Maintaining Patient Privacy and Security in Telehealth

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

What comes to mind when you hear terms like HIPAA, cybersecurity training, information security policy and procedures?

Now, what imagine that your protected health information was compromised such that it cost you a personal loss of time, money, or confidentiality of your healthcare information.

What thoughts come to mind about the incident, the responsibilities of the healthcare provider or their business partner that was required to protect your health information?

Example Types of Telemedicine and Telehealth Communications (selected)

- Video conferencing
  - Face to face
  - Real-time medical imaging applications
- 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

https://youtu.be/BSsIBuUAVU4

SECURE EVERY THING!

- Computers are increasing integrated into to the things that we use, including medical devices, and they are also increasingly connected to and communicating via the Internet.
- Every device utilized to store, transmit, process, or access healthcare information, as well as therapeutic and monitoring devices involved in patient care delivery, has potential vulnerabilities. Some of these vulnerabilities are as of yet undiscovered, but it is essential to patch vulnerabilities rapidly as patches become available.

MEDPAGE TODAY

https://www.medpagetoday.com/practicemanagement/telehealth/88469

Practice Management > Telehealth

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

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 i Blood Vessel Scam

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home News Features I

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

HealthITSecurity › Latest Health Data Breaches

Latest Health Data Breaches News

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

Ransomware: Extortion Actors Leak Data, Vendor Attack Disrupts Services

April 08, 2021 by Jessica Davis
Ransomware threat actors are continuing to target the healthcare sector in droves. In the last month alone four hacking groups have posted data allegedly stolen from nine healthcare providers, while an attack on a vendor disrupted care at...

586K Trinity Health Patients Added to Accellion Tally, as Lawsuits Pile Up

April 08, 2021 by Jessica Davis
Michigan-based Trinity Health recently notified 586,869 patients that their data was compromised during the hack on Accellion's File Transfer Application (FTA). As the breach tally continues to expand, the vendor now faces at least...

Accellion Breach Tally for Centene's Subsidiaries: 1.3M Patients Impacted

April 06, 2021 by Jessica Davis
The Department of Health and Human Services' breach reporting tool shows over 1.3 million patients of Centene subsidiaries were impacted by the massive Accellion File Transfer Appliance vulnerability hack and subsequent data...

Allergy Partners: Data Stolen During Ransomware Attack, EHR Outage

May 18, 2021 - Following reports of a ransomware attack and subsequent EHR outage at Allergy Partners in February, the North Carolina specialist is notifying an undisclosed number of patients that their data was exfiltrated during the security event. As previously reported in March, the FBI was tasked with investigating a cyberattack on Allergy Partners that began on February 23 and lasted...

Read More

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...

MedTech Intelligence

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?

THE VERGE TWITTER FACEBOOK

SCIENCE

HEALTH CARE'S HUGE CYBERSECURITY PROBLEM

Cyberattacks aren't just going after your data

By Nicole Wetsman | Apr 4, 2019, 9:30am EDT

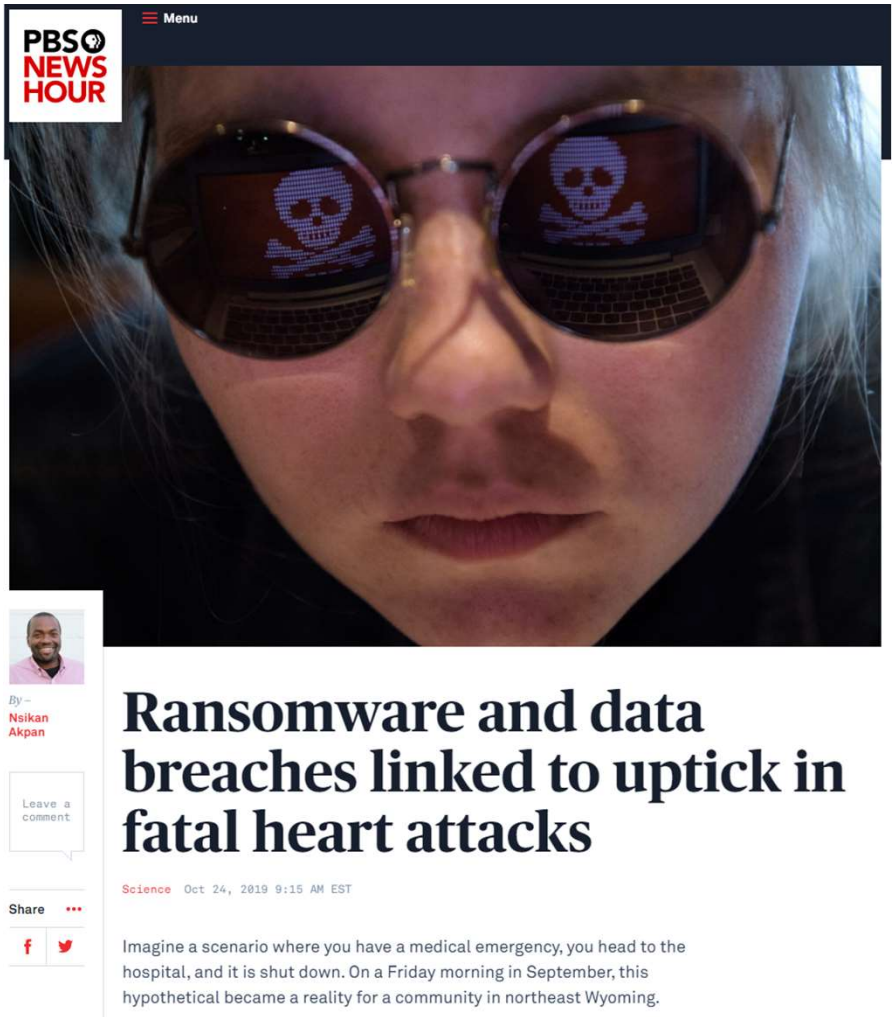
Illustration by Alex Castro / The Verge

SHARE

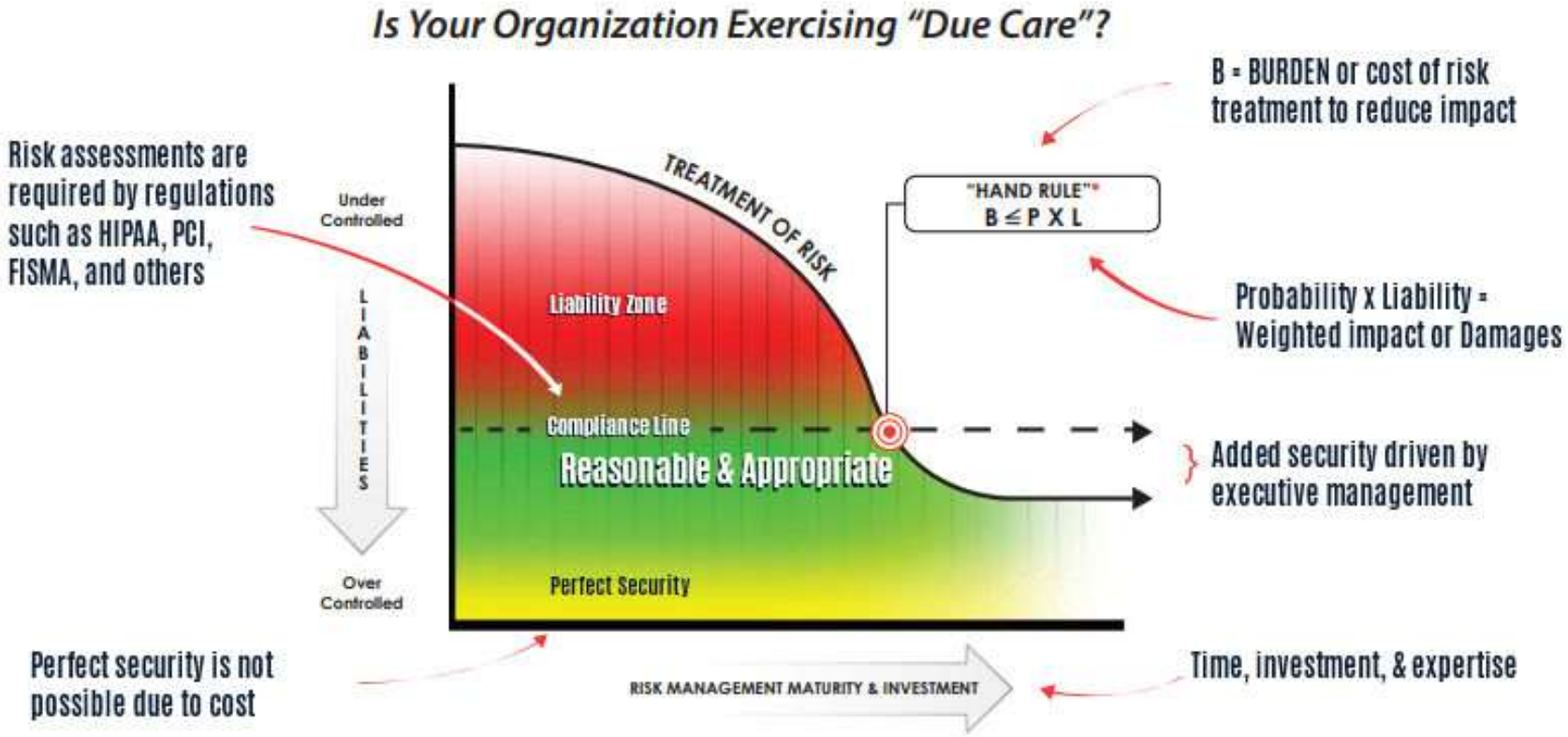
The patient lying on the emergency room table in front of Paul Pugsley was having a stroke. Time was running out. Pugsley, an emergency medicine resident at Maricopa Medical Center, knew he needed to send the patient for a CT scan.

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



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



https://www.halock.com/hand-rule-managing-upper-limits-security-costs/
https://en.wikipedia.org/wiki/Learned_Hand

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

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

Telemedicine and Telehealth Security

- **What needs to be secured?**
  - **Protected Health Information**
    - Both at rest and in transit
  - **All of the computing and network devices and systems and their associated firmware along with software that runs on those devices**
    - Network and computing infrastructure
    - End-user computing devices utilized by patients and providers
    - Medical devices prescribed by 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
- 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 a regularly updated copy 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

Make Security of Your Organization's Telemedicine Information and Communications "SIMPLER"

- Scalable
- Integral
- Managed
- Pro-active
- Layered
- Effective
- Responsive

Telemedicine 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

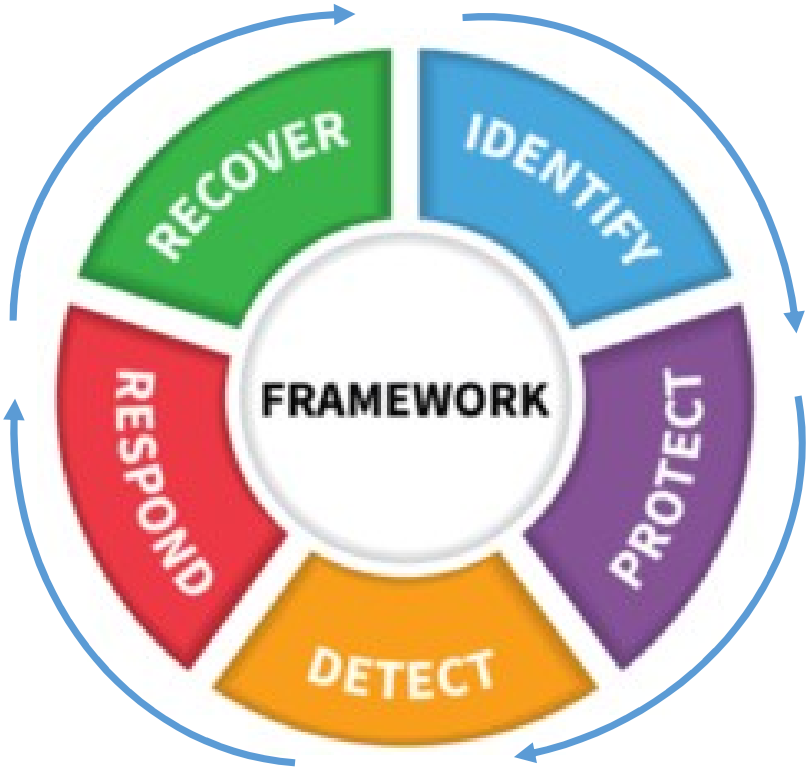
Telehealth Extra-Visit Communications and Data

- 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?

NIST Cybersecurity Framework

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

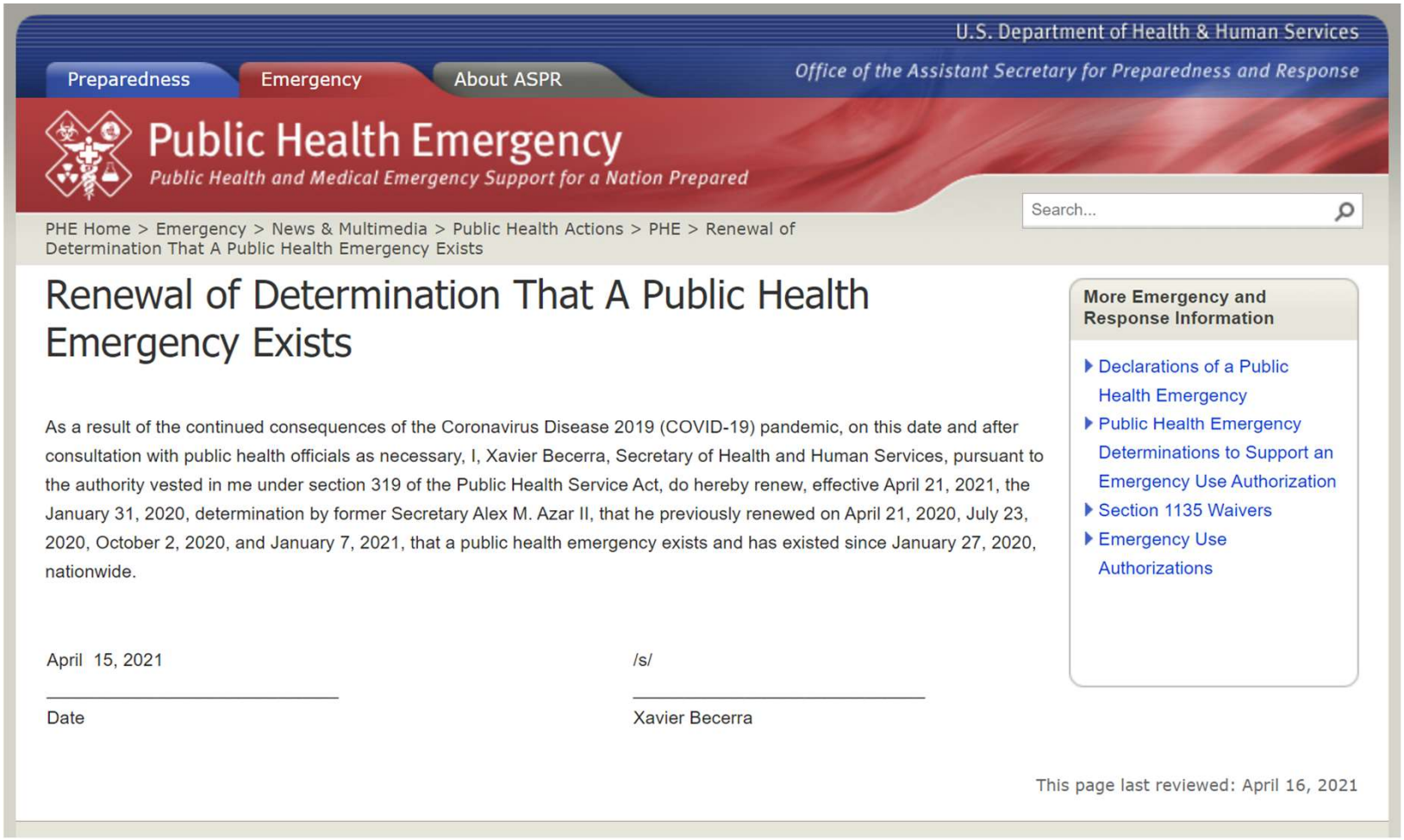
NIST Cybersecurity Framework



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

HHS.gov
Health Information Privacy
U.S. Department of Health & Human Services
I'm looking for...
HHS A-Z Index
HIPAA for Individuals
Filing a Complaint
HIPAA for Professionals
Newsroom
HHS > HIPAA Home > For Professionals > Special Topics > Emergency Preparedness > Notification of Enforcement Discretion for Telehealth
HIPAA for Professionals
Regulatory Initiatives
Privacy +
Security +
Breach Notification +
Compliance & Enforcement +
Special Topics −
HIPAA and COVID-19
Mental Health & Substance Use Disorders
De-Identification Methods
Text Resize A A A
Print
Share +
Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency
We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities. – Roger Severino, OCR Director.
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.

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



U.S. Department of Health & Human Services

Preparedness | Emergency | About ASPR

Office of the Assistant Secretary for Preparedness and Response

Public Health Emergency

Public Health and Medical Emergency Support for a Nation Prepared

Search...

PHE Home > Emergency > News & Multimedia > Public Health Actions > PHE > Renewal of Determination That A Public Health Emergency Exists

Renewal of Determination That A Public Health Emergency Exists

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 21, 2021, 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, that a public health emergency exists and has existed since January 27, 2020, nationwide.

April 15, 2021
Date

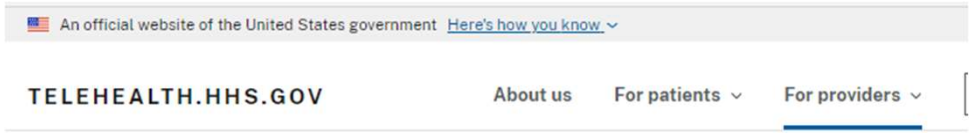
/s/
Xavier Becerra

This page last reviewed: April 16, 2021

More Emergency and Response Information

- Declarations of a Public Health Emergency
- Public Health Emergency Determinations to Support an Emergency Use Authorization
- Section 1135 Waivers
- Emergency Use Authorizations

https://www.phe.gov/emergency/news/healthactions/phe/Pages/COVID-15April2021.aspx



HIPAA flexibility for telehealth technology

Providers have more flexibility to use everyday technology for virtual visits during the COVID-19 public health emergency. HIPAA-compliant products also provide patient privacy protection for long-term use.

https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/hipaa-flexibility-for-telehealth-technology/#hipaa-flexibilities-during-covid-19

Technology considerations

What's allowed during COVID-19?

Under this notice, covered health care providers **may** use popular applications to deliver telehealth as long as they are "non-public facing." Examples of non-public facing applications include:

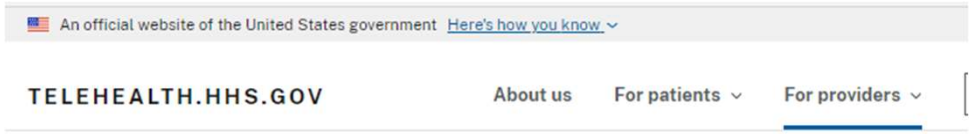
Video chat applications

- Apple FaceTime
- Facebook Messenger video chat
- Google Hangouts video
- Zoom
- Skype

Text-based applications

- Signal
- Jabber
- Facebook Messenger
- Google Hangouts
- WhatsApp
- iMessage

Examples of **public facing applications not allowed for this use** are Facebook Live and Twitch.



HIPAA flexibility for telehealth technology

Providers have more flexibility to use everyday technology for virtual visits during the COVID-19 public health emergency. HIPAA-compliant products also provide patient privacy protection for long-term use.

https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/hipaa-flexibility-for-telehealth-technology/#hipaa-flexibilities-during-covid-19

HIPAA-compliant technology

Under this notice, covered health care **providers that seek additional privacy protections** should use technology vendors that are HIPAA compliant and will enter into HIPAA business associate agreements in connection with the provision of their video communication products. The list below includes some vendors that say they provide HIPAA-compliant video communication products and that they will enter into a HIPAA business associate agreement.

Although it's always important to confirm, examples of vendors who say they meet HIPAA requirements include:

- 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

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

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-security-lagging-behind

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

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

By Jessica Davis

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

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

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

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

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

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

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

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

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home News Features In

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

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

BECKER'S HOSPITAL REVIEW

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

Telemedicine creates big cybersecurity risks, Harvard researchers say

Jackie Drees - Thursday, December 17th, 2020 Print | Email

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.

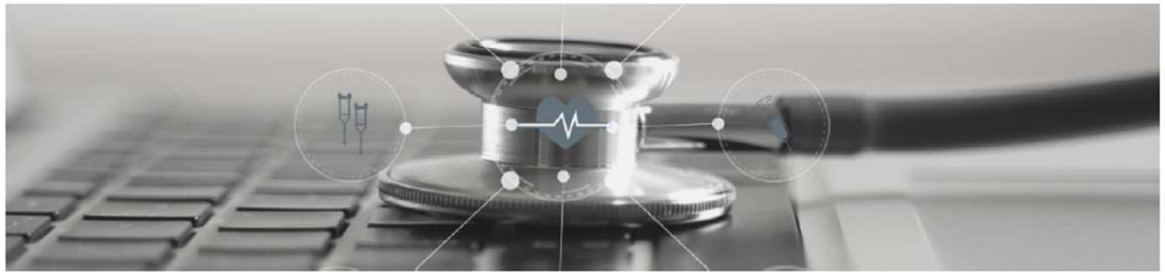
5. While prevention and detection capabilities are critical, organizations should also prepare with incident response plans in the event they do get hit by a cyberattack so they are well prepared and minimize negative consequences.

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

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY - SECURING TELEHEALTH AND TELEMEDICINE

April 2021

Associated Cybersecurity Risk

Expanding use of remote technology in healthcare, including for telehealth and telemedicine, has been accompanied by a substantial increase in connectivity and exposure. According to a recent study by SecurityScorecard and DarkOwl LLC, the rapid adoption and onboarding of telehealth vendors has led to a significantly increased digital footprint and attack surface, leaving both provider and patient data at risk[7].

Consequently, hackers and criminal groups are able to exploit these vulnerabilities and easily infiltrate a network for financial gain or operational disruption. For example, in 2020 according to the study, telehealth providers have experienced a nearly exponential increase in targeted attacks as popularity skyrocketed.

- 117% increase in website/IP malware security alerts
- 65% increase in security patching of known vulnerabilities
- 56% increase in endpoint vulnerabilities that enable data theft
- 16% increase in patient-accessed web application vulnerabilities
- 42% increase in file transfer protocol vulnerabilities that expose information travelling between a client and a server on a network
- 27% increase in remote desktop protocol security issues given the widespread adoption of remote work

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

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY - SECURING TELEHEALTH AND TELEMEDICINE

April 2021

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 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

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
  - Accurate source of truth
  - Operates as designed and intended
  - Change logs
- Availability
  - Accessible and usable as designed and on demand commensurate with service requirements

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.*

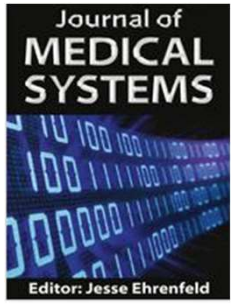
The American Medical Association (AMA) and American Hospital Association (AHA) have monitored a variety of technology issues associated with the novel coronavirus and developed a range of resources to assist their members, including our joint resource, What Physicians Need to Know: Working from home 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



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

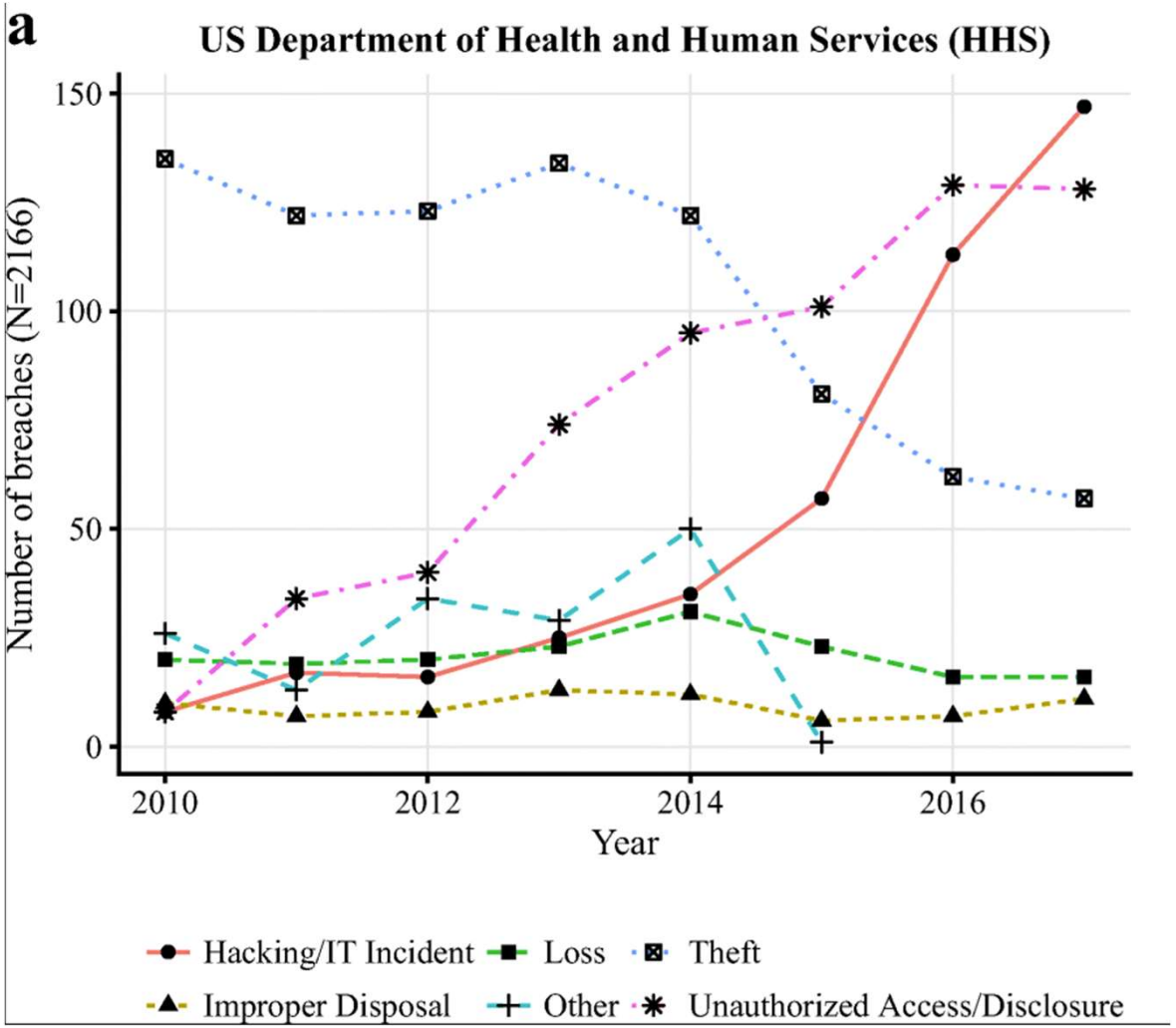


Figure 1 part a
Breakdown of healthcare breach types by year based on data provided by the US Department of Health and Human Services (HHS) including archived breaches and breaches under investigation
(2010- Apr 2018)

HIPAA JOURNAL

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/

Welcome File a

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.

Show Advanced Options

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
	Bayhealth Medical Center, Inc.	DE	Healthcare Provider	565	05/18/2021	Hacking/IT Incident	Network Server
	The Miriam Hospital	RI	Healthcare Provider	2999	05/17/2021	Unauthorized Access/Disclosure	Email
	New England Dermatology, P.C.	MA	Healthcare Provider	58106	05/11/2021	Improper Disposal	Paper/Films
	Master Equity Texas Limited Partnership	TX	Healthcare Clearing House	1962	05/11/2021	Unauthorized Access/Disclosure	Email
	Shands Teaching Hospitals and Clinics, Inc.	FL	Healthcare Provider	1562	05/07/2021	Unauthorized Access/Disclosure	Electronic Medical Record
	Exceltox Laboratories	CA	Healthcare Provider	4571	05/07/2021	Loss	Paper/Films
	Nocona General Hospital	TX	Healthcare Provider	3254	05/07/2021	Hacking/IT Incident	Network Server
	MidMichigan Health Services	MI	Healthcare Provider	2800	05/07/2021	Hacking/IT Incident	Network Server
	Charles Cole Memorial Hospital, d/b/a UPMC Cole	PA	Healthcare Provider	7376	05/07/2021	Hacking/IT Incident	Network Server
	Our Lady of Lourdes Memorial Hospital Inc.,	NY	Healthcare Provider	1745	05/07/2021	Hacking/IT Incident	Network Server
	St. Agnes Healthcare Inc.	MD	Healthcare Provider	2821	05/07/2021	Hacking/IT Incident	Network Server
	Ascension Standish Hospital	MI	Healthcare Provider	1705	05/07/2021	Hacking/IT Incident	Network Server
	Ascension St. Joseph Hospital	MI	Healthcare Provider	5807	05/07/2021	Hacking/IT Incident	Network Server
	Brownsville Community Health Center dba New Horizon Medical Center	TX	Healthcare Provider	4258	05/06/2021	Hacking/IT Incident	Network Server
	Tyler Family Circle of Care	TX	Healthcare Provider	1860	05/06/2021	Hacking/IT Incident	Network Server
	Implant and Prosthodontic Associates	OK	Healthcare Provider	6134	05/06/2021	Theft	Other Portable Electronic Device
	SummaCare	OH	Health Plan	5532	05/06/2021	Unauthorized Access/Disclosure	Paper/Films
	NEC Networks, LLC d/b/a CaptureRx	TX	Business Associate	1656569	05/05/2021	Hacking/IT Incident	Network Server
	Orthopedic Associates of Dutchess County	NY	Healthcare Provider	331376	05/04/2021	Hacking/IT Incident	Network Server
	Monadnock Community Hospital	NH	Healthcare Provider	14340	05/04/2021	Hacking/IT Incident	Network Server
	Arizona Asthma and Allergy Institute	AZ	Healthcare Provider	50000	05/03/2021	Hacking/IT Incident	Network Server

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

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home News Features In

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

HealthITSecurity › Latest Health Data Breaches

Latest Health Data Breaches News

https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020

UPDATE: The 10 Biggest Healthcare Data Breaches of 2020

Much like in 2019, the biggest healthcare data breach of 2020 was caused by a third-party vendor, while ransomware and other risks dominated the threat landscape.

By Jessica Davis

December 10, 2020 Cybersecurity proved to be a massive challenge for many in the healthcare sector in 2020 as providers worked to combat the COVID-19 crisis, while simultaneously being pummeled with targeted cyberattacks. These led to some of the biggest healthcare data breaches seen in recent years.

While the first half of the year saw a reduction in the number of reported incidents, active threats continued to plague the sector, from ransomware to insiders, which came to a head in September with a steady **onslaught** of ransomware attacks.

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home News Features In

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

HealthITSecurity › Latest Health Data Breaches

Latest Health Data Breaches News

https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far

July 08, 2020

1. HEALTH SHARE OF OREGON: 654,000 PATIENTS

READ MORE: Magellan Health Data Breach Victim Tally Reaches 365K Patients

The theft of a laptop owned by the transportation vendor of the **Health Share** of Oregon, shows that physical security controls and vendor management need equal attention as cybersecurity priorities.

Oregon's largest Medicaid coordinated care organization notified 654,000 patients due to the device theft from its vendor GridWorks. The notification did not clarify whether the laptop was encrypted. But the stolen device contained patient names, contact details, dates of birth, and Medicaid ID numbers.

Fortunately, health histories were not stored on the laptop. Health Share updated its annual audit processes with its contractors and improved workforce training, in response.

2. FLORIDA ORTHOPAEDIC INSTITUTE: 640,000 PATIENTS

A ransomware attack on the Florida Orthopaedic Institute (FOI) potentially breached the data of about 640,000 patients, as reported to HHS on July 1.

The attack was first discovered on or about April 9, with the malware encrypting data stored on FOI servers. Administrators were able to quickly secure the system, but the investigation found that patient data was potentially exfiltrated or accessed during the attack.

3. ELITE EMERGENCY PHYSICIANS (FORMERLY KNOWN AS ELKHART EMERGENCY PHYSICIANS): 550,000 PATIENTS

The provider now known as **Elite** Emergency Physicians was included in a massive security incident involving the improper disposal of patient records, including records from its **Elkhart** Emergency Physicians.

In **June**, it was reported that third-party vendor Central Files, which was tasked with secure record storage and disposal for a number of healthcare covered entities, had improperly disposed of some patient files. The impacted providers also included St. Joseph

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home News Features In

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

HealthITSecurity › Latest Health Data Breaches

Latest Health Data Breaches News

https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020

December 10, 2020

Importantly, multiple providers faced attempted extortion after data exfiltration, some of which have not yet been reported to HHS and as such, are not included. The list also does not account for some massive data leaks, such as those caused by vulnerabilities in **PACS**.

However, these leading breaches do highlight the continued work providers must take, even as the pandemic stretches on into the new year. As hackers have fully demonstrated in 2020, there's no honor among thieves even during a global crisis.

1. BLACKBAUD: DOZENS OF HEALTHCARE ENTITIES, MILLIONS OF PATIENTS

Much like in 2019, the largest healthcare data breach was caused by a third-party vendor. The Blackbaud ransomware attack mirrored the **AMCA** breach, as it's still unclear just how much data and how many providers were affected.

It's estimated that more than two dozen providers and well over 10 million patients have been included in the final breach tally.

2. DCA ALLIANCE: 1,000,000 PATIENTS

Reported in early December, a near-monthlong system hack on third-party vendor Dental Care Alliance potentially breached the protected health information and payment card numbers of 1 million patients. DCA is a practice support vendor for more than 320 affiliated practices across

3. LUXOTTICA: 829,454 PATIENTS

Eyecare conglomerate Luxottica of America faced at **least** two security incidents this fall, one directly involving the breach of patient data.

In **August**, a threat actor gained access to the web-based appointment scheduling application managed by Luxottica and used by its eyecare providers to help patients make appointments. The hack went on for four days before it was detected.

An investigation later determined the hacker was able to access a trove of patient data, including full appointment notes related to treatment, health insurance policy numbers, health conditions, prescriptions, appointment dates and times, and other sensitive information.

The attacker may have also accessed and acquired third-party information from the app, while some patients also saw their SSNs and credit card information breached.

Evaluation of Causes of Protected Health Information Breaches

- Study of 1138 breaches reported to US HHS between 2009 and 12/31/2017, affecting 164 million patients
- **53% of breaches due to internal causes** including loss, theft, mailing mistakes, unauthorized access, phishing
- **47% of breaches due to external causes** including theft, malware, loss by business associate
- **Of all 1138 breaches (internal and external causes)**
  - 41.5% theft
  - 25% unauthorized access
  - 20.5% hacking or IT incident
  - 10.5% loss
  - 3% due to improper disposal
- John (Xuefeng) Jiang, PhD, Ge Bai, PhD, CPA, JAMA Internal Medicine February 2019 Volume 179, Number 2, August 2018

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.

https://rgw.arizona.edu/sites/researchgateway/files/hipaa_data_reference_guide_12.21.2016.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.

NIST Cybersecurity Framework

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

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

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

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

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 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

(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 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

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

Ronnie Daldos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

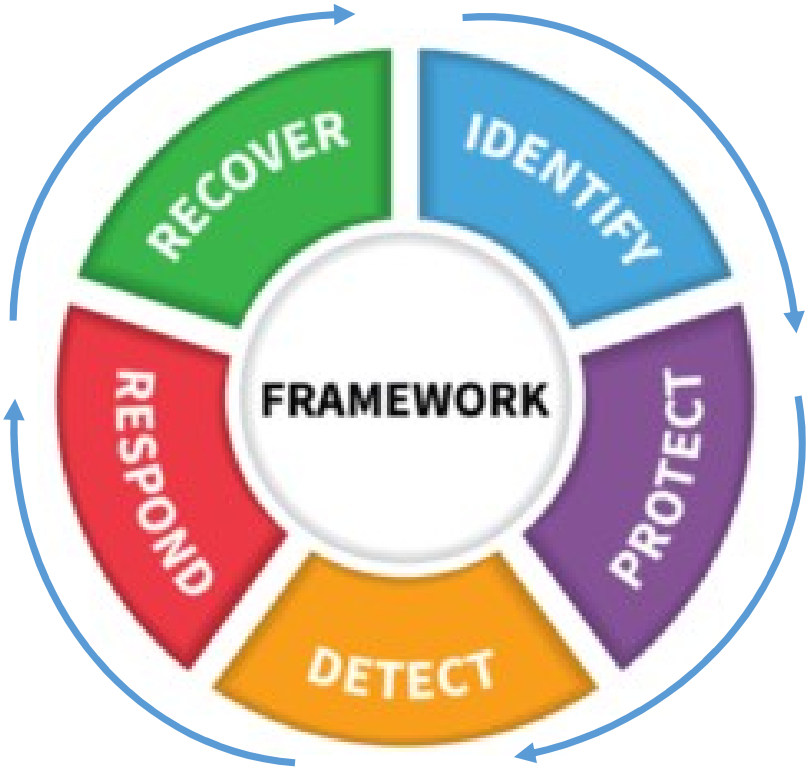
May 2019
hit_nccoe@nist.gov

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

NIST Cybersecurity Framework



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

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 Lack of IT resource for managing suspicious e-mails Lack of software scanning e-mails for malicious content or bad links Lack of e-mail detection software testing for malicious content Lack of e-mail sender and domain validation tools	Loss of reputation in the community (referrals dry up, patients leave the practice) Stolen access credentials used for access to sensitive data Erosion of trust or brand reputation Potential negative impact to the ability to provide timely and quality patient care Patient safety concerns	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) Train staff to recognize suspicious e-mails and to know where to forward them (1.S.B) Never open e-mail attachments from unknown senders (1.S.B) Tag external e-mails to make them recognizable to staff (1.S.A) 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)

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

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

PROJECT DESCRIPTION

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

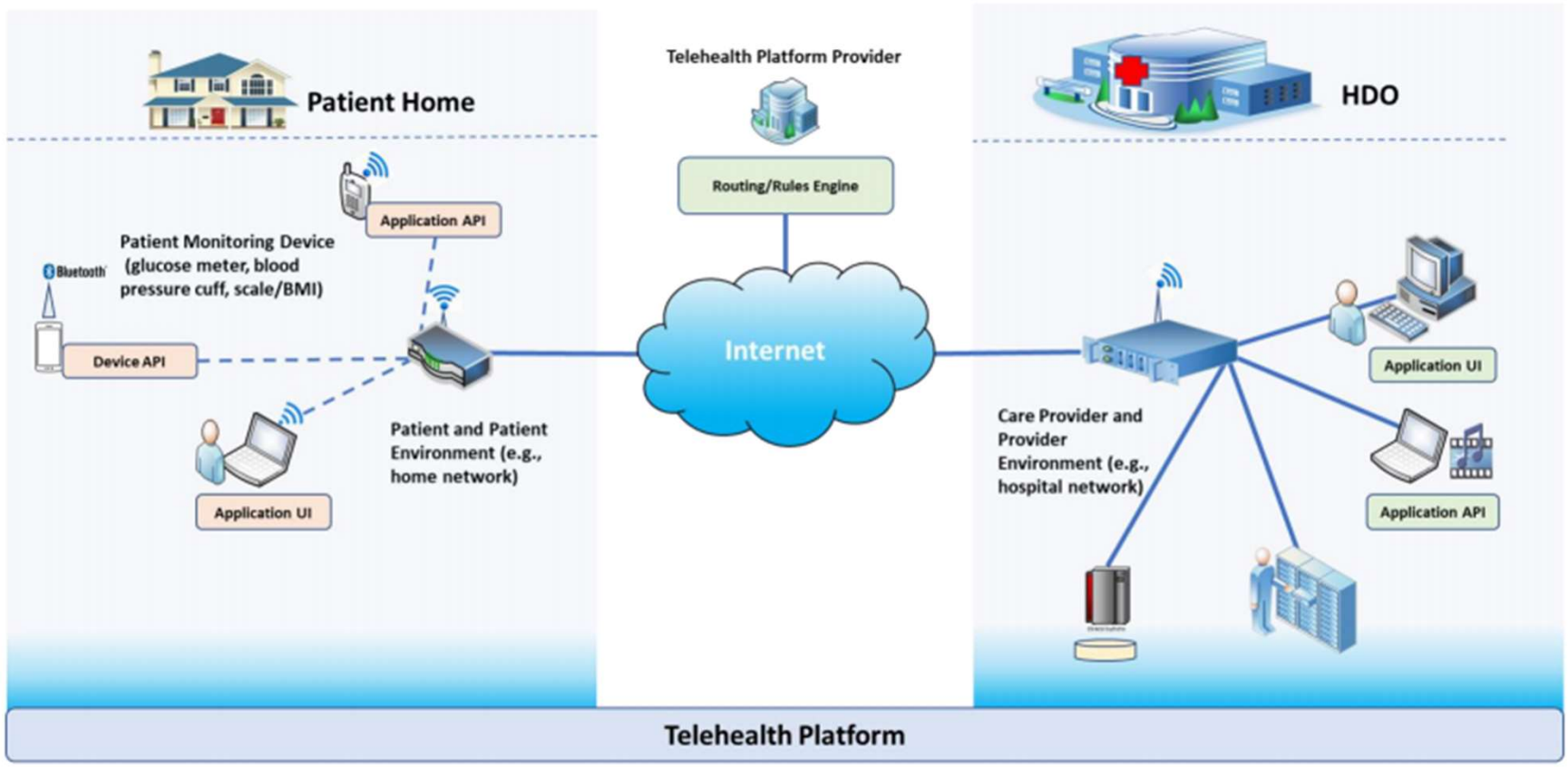
NCCoE National Cybersecurity Center of Excellence

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.

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

ARIZONA TELEMEDICINE PROGRAM

SOUTHWEST TRC TELEHEALTH RESOURCE · CENTER™

Thank you!

Questions?

mholcomb@telemedicine.arizona.edu