

ARIZONA
TELEMEDICINE
PROGRAM



Securing Telemedicine Communications

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

Example Types of Telemedicine and Telehealth Communications

- Video conferencing
 - Face to face
 - Medical imaging
- 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



COVID-19 Resource Center

Topics ▾

News ▾

Training ▾

Resources ▾

Events ▾

Jobs ▾



Endpoint Security , Governance & Risk Management

Telehealth App Breach Spotlights Privacy, Security Risks

Glitch Briefly Allowed Potential Access to Patient Consultation Recordings

Marianne Kolbasuk McGee (HealthInfoSec) • June 10, 2020

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

I'm looking for...

[HHS A-Z Index](#)HIPAA for
IndividualsFiling a
ComplaintHIPAA 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.

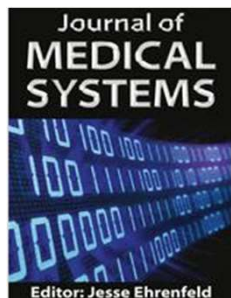
The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) is responsible for enforcing certain regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (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.youtube.com/watch?v=bPVaOIJ6In0>



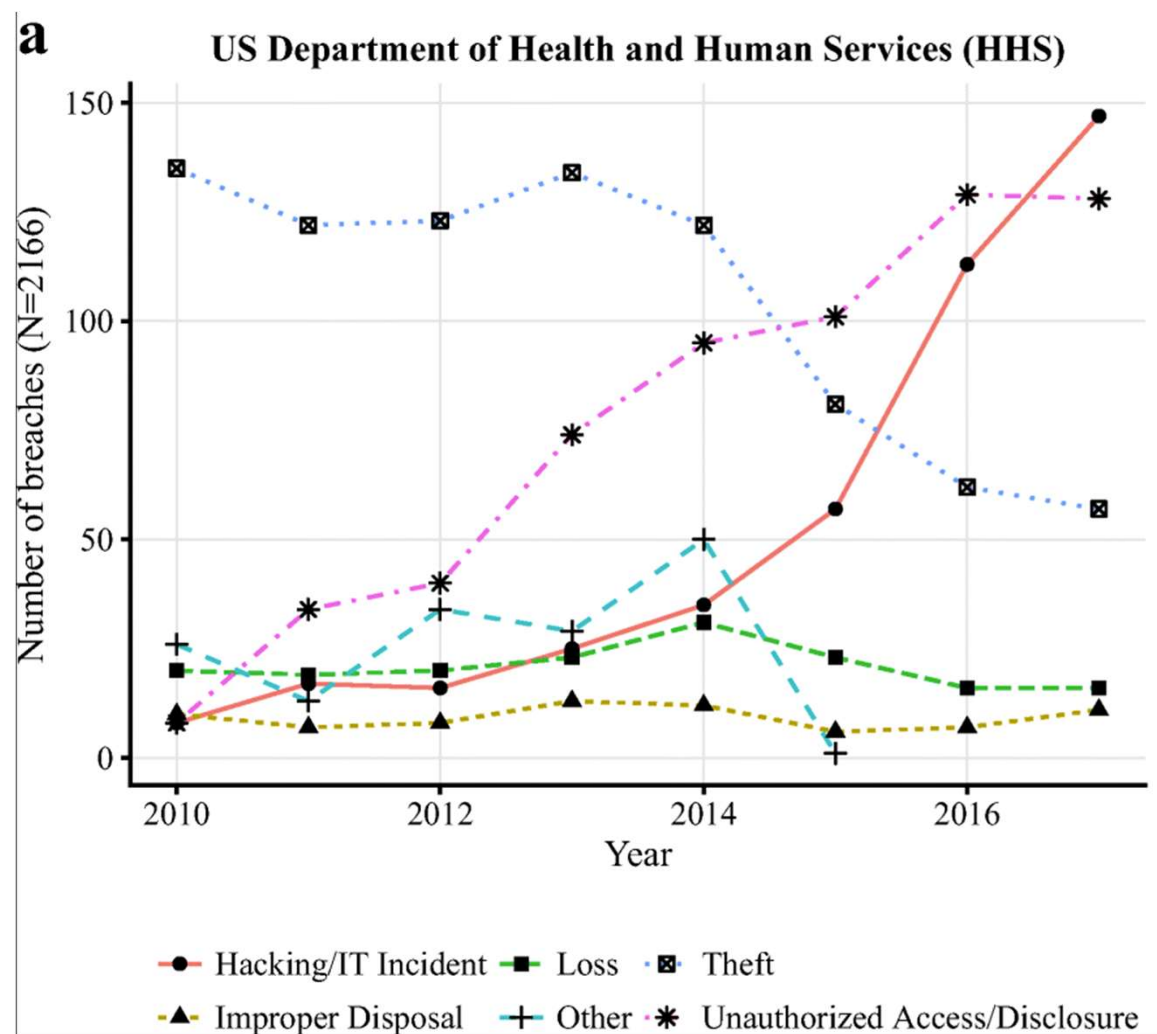
Healthcare Data Breaches: Implications for Digital Forensic Readiness

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

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

Figure 1 part a

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





Healthcare Data Breach Statistics

Breaches by Covered Entity Type

Year	Healthcare Provider	Health Plan	Business Associate	Healthcare Clearinghouse	Total
2009	14	1	3	0	18
2010	134	21	44	0	199
2011	137	20	42	1	200
2012	152	22	40	1	215
2013	190	19	64	2	275
2014	193	40	77	0	310
2015	195	61	14	0	270
2016	256	51	22	0	329
2017	284	52	21	0	357
2018	276	53	42	0	371
2019	396	59	53	2	510
Total	2227	399	422	6	3054

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

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
1	Renee Applebaum Phd Pc	MI	Healthcare Provider	3800	05/24/2020	Hacking/IT Incident	Network Server
1	Medicaid, LLC	MI	Business Associate	14931	05/22/2020	Hacking/IT Incident	Network Server
1	Woodlawn Dental Center	OH	Healthcare Provider	14419	05/18/2020	Hacking/IT Incident	Network Server
1	Geisinger Wyoming Valley Medical Center	PA	Healthcare Provider	805	05/18/2020	Unauthorized Access/Disclosure	Electronic Medical Record
1	Mat-Su Surgical Associates, APC	AK	Healthcare Provider	13146	05/15/2020	Hacking/IT Incident	Laptop, Network Server
1	Alexander Chun, MD, PLLC	NY	Healthcare Provider	595	05/12/2020	Improper Disposal	Paper/Films
1	Mille Lacs Health System	MN	Healthcare Provider	10630	05/11/2020	Hacking/IT Incident	Email
1	District Medical Group	AZ	Healthcare Provider	10190	05/08/2020	Hacking/IT Incident	Email
1	Ashtabula County Medical Center	OH	Healthcare Provider	3683	05/08/2020	Unauthorized Access/Disclosure	Other
1	Midmark RTLS Solutions, Inc.	MI	Business Associate	7422	05/05/2020	Hacking/IT Incident	Other
1	The Nebraska Medical Center	NE	Healthcare Provider	1311	05/05/2020	Unauthorized Access/Disclosure	Electronic Medical Record
1	Management and Network Services, LLC	OH	Business Associate	30132	05/04/2020	Hacking/IT Incident	Email
1	Ann & Robert H. Lurie Children's Hospital of Chicago	IL	Healthcare Provider	4824	05/04/2020	Unauthorized Access/Disclosure	Electronic Medical Record
1	Saint Francis Healthcare Partners	CT	Business Associate	38529	05/04/2020	Hacking/IT Incident	Email
1	Lisa Burkett DDS MS	TX	Healthcare Provider	818	04/30/2020	Unauthorized Access/Disclosure	Email
1	Stamford Hospital, The	CT	Healthcare Provider	1255	04/30/2020	Unauthorized Access/Disclosure	Email

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

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



© 2020 ARIZONA TELEMEDICINE PROGRAM



Latest Health Data Breaches News

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

Articles

Ransomware Attack on Magellan Health Results in Data Exfiltration

May 13, 2020 by Jessica Davis

Arizona-based Magellan Health is notifying an undisclosed number of its current employees that their data was compromised after threat actors first exfiltrated sensitive data, before deploying a ransomware attack in April. On April 11,...

Maze Ransomware Hackers Post Patient Data Stolen from 2 Providers

May 06, 2020 by Jessica Davis

The notorious Maze ransomware hacking group has failed to follow through with their assurance the healthcare sector would be off-limits during the COVID-19 pandemic, by publishing data stolen from two separate plastic surgeons for sale on...

Ransomware Shuts Down Colorado Hospital IT Network Amid COVID-19

April 28, 2020 by Jessica Davis

Colorado-based Parkview Medical Center's technology infrastructure was hit with a ransomware attack a week ago on April 21, which caused a number of IT network outages, according to local news outlet KOAA. The hospital is...

Beaumont Health Reports 2019 Data Breach Impacting 114K Patients

April 21, 2020 by Jessica Davis

Michigan-based Beaumont Health recently began notifying about 114,000 patients that their personal data was potentially breached after a hack on several employee email accounts in 2019. The notification does not explain when the breach...

Ransomware Attack on Brandywine Urology Impacts 131K Patients

April 14, 2020 by Jessica Davis

About 131,825 patients of Brandywine Urology Consultants are being notified that their data was potentially compromised during a ransomware attack. The Delaware specialist is continuing to investigate the scope of the incident. On January...

Latest Health Data Breaches News

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

Articles

National Cardiovascular Partners Email Hack Impacts 78K Patients

July 27, 2020 by Jessica Davis

National Cardiovascular Partners recently notified 78,070 patients that their data was potentially compromised after an attacker gained access to an employee email account. According to its notice to California Attorney General...

Lorien Health Services Ransomware Attack Impacts 48K Patients

July 21, 2020 by Jessica Davis

Maryland Health Services, DBA Lorien Health Services, recently reported that a June ransomware attack on its systems potentially breached the data of 47,754 patients. Lorien operates assisted living facilities in the...

274K Patients Impacted by Benefit Recovery Specialists Credential Hack

July 13, 2020 by Jessica Davis

More than 274,000 patients from several healthcare providers and payers that use Benefit Recovery Specialists (BRSI) for billing and collections services are being notified that their data was potentially...

UPDATE: The 10 Biggest Healthcare Data Breaches of 2020, So Far

July 08, 2020 by Jessica Davis

The healthcare sector saw a whopping 41.4 million patient records breached in 2019, fueled by a 49 percent increase in hacking, according to the Protenus Breach Barometer. And despite the COVID-19 crisis, the pace of...

Magellan Health Data Breach Victim Tally Reaches 365K Patients

July 07, 2020 by Jessica Davis

The extent of the ransomware attack that hit Arizona-based Magellan Health in April became clear this week, with eight Magellan Health affiliates and healthcare providers reporting breaches stemming...

American Medical Tech Reports 2019 Email Hack Impacting 47K Patients

June 30, 2020 by Jessica Davis

California-based American Medical Technologies (AMT), a healthcare supplier, recently began notifying 47,767 patients that their data was potentially breached after a hack of an employee email account in 2019. On...

Care New England Resolves Weeklong Cyberattack Impacting Servers

June 22, 2020 by Jessica Davis

Rhode Island-based Care New England (CNE) has fully recovered from a cyberattack that hit its servers nearly a...

Latest Health Data Breaches News

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

UPDATE: The 10 Biggest Healthcare Data Breaches of 2020, So Far

Despite the COVID-19 crisis, phishing campaigns, mishandled health record disposals, and sophisticated cyberattacks are behind some of the biggest healthcare data breaches of 2020.



By Jessica Davis



July 08, 2020 - The healthcare sector saw a whopping 41.4 million patient records breached in 2019, fueled by a 49 percent increase in hacking, according to the **Protenus** Breach Barometer. And despite the COVID-19 crisis, the pace of healthcare data breaches in 2020 continue to highlight some of the sector's biggest vulnerabilities.

Latest Health Data Breaches News

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

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

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.

Why do we need to secure telemedicine technologies and communications?

- Protect patients
- Good business practice to maintain confidentiality of patient information
 - Patients will 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



<https://youtu.be/BSsIBuUAVU4>

SECURE EVERY THING!

- Computers are increasingly integrated into the things that we use, including medical devices, and they are also increasingly connected to and communicating via the Internet.

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 utilized by patients and providers

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.

What are some of the most effective things we can do to secure telemedicine communications?

- Understand telemedicine data communication flows
- Utilize secure technologies
- Limit network access to authorized users
- Encrypt PHI in transit and at rest
- Use multi-factor authentication
- Lock sessions and devices after defined periods of idle time requiring re-authentication to access PHI again
- Limit physical access to systems that store, transmit, or process PHI
- Utilize malware prevention systems and services
- Maintain “Air-gapped” backups of PHI and critical systems
- Conduct regular risk assessments and modify security to minimize risks
- Train all users of organization’s systems about information security practices
- Prioritize testing and deployment of security related patches/fixes
- Log access and review for irregularities, Test for vulnerabilities, Manage changes

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

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

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



<https://youtu.be/BSsIBuUAVU4>

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

SCIENCE

HEALTH CARE'S HUGE CYBERSECURITY PROBLEM

Cyberattacks aren't just going after your data

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

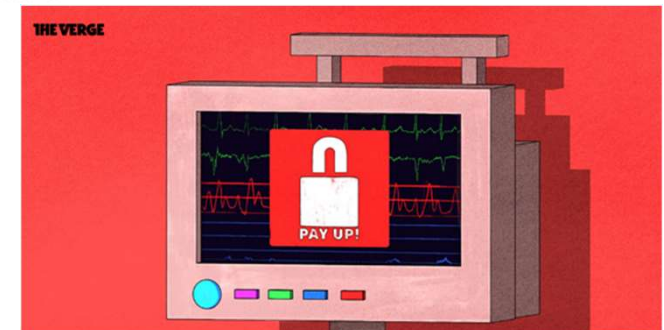
Illustration by Alex Castro / The Verge



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>

PBS NEWS HOUR Menu



By: **Nsikan Akpan**

Leave a comment

Share

Science Oct 24, 2019 9:15 AM EST

Ransomware and data breaches linked to uptick in fatal heart attacks

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>

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>

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

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

Ronnie Dailos
Kevin Littlefield
Sue Wang
David Weltzel
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 Castra
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Ronnie Dailos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov



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

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



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

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

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

Ronnie Dailos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov



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

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



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

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

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

Ronnie Dailos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov



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

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

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

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

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

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

© 2020 ARIZONA TELEMEDICINE PROGRAM

SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM

Cybersecurity for the Healthcare Sector

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

Ronnie Daldos
Kevin Littlefield
Sue Wang
David Weitzel
The MITRE Corporation

May 2019
hit_nccoe@nist.gov

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

NCCOE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE



2 SCENARIO: REMOTE PATIENT MONITORING AND VIDEO TELEHEALTH

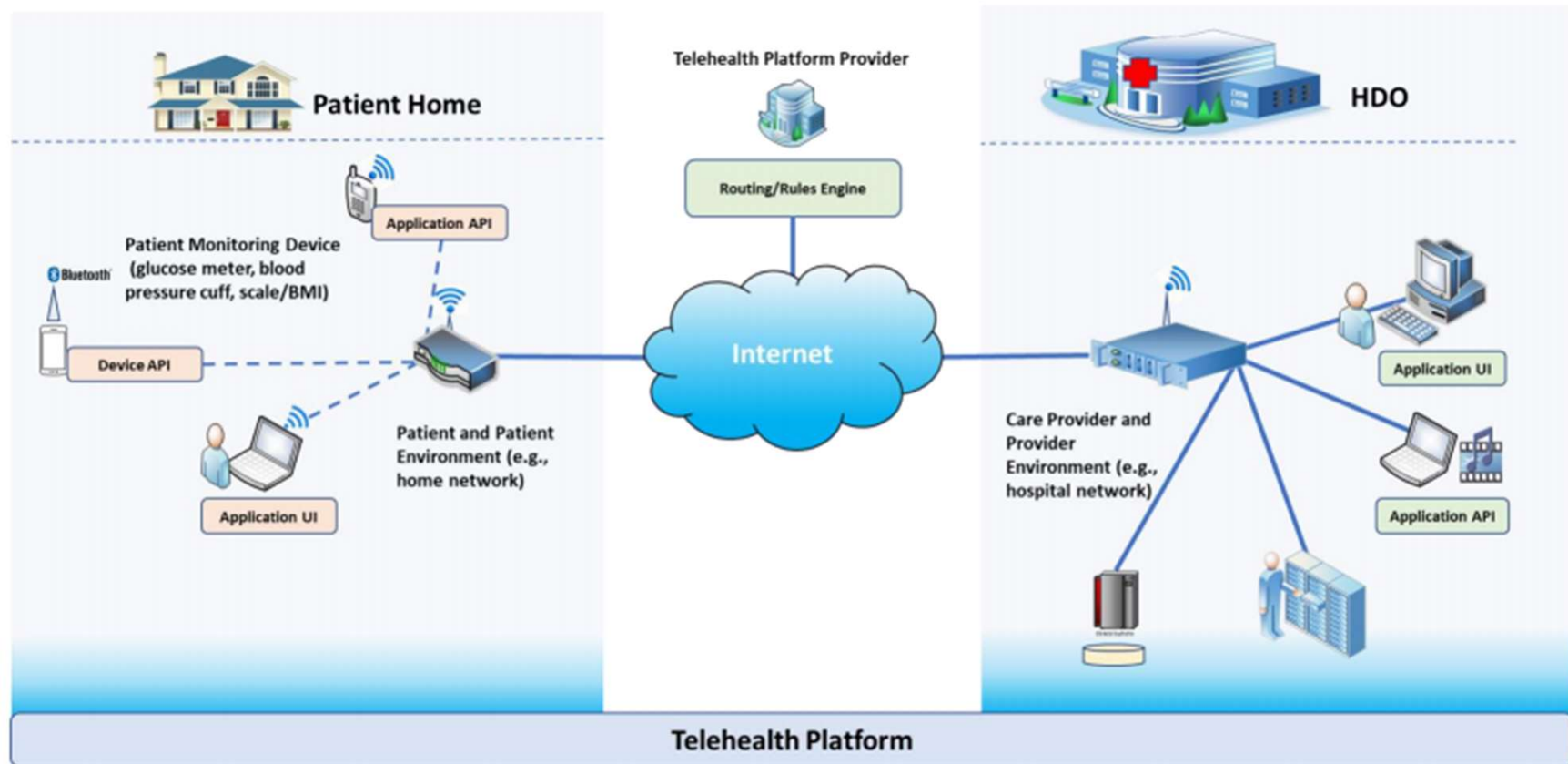
The scenario considered for this project involves RPM equipment deployed to the patient's home [2]. RPM equipment that may be provided to patients includes devices for blood pressure monitoring, heart rate monitoring, BMI/weight measurements, and glucose monitoring. An accompanying application may also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

Project Description: Securing Telehealth Remote Patient Monitoring Ecosystem

5

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

Figure 3-1: High-Level Architecture

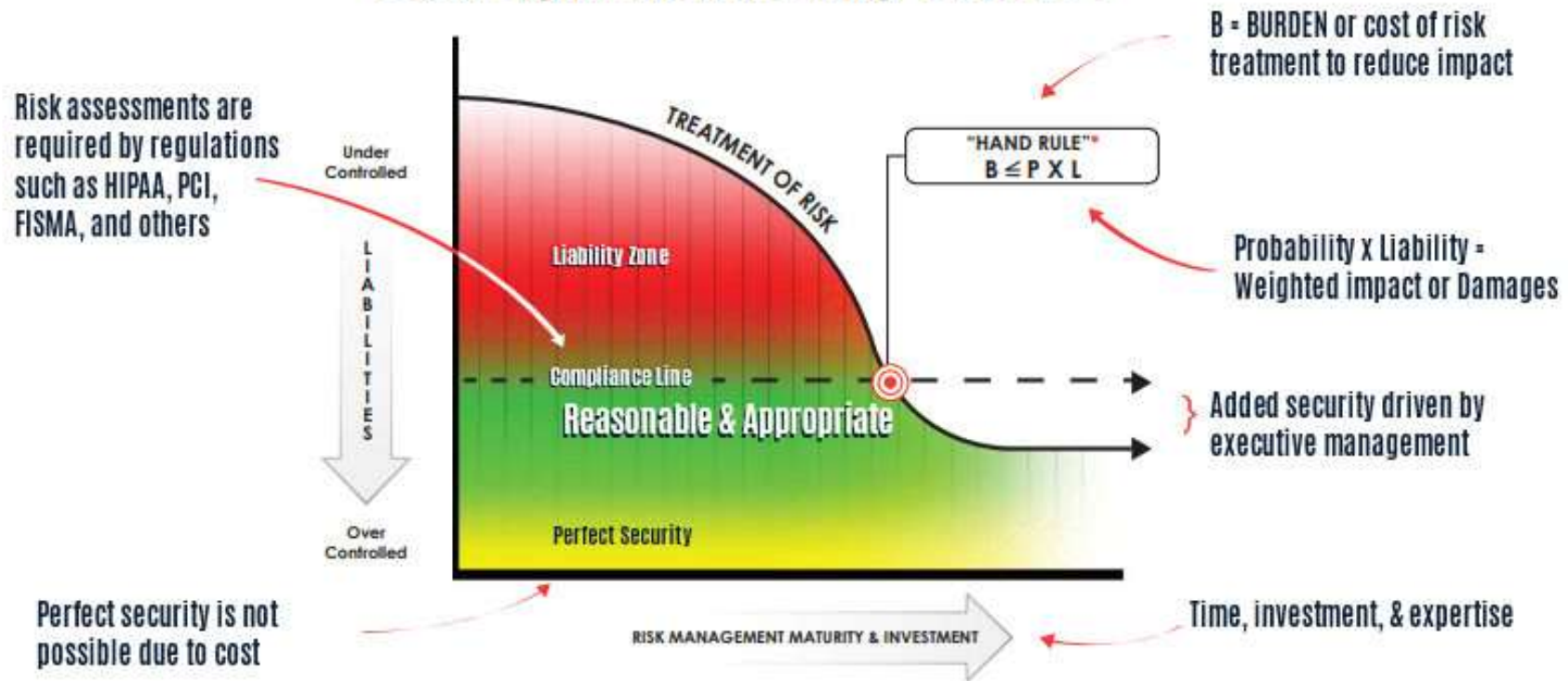


<https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf>

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>

Is Your Organization Exercising "Due Care"?



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

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

ARIZONA
TELEMEDICINE
PROGRAM



Thank you!

Questions?

mholcomb@telemedicine.arizona.edu