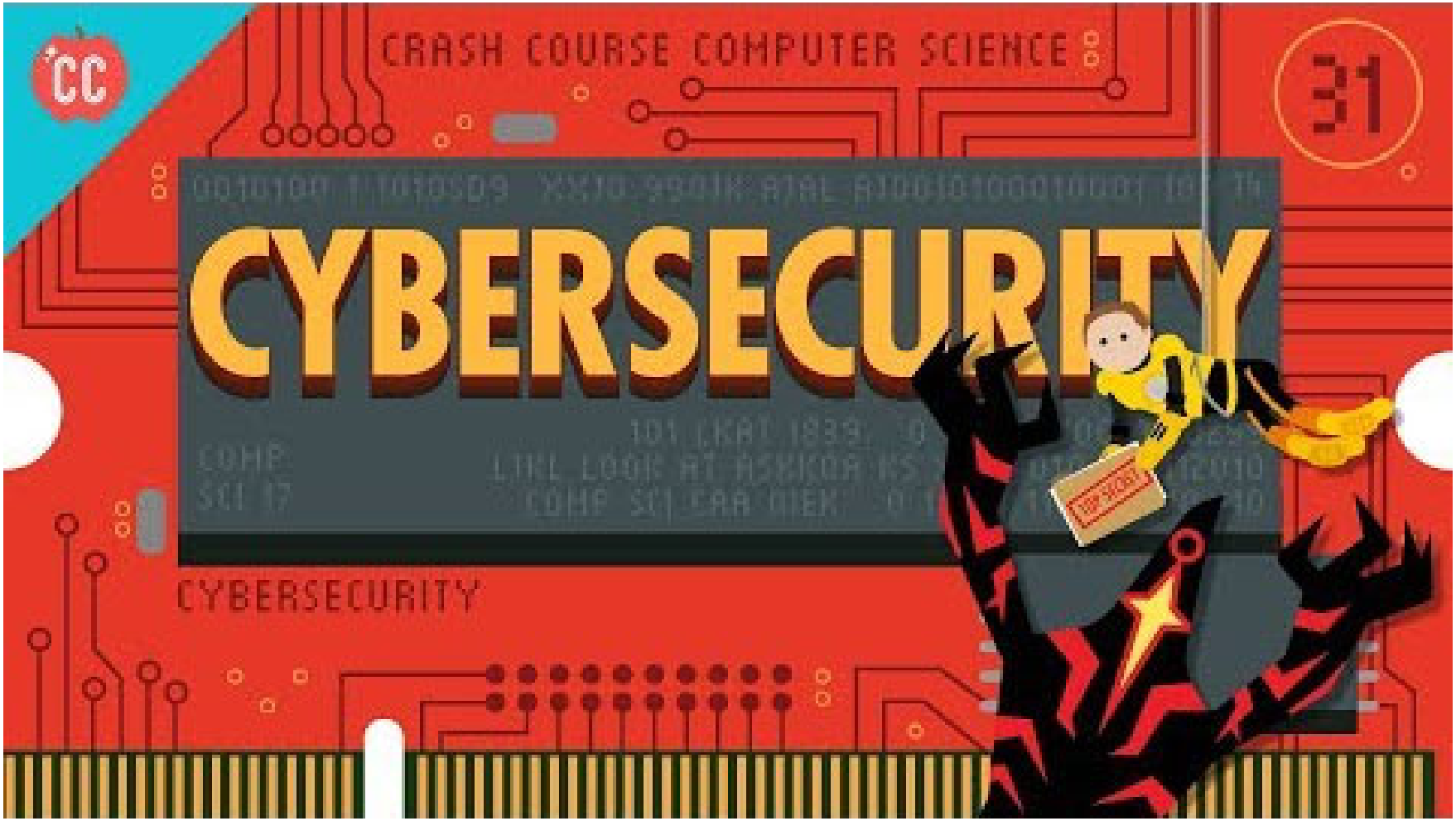
Securing Telemedicine Communications

Michael Holcomb, BS
Associate Director, Information Technology



https://www.youtube.com/watch?v=bPVaOlJ6ln0

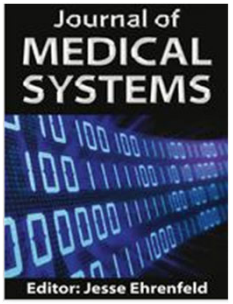
Protected Health Information

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.



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

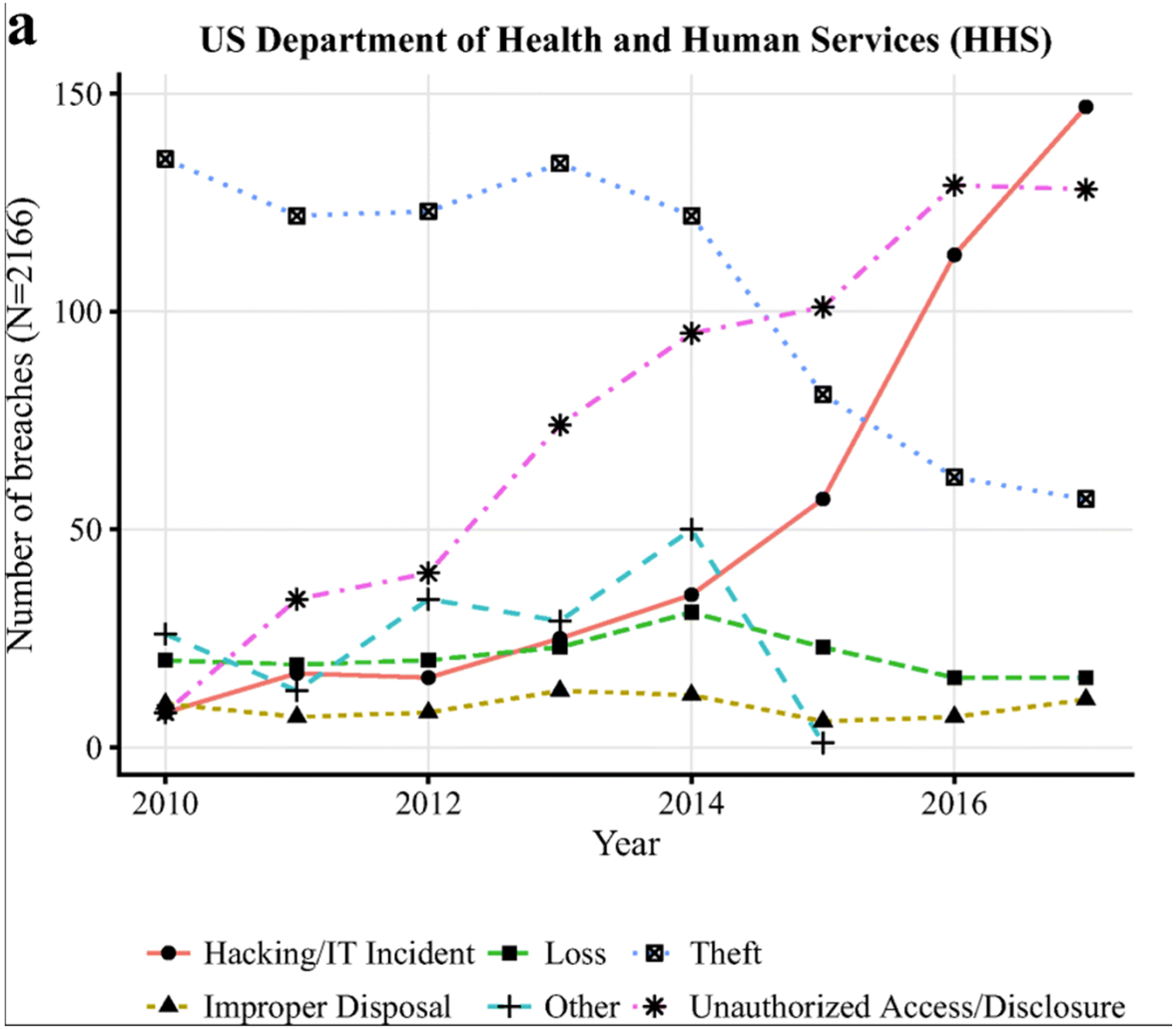
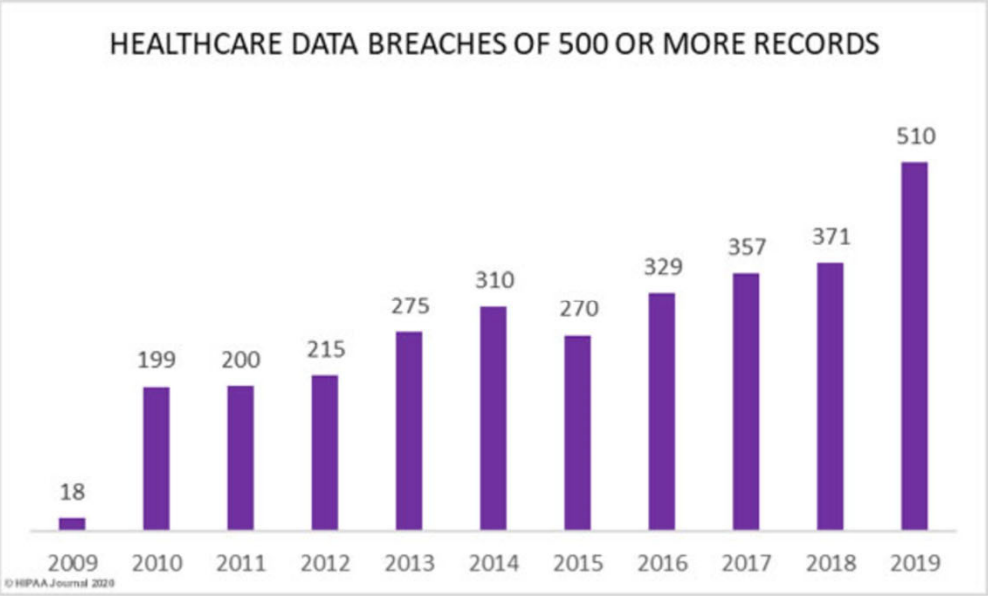
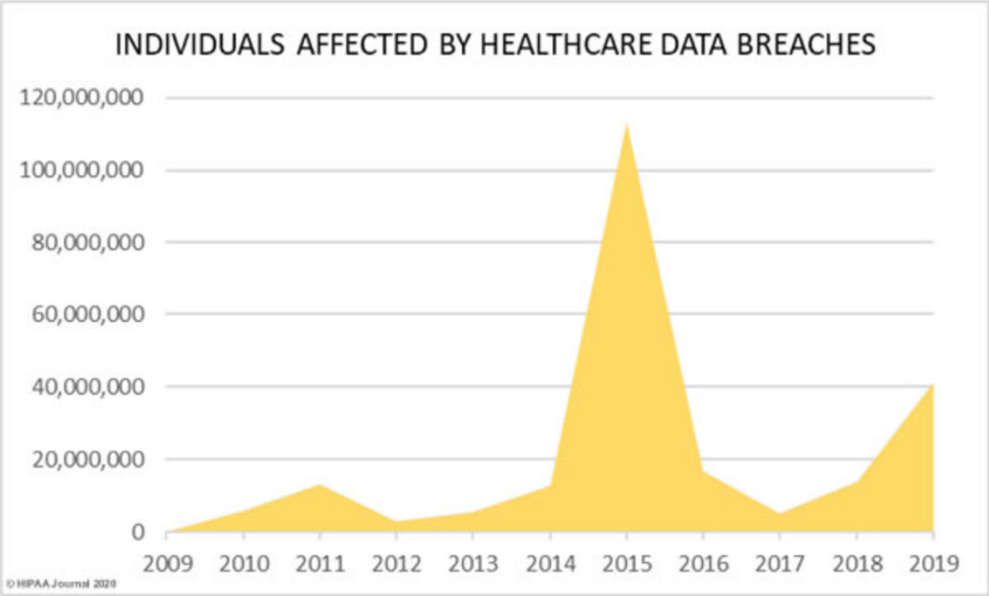


Figure 1 part a
Breakdown of healthcare breach types by year based on data provided by the US Department of Health and Human Services (HHS) including archived breaches and breaches under investigation
(2010- Apr 2018)

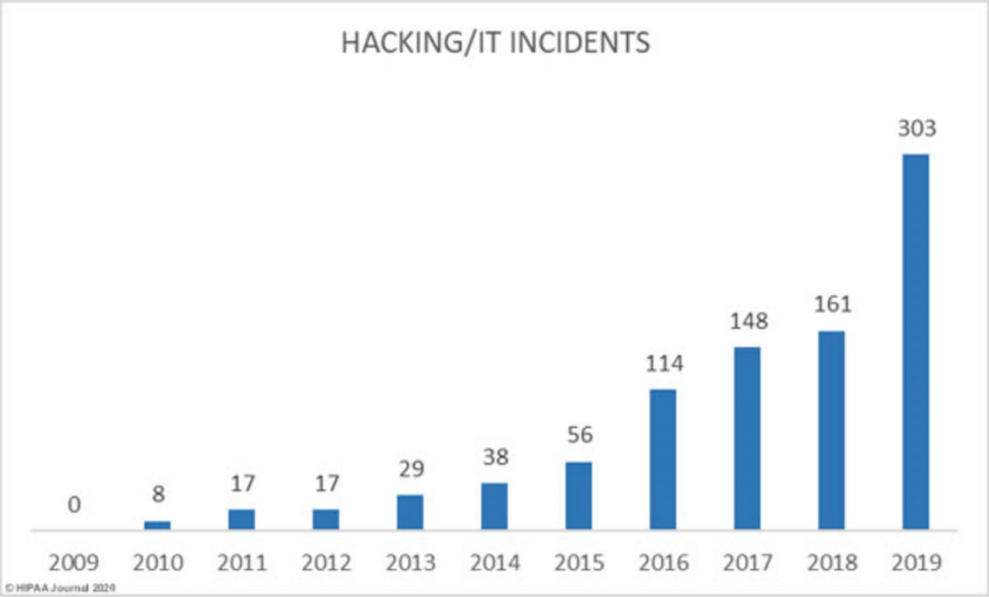
Healthcare Data Breach Statistics





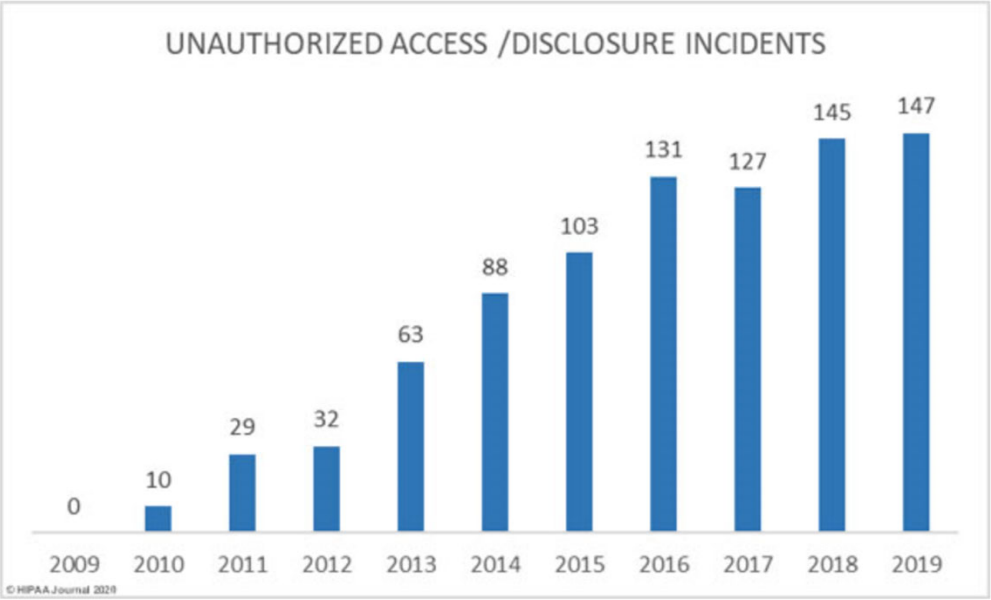
https://www.hipaajournal.com/healthcare-data-breach-statistics/

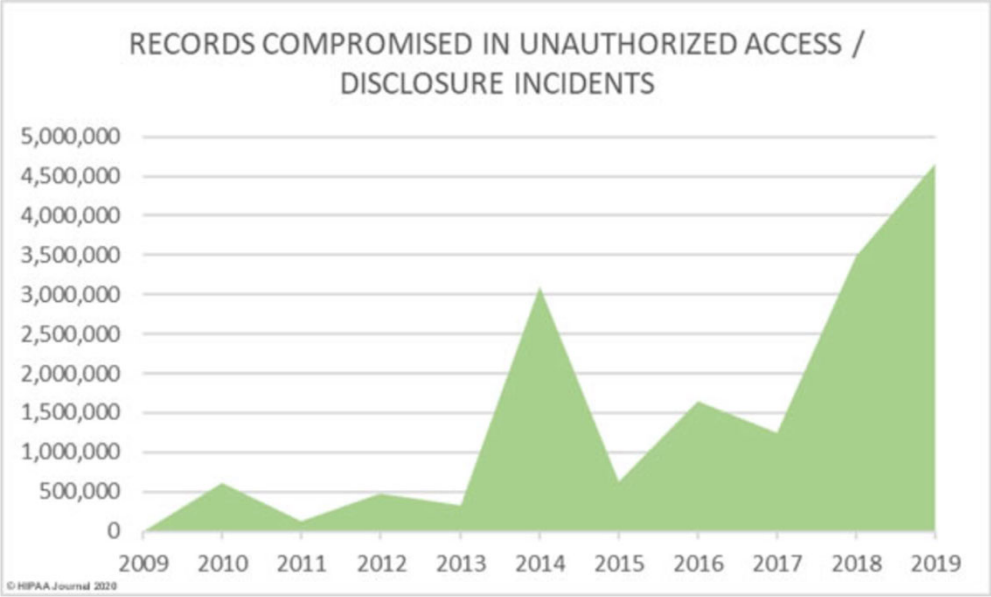
Healthcare Data Breach Statistics



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

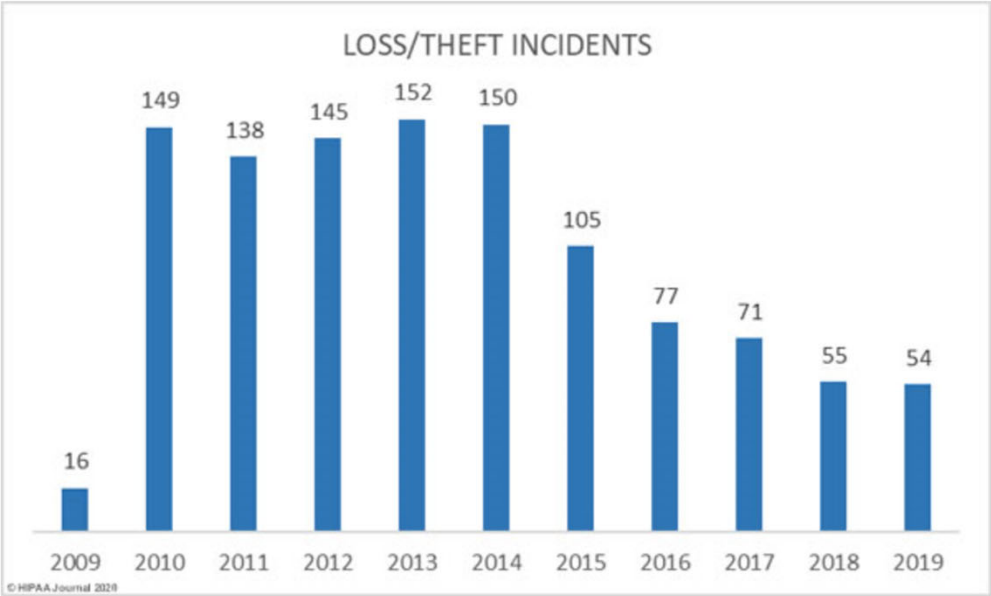
Healthcare Data Breach Statistics

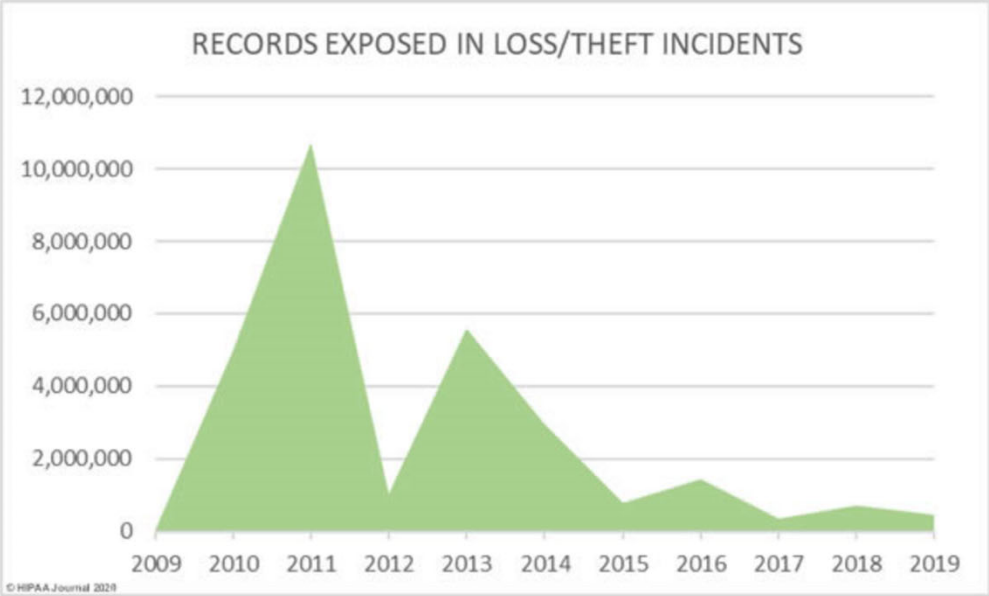




https://www.hipaajournal.com/healthcare-data-breach-statistics/

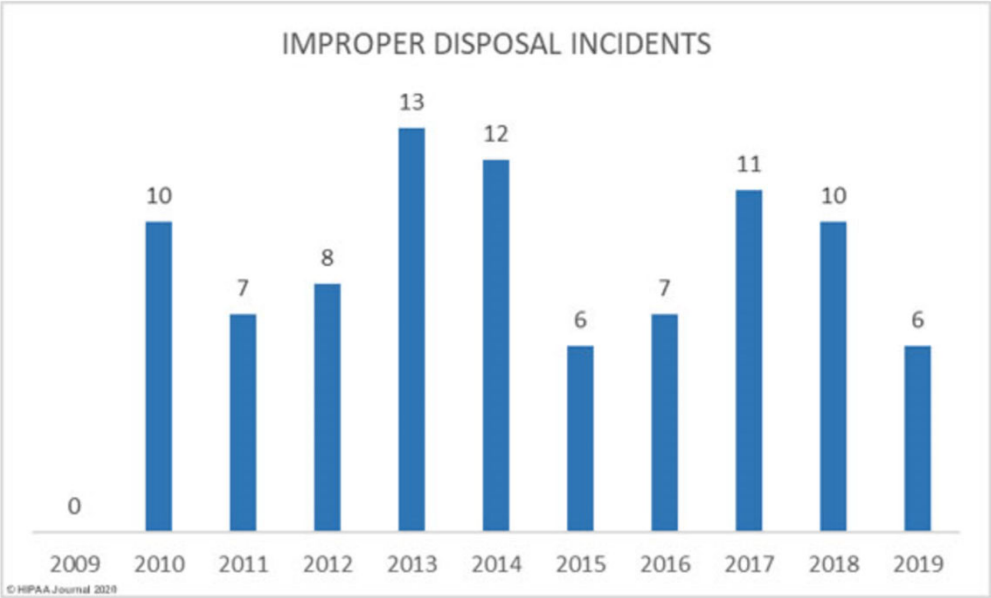
Healthcare Data Breach Statistics

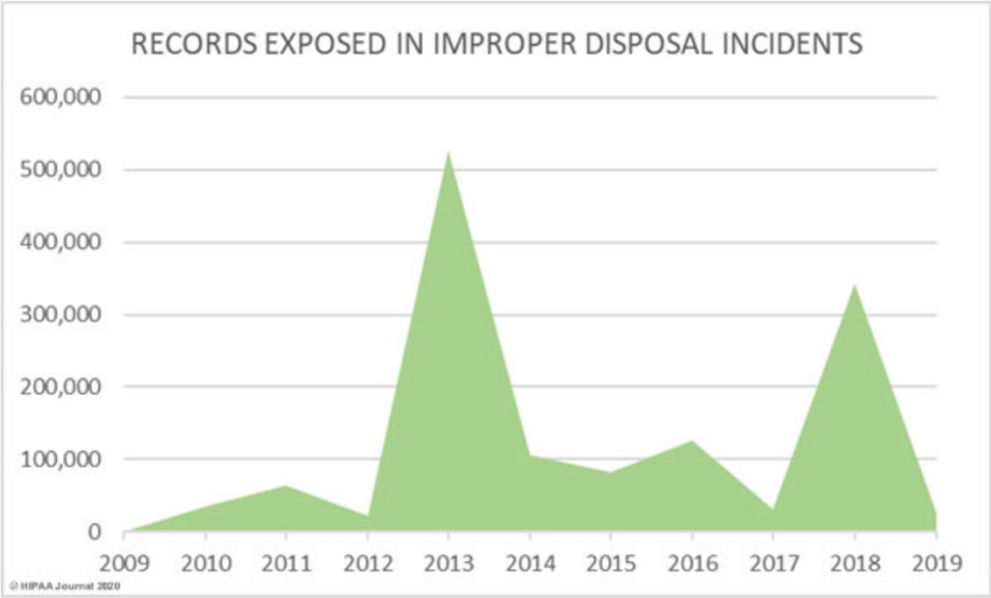




https://www.hipaajournal.com/healthcare-data-breach-statistics/

Healthcare Data Breach Statistics





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

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

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

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://youtu.be/BSsIBuUAVU4

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/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...

PBS NEWS HOUR

Menu

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

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

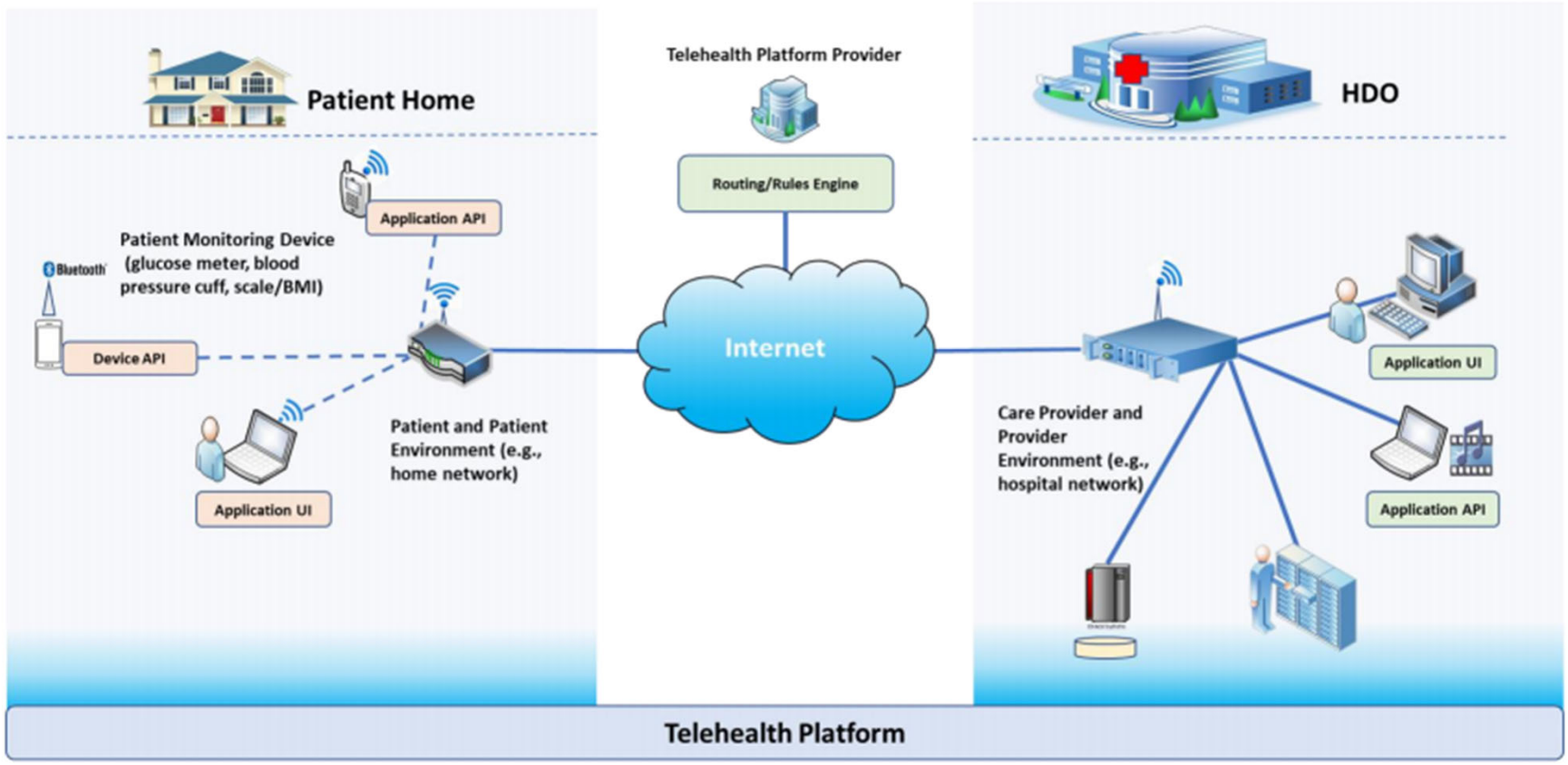
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

(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

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

Additional Information Security Resource for Healthcare Providers

- 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

The Office of the National Coordinator for Health Information Technology
HEALTH IT PLAYBOOK

Search

Section 7
Privacy & Security

In this section

Learn how to:

- Safeguard **personal health information**
- Incorporate **privacy and security** into your EHR
- **Perform a risk assessment** of your practice

Take Steps to Protect and Secure Information When Using a Mobile Device

Overview
Tips for protecting and securing patient health information on mobile devices

Who it's for
Clinicians and support staff who use mobile devices to send, receive, transmit, or store patient health information

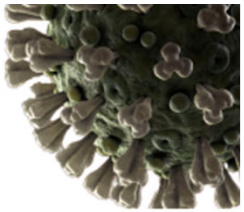
When it's used
To educate staff on privacy and security awareness, to plan an EHR implementation involving mobile technology, or to implement major system upgrades

Download Take Steps to Protect and Secure Information When Using a Mobile Device [PDF – 350 KB]

How do I protect the confidentiality, integrity, and availability of personal health information?

AMA AMERICAN MEDICAL ASSOCIATION

American Hospital Association™ Advancing Health in America



WHAT PHYSICIANS NEED TO KNOW

Working from home during COVID-19 pandemic

During the COVID-19 pandemic, many physicians are working from home, using their personal computers and mobile devices to help care for patients. Fortunately, technology can allow physicians and care teams to do much of what they could do at the medical office, remotely. Telemedicine is a powerful tool that spans a continuum of technologies and offers new ways to deliver care. Many electronic health record (EHR) systems allow you to connect over the Internet just as if you were in the clinic. While you are doing your part to help during the COVID-19 pandemic, the American Medical Association (AMA) and American Hospital Association (AHA) want to ensure you have resources to help keep your work environment safe from cyber-threats that could disrupt your practice, the hospital, or negatively impact your patients' safety and well-being.

Your Home Personal Computer (PC)

Your home computer, whether it be a Windows or Mac, laptop or desktop, is susceptible to cyber threats. It is important to take steps to keep your home office as resilient as your medical practice. We are learning of increased security threats to medical data due to the pandemic. Many cyber criminals are taking advantage of clinician interest in COVID-19 to infect practices', and hospitals' computers and networks with the hope of stealing or holding medical records for ransom.

To help protect you and your patients, the AMA has compiled a Checklist for Computers, which is a non-exhaustive list of **actions you should take immediately** to strengthen your home computer and network.

- Watch out for these common threats:
  - **E-mail phishing** is an attempt to trick you into giving out information using e-mail. E-mail cybersecurity should remain a top priority for clinicians and hospitals as a vast majority of cyber-attacks are initiated by clicking on a phishing e-mail containing malware (malicious software) or a malicious link appearing to be COVID-19 related from a legitimate organization. Additional information on e-mail phishing can be found at this resource on pages 16-17. The FBI has also issued several Public Service Announcements on business email frauds and CORVID-19 themed frauds and they can be found here.
  - **Ransomware** is a type of malware (malicious software) that attempts to deny access to data, usually by encrypting the data with a key known only to the hacker who deployed the malware until a ransom is paid. Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. The FBI discourages paying the ransom as it may incentivize continued ransomware attacks and fund more serious crimes including violent crimes. Most ransomware

https://www.ama-assn.org/system/files/2020-04/cybersecurity-work-from-home-covid-19.pdf

Thank you!

Questions?

mholcomb@telemedicine.arizona.edu