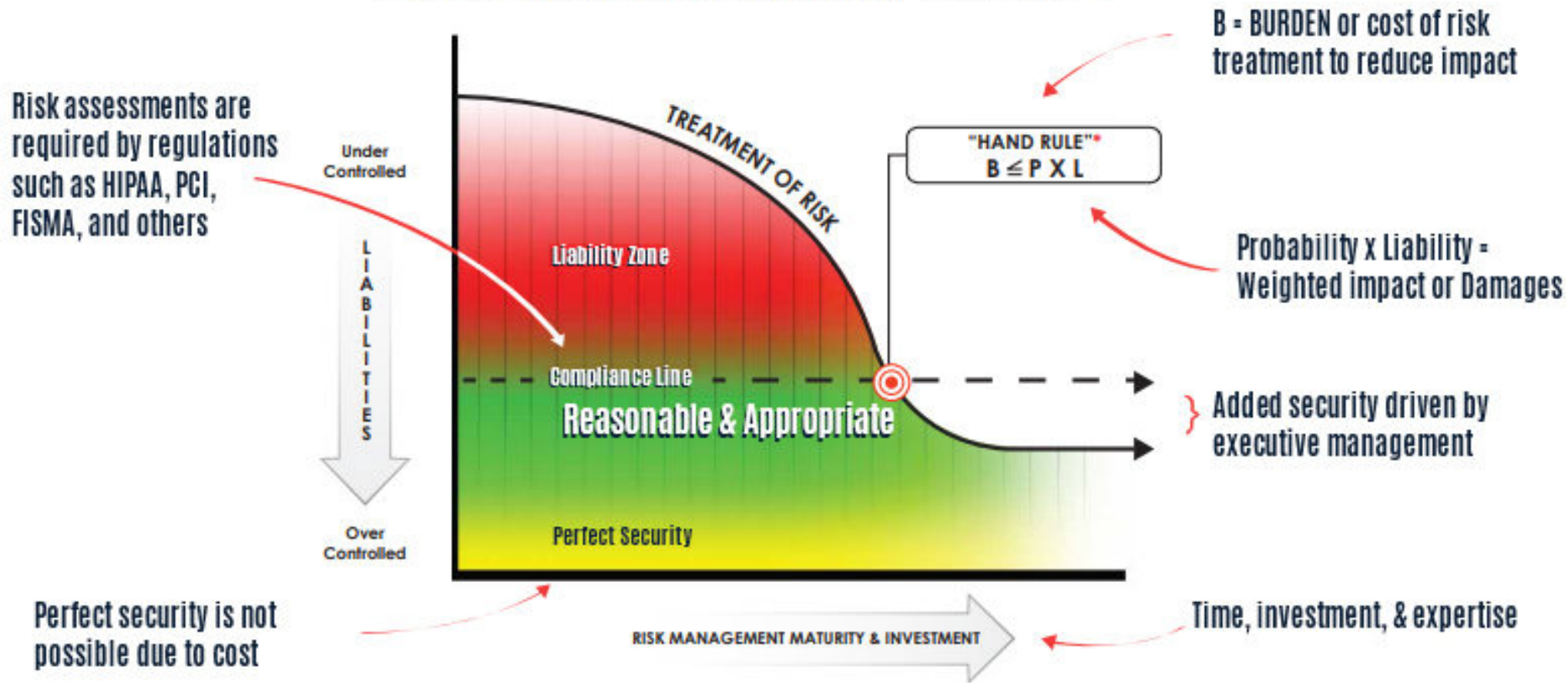
Telehealth: Visit Metacommunications and Metadata

- 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?

What type(s) of business(es) or organization(s) would you choose to share your personal health, insurance and payment information with if you knew they did not have and/or did not reliably follow effective policies and procedures to safeguard the information that you share with them?

What device(s) and/or software would you feel comfortable using to store or communicate your personal health and financial information if you knew they were known to be insecure or were not updated with the latest security patches?

Is Your Organization Exercising "Due Care"?



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

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

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)





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**

Patient **RISK**

Organization **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

Enterprise **RISK**



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)





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 your 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)



Why do we need to secure telemedicine technologies and communications?

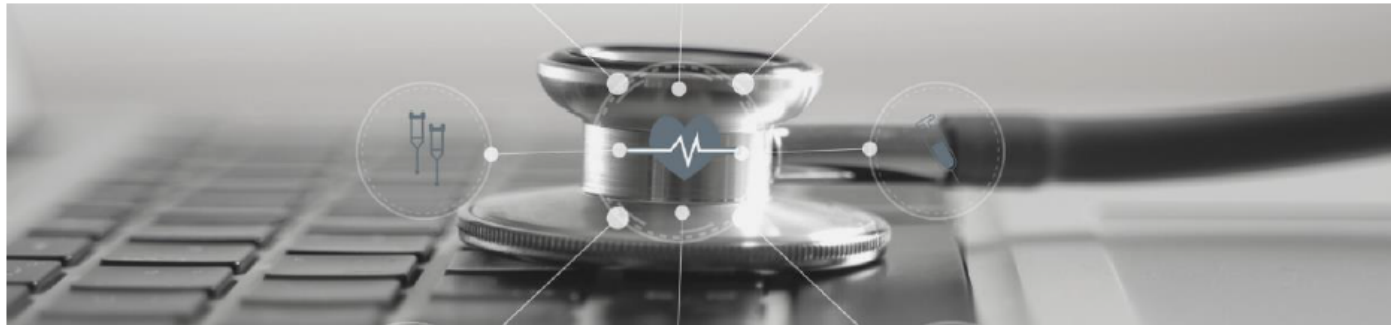
- Protect patients and business partners
- Good business practice to maintain confidentiality of patient information
 - Patients and business partners may lose trust in a business and potentially take their business to competitors if their information is compromised
- Laws such as Health Insurance Privacy 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



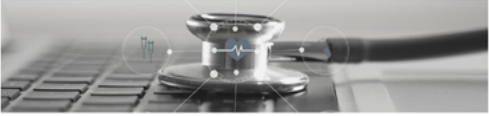
Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

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 PII or PHI
- 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>

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>



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>



 Resources


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/>

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
xelligent HEALTHCARE MEDIA

Home News Features In

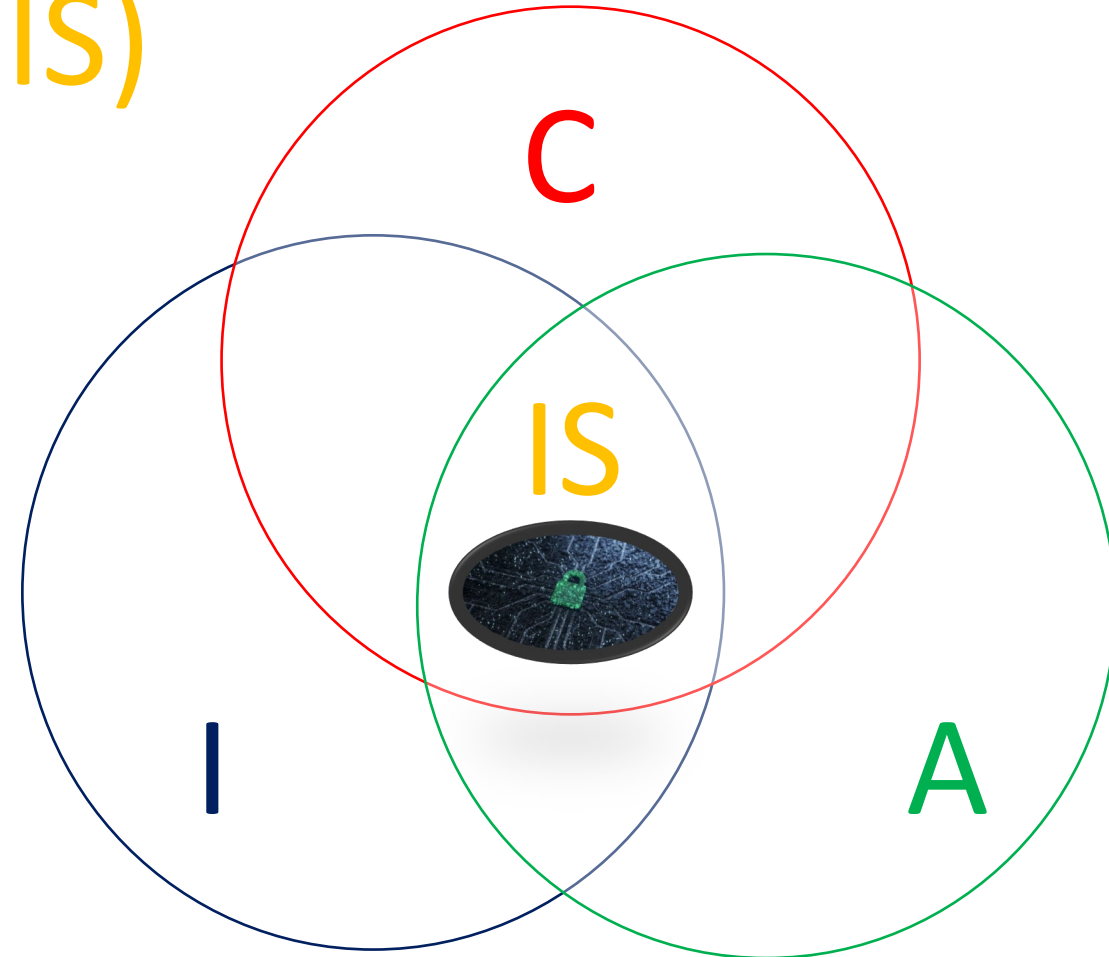
HIPAA and Compliance Cybersecurity Cloud Mobile Patient Privacy Data Breaches

<https://healthitsecurity.com/news/report-covid-10-telehealth-risks-and-best-practice-privacy-security>



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



Security Triad

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



HHS 405(d) Aligned Health Care Industry Security Approaches

HICP's 10 Best Practices



As presented in Technical Volumes 1 and 2, the ten Cybersecurity Practices range from personnel training and awareness to the development and implementation of new processes, the acquisition and customization of new technology, and, ultimately, to fostering a consistent, robust, and continually updated approach to cybersecurity. The Practices introduced in this publication strengthen cybersecurity capabilities in health care organizations by:

- Enabling organizations to evaluate and benchmark cybersecurity capabilities effectively and reliably
- Sharing knowledge, common practices, and appropriate references across organizations to improve cybersecurity competencies
- Enabling organizations to prioritize actions and investments—knowing what to ask—to improve cybersecurity

Click the boxes on the left to see an overview of each of the 10 Best Practices.

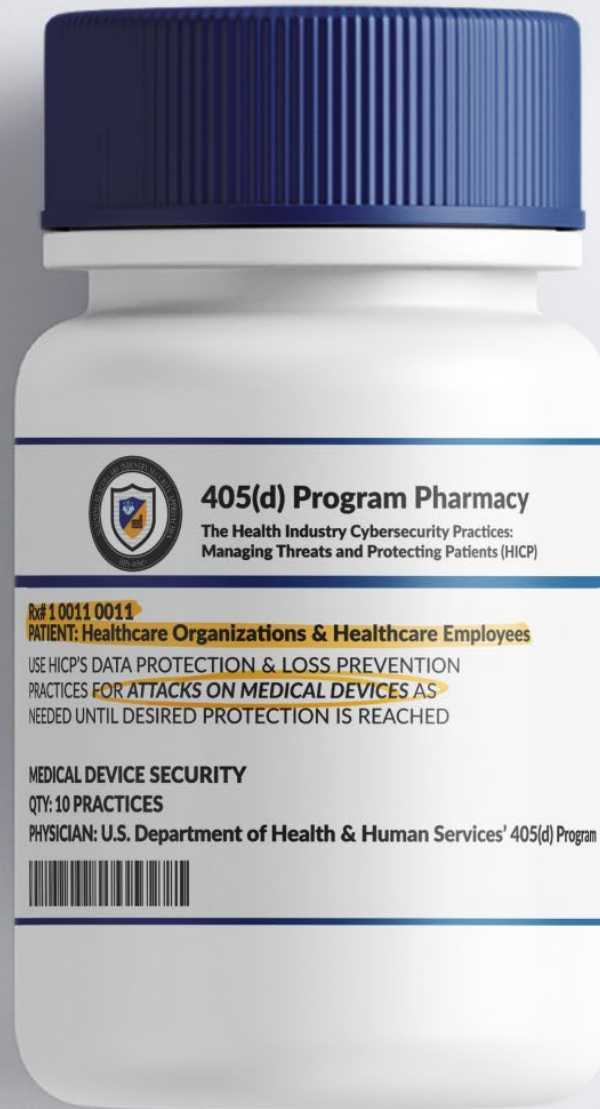
The following are supporting resources focused on the various practices:

- The HICP Threat Mitigation Matrix is designed to help your organization's IT team identify the five key cybersecurity threats outlined in the Health Industry Cybersecurity Practices (HICP) that are most pertinent to your unique organization and apply controls to mitigate those threats. The controls and sub-controls are categorized based on their applicability to organization "size".
 - Download the HICP Threat Mitigation Matrix

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



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>

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>

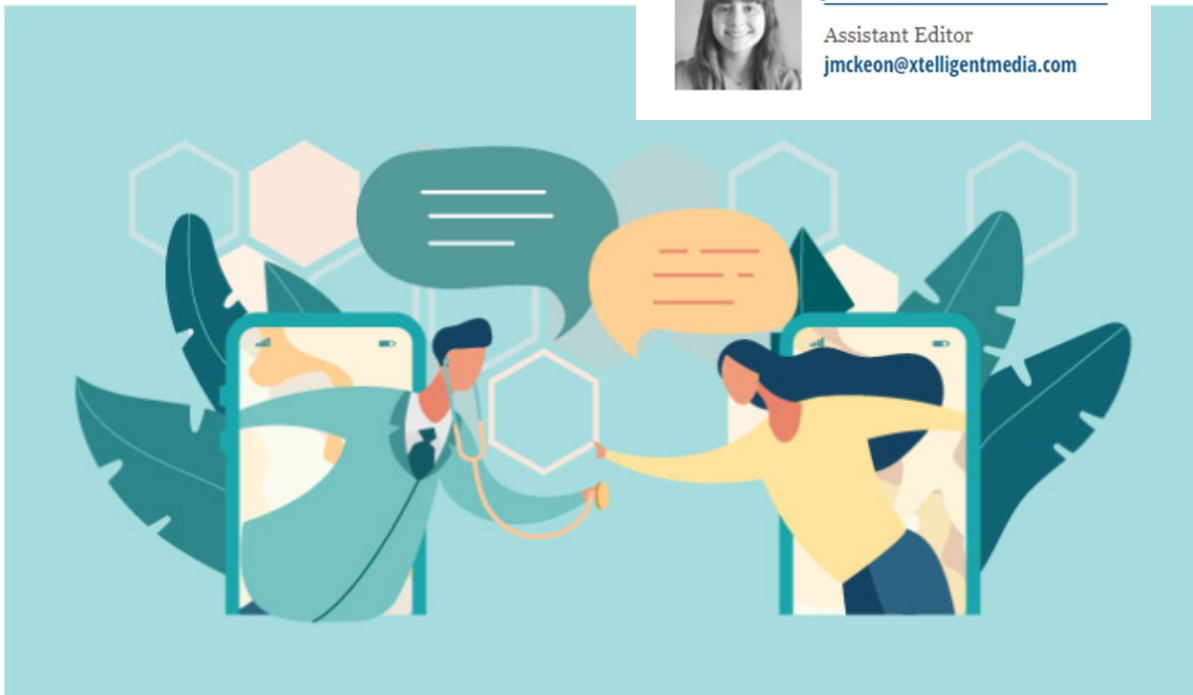
Managing Telehealth, Remote Patient Monitoring Security Concerns

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>



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>

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/88469>



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 in Blood Vessel Scam](#)



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

NIST Cybersecurity Framework



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



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>

(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>

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

Ronnie Daldos
Kevin Littlefield
Sue Wang
David Weltzel
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 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



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>

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 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

Always ask and educate your patients about cybersecurity.

- 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 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.


© CTCRC 2021

The California Telehealth Resource Center (CTCRC) and resources and activities produced or supported by the CTCRC are made possible by grant number 94381224 from the Office for the Advancement of Telehealth, Health Resources and Services Administration (OATS). The information and conclusions herein are those of the CTCRC. They should not be construed as the official position or policy of HHS, HRSA, or the U.S. Government, nor official endorsement of any kind. If any of these entities, should be referred.

VIRTUAL CARE SECURITY TIPS for providers

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

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



PRACTICE GOOD CYBER HYGIENE

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

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

VIRTUAL CARE SECURITY TIPS for providers

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

Disclaimer: 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 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 device(s), 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 protocol for response to a possible data breach.

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

PATIENT SECURITY AND PRIVACY

Always risk and educate your patients about cyber security.

- 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

© CTCRC 2021

The California Telehealth Resource Center (CTCRC) and resources and activities produced or supported by the CTCRC are made possible by grant number 1A018212-01-0 from the Office for the Advancement of Telehealth, Health Resources and Services Administration (OATS). The information and conclusions herein are those of the CTCRC. They should not be construed as the official position or policy of HRSA, HHS or the U.S. Government, nor official endorsement of any kind. If any of these entities, should be referred.

FOLLOW SECURITY POLICY AND REGULATIONS

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

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

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 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

Mitigate risks and educate your patients about cybersecurity.

- 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 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

© CTRC 2021
The California Telehealth Resource Center (CTRC) and resources and activities produced or supported by the CTRC are made possible by grant number GA5RH37469 from the Office for the Advancement of Telehealth, Health Resources and Services Administration (DHHS). The information and conclusions herein are those of the CTRC. They should not be construed as the official position or policy of HHS, HRSA, or the U.S. Government, nor official endorsement of any kind. If any of these entities, should be referred.

PATIENT SECURITY AND PRIVACY

Mitigate risks and educate your patients about cybersecurity.



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



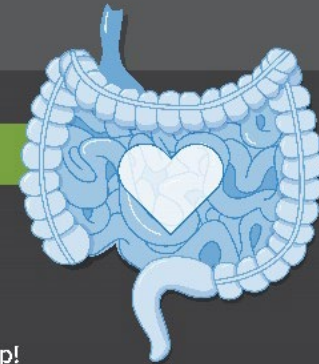
Educate patients about healthcare cybersecurity, including the benefits and risks of virtual care



Introduce any other staff present and explain why they are there

TRUST YOUR GUT

Often our senses alert us to trouble. If something 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/>

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
- 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

NCTRC Webinar – Ransomware In Health

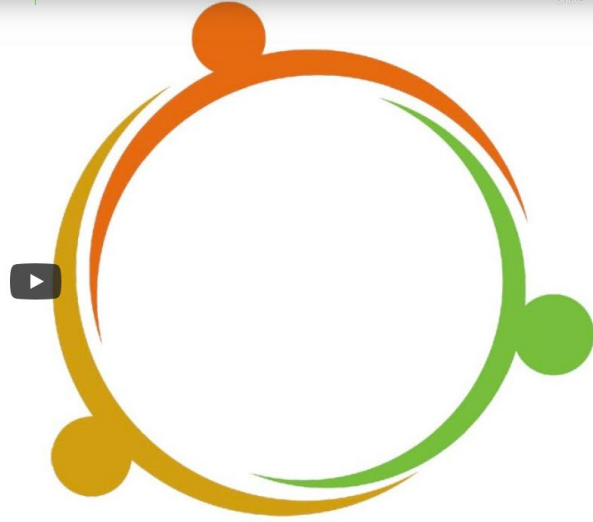
BY SOUTHWEST TELEHEALTH RESOURCE CENTER • OCTOBER 14, 2021

Ransomware in Health



Ransomware in Health

October 14, 2021



Watch on YouTube

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/>

ARIZONA
TELEMEDICINE
PROGRAM



Thank you!

Questions?

mholcomb@telemedicine.arizona.edu

