ARIZONA TELEMEDICINE PROGRAM

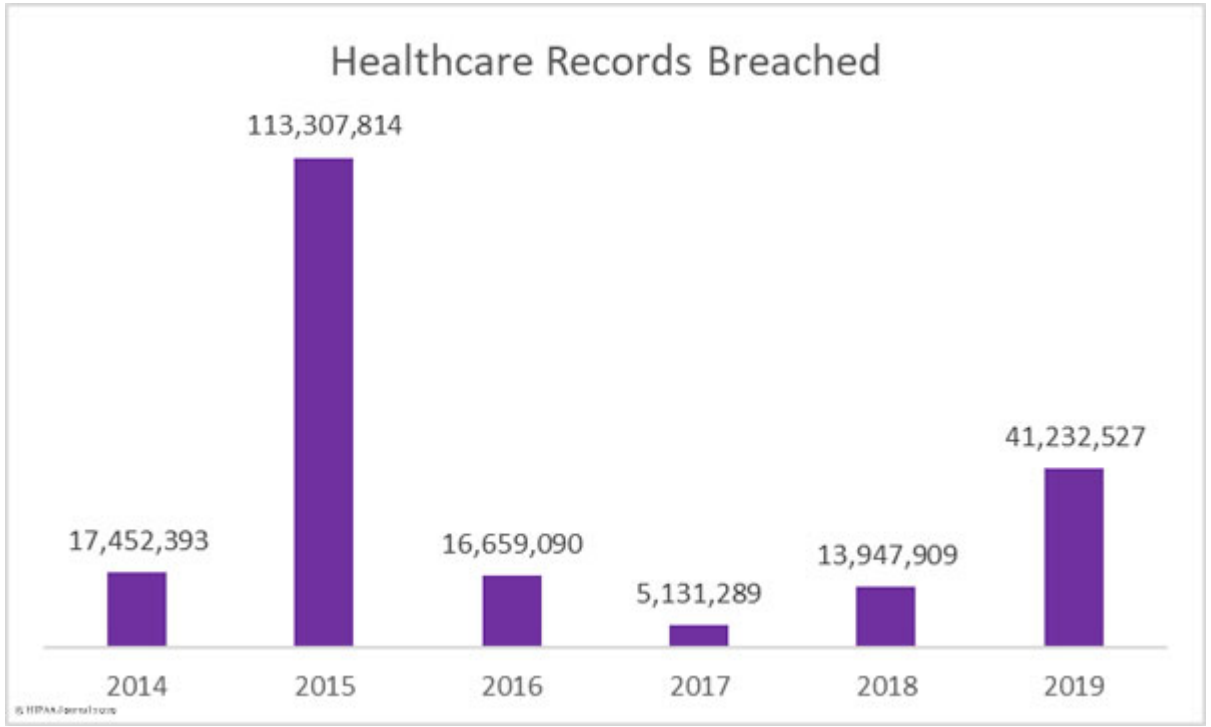
SOUTHWEST TRC TELEHEALTH RESOURCE · CENTER™

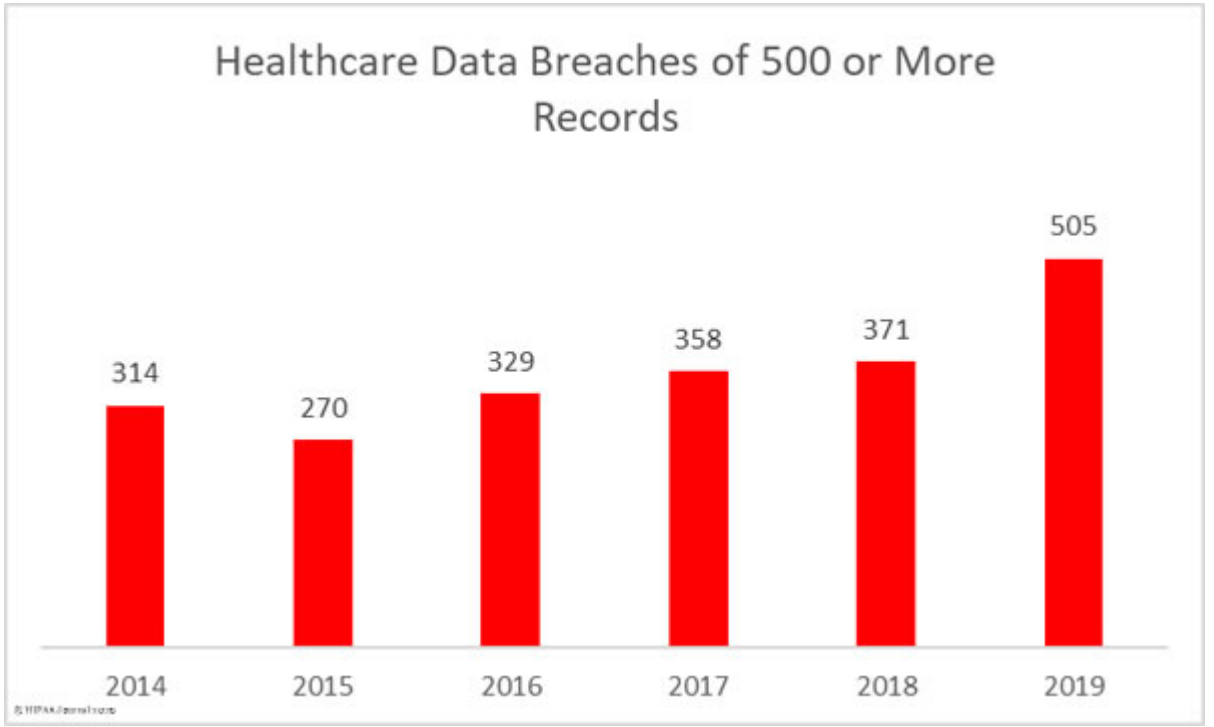
Securing Telemedicine Communications

Michael Holcomb, BS
Associate Director, Information Technology

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

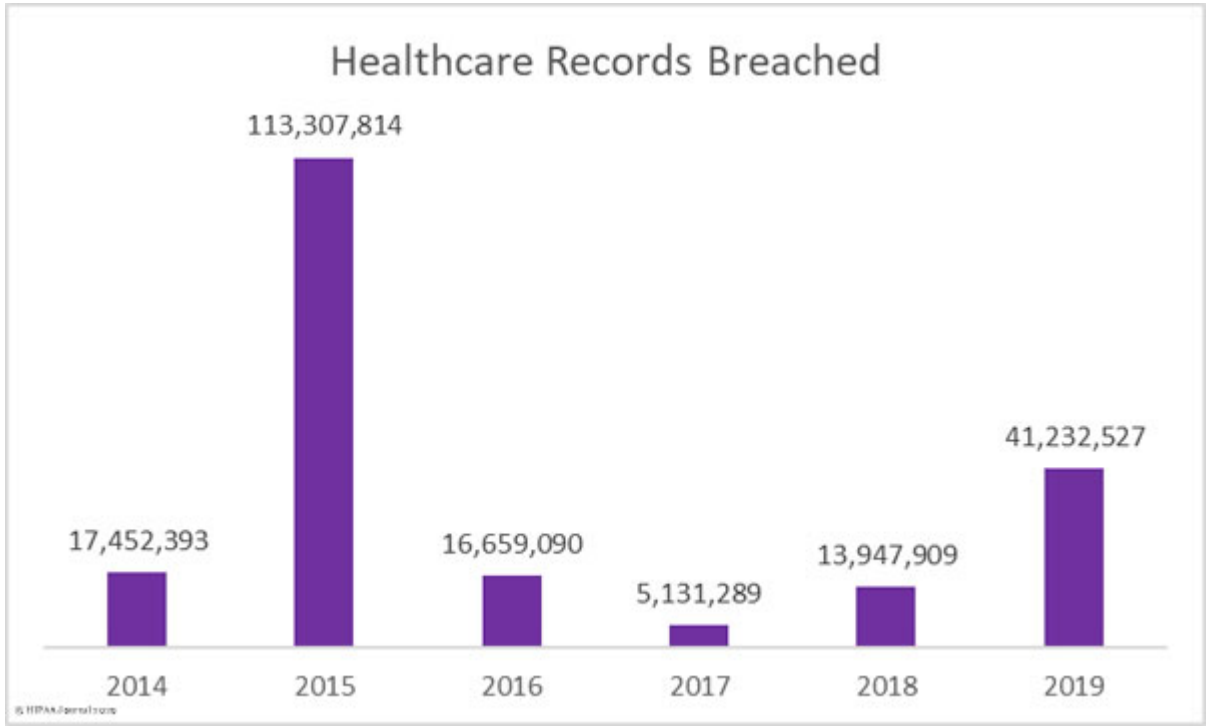
December 2019 Healthcare Data Breach Report

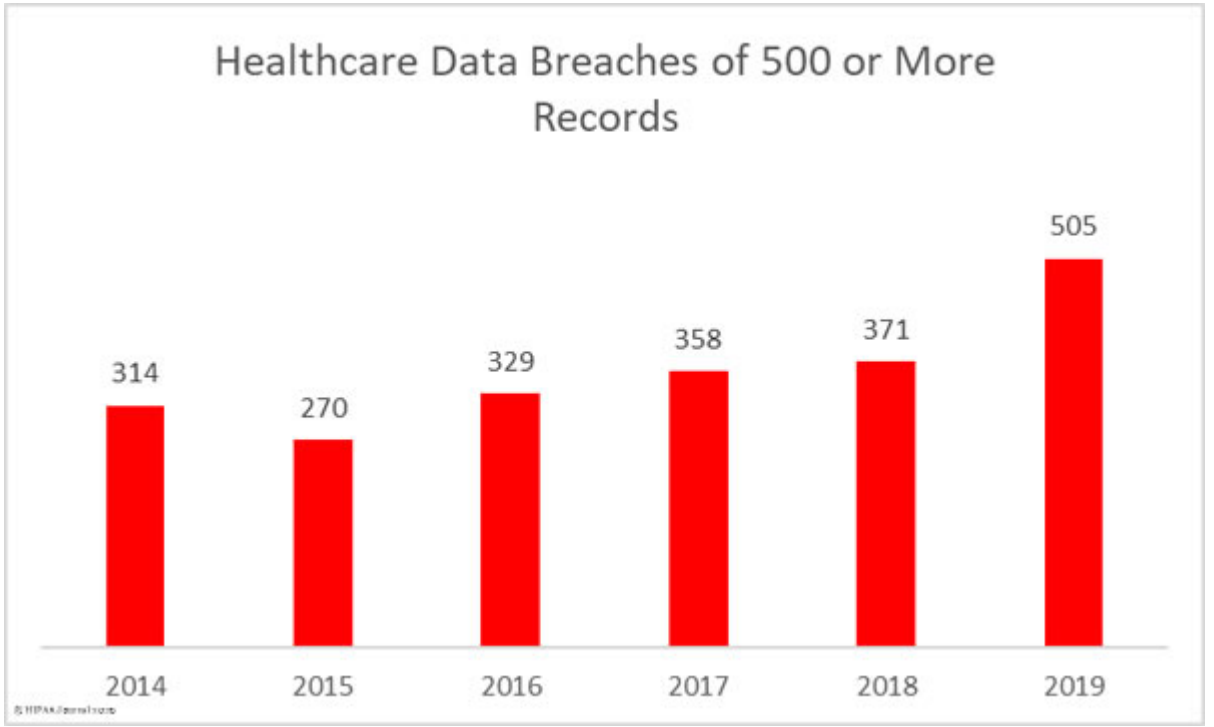




https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/

December 2019 Healthcare Data Breach Report





https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/

Becker's Healthcare: Hospital

BECKER'S
HEALTH IT & CIO REPORT

10 largest data breaches of 2019

Mackenzie Garrity - Tuesday, December 3rd, 2019 Print | Email

SHARE Tweet Share 6

Numerous privacy incidents at hospitals, IT suppliers and other healthcare organizations captured public attention throughout 2019.

While some security incidents only affected only a few hundred patients, others were said to have affected millions.

Here are the 10 largest healthcare privacy incidents reported by *Becker's Hospital Review* thus far in 2019:

Editor's note: Incidents are presented in order of the number of patients or organizations affected.

1. Quest Diagnostics notified 11.9 million patients of a data breach that happened at one of its billing collections vendors.

2. Medical testing company Laboratory Corp. of America learned 7.7 million of its patients may have had their data exposed in the same vendor breach as Quest Diagnostics.

3. Lab testing company Clinical Pathology Laboratories began notifying 2.2 million patients July 5 that their personal health information may have been exposed in a vendor data breach.

4. Inmediata Health Group, a healthcare clearinghouse company, notified its customers of a data breach that may have exposed the personal information of more than 1.5 million people.

5. Nine employees within Oregon's Department of Human Services opened a phishing email on Jan. 8 that may have exposed around 645,000 people.

6. Tampa-based Women's Care Florida alerted all current and former patients — 528,188 people — that their medical or personal information may have been exposed due to an April 29 cybersecurity incident.

7. The Oregon Department of Human Services reported an email phishing attack on 2 million agency emails that may have exposed the medical information of more than 350,000 people.

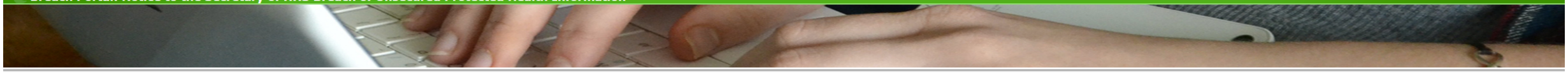
8. A cyberattack last July on Macon, Ga.-based Navicent Health's employee email account system may have affected 278,016 patients' personal information.

9. Medical device and software developer Zoll notified 277,319 patients in March of a security incident that put their personal and medical information at risk from Nov. 8 to Dec. 28, 2018.

10. Health Alliance Plan and Blue Cross Blue Shield of Michigan alerted nearly 270,000 members combined in March that their personal information may have been compromised after a data breach at the payers' mailing service vendor in September 2018.

https://www.beckershospitalreview.com/cybersecurity/10-largest-data-breaches-of-2019.html

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



Under Investigation | Archive | Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

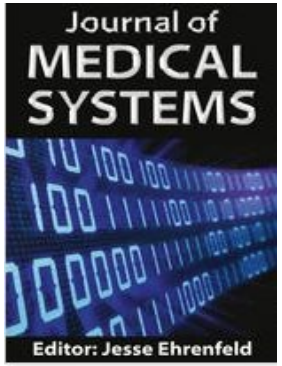
Cases Currently Under Investigation

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
	Children's Hope Alliance	NC	Healthcare Provider	4564	01/14/2020	Hacking/IT Incident	Email
	Spectrum Healthcare Partners	ME	Healthcare Provider	11308	01/10/2020	Hacking/IT Incident	Email
	InterMed, PA	ME	Healthcare Provider	33000	01/08/2020	Hacking/IT Incident	Email
	CAH Holdings, Inc.	AL	Business Associate	1158	01/06/2020	Hacking/IT Incident	Email
	RCM Enterprise Services, Inc.	FL	Business Associate	5965	01/06/2020	Unauthorized Access/Disclosure	Paper/Films
	Native American Rehabilitation Association of the Northwest, Inc.	OR	Healthcare Provider	25187	01/03/2020	Hacking/IT Incident	Email
	Douglas County Hospital dba Alomere Health	MN	Healthcare Provider	49351	01/03/2020	Hacking/IT Incident	Email
	SEES Group, LLC	TN	Healthcare Provider	13000	12/31/2019	Hacking/IT Incident	Email
	The Center for Facial Restoration, Inc.	FL	Healthcare Provider	3600	12/26/2019	Hacking/IT Incident	Network Server
	Ann & Robert H. Lurie Children's Hospital of Chicago	IL	Healthcare Provider	4195	12/26/2019	Unauthorized Access/Disclosure	Electronic Medical Record
	btyDENTAL	AK	Healthcare Provider	2008	12/26/2019	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Email, Network Server
	Baylor Miraca Genetics Laboratories, LLC d/b/a Baylor Genetics	TX	Business Associate	1240	12/24/2019	Unauthorized Access/Disclosure	Email
	PediHEalth, PLLC, dba Children's Choice Pediatrics	TX	Healthcare Provider	12689	12/20/2019	Hacking/IT Incident	Network Server
	Roosevelt General Hospital	NM	Healthcare Provider	28847	12/19/2019	Hacking/IT Incident	Network Server
	Texas Family Psychology Associates, P.C.	TX	Healthcare Provider	12000	12/17/2019	Unauthorized Access/Disclosure	Electronic Medical Record
	San Francisco Department of Public Health - Zuckerberg SF General Hospital	CA	Healthcare Provider	1174	12/16/2019	Improper Disposal	Paper/Films
	Aflac	GA	Health Plan	1601	12/16/2019	Unauthorized Access/Disclosure	Network Server
	Texas Children's Hospital	TX	Healthcare Provider	597	12/16/2019	Unauthorized Access/Disclosure	Paper/Films
	North Ottawa Community Health System	MI	Healthcare Provider	4013	12/16/2019	Unauthorized Access/Disclosure	Electronic Medical Record
	INTEGRIS Health, Inc.	OK	Healthcare Provider	500	12/16/2019	Loss	Other Portable Electronic Device
	Colorado Department of Human Services	CO	Healthcare Provider	12230	12/16/2019	Hacking/IT Incident	Other
	Vimly Benefit Solutions, Inc.	WA	Business Associate	2675	12/13/2019	Hacking/IT Incident	Email
	Sinai Health System	IL	Healthcare Provider	12578	12/13/2019	Hacking/IT Incident	Email
	Prestige Health Choice	FL	Health Plan	4662	12/13/2019	Unauthorized Access/Disclosure	Other Portable Electronic Device
	Therapeutic Oasis of the Palm Beaches LLC	FL	Healthcare Provider	1100	12/13/2019	Theft	Desktop Computer
	Marion Eye Center, LTD.	IL	Healthcare Provider	811	12/13/2019	Loss	Paper/Films
	Aetna affiliated covered entity (ACE)	CT	Health Plan	5991	12/13/2019	Hacking/IT Incident	Email
	Service Benefit Plan Administrative Services Corporation	DC	Business Associate	11536	12/12/2019	Unauthorized Access/Disclosure	Network Server
	Jewish Social Service Agency	MD	Healthcare Provider	3145	12/12/2019	Hacking/IT Incident	Email



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

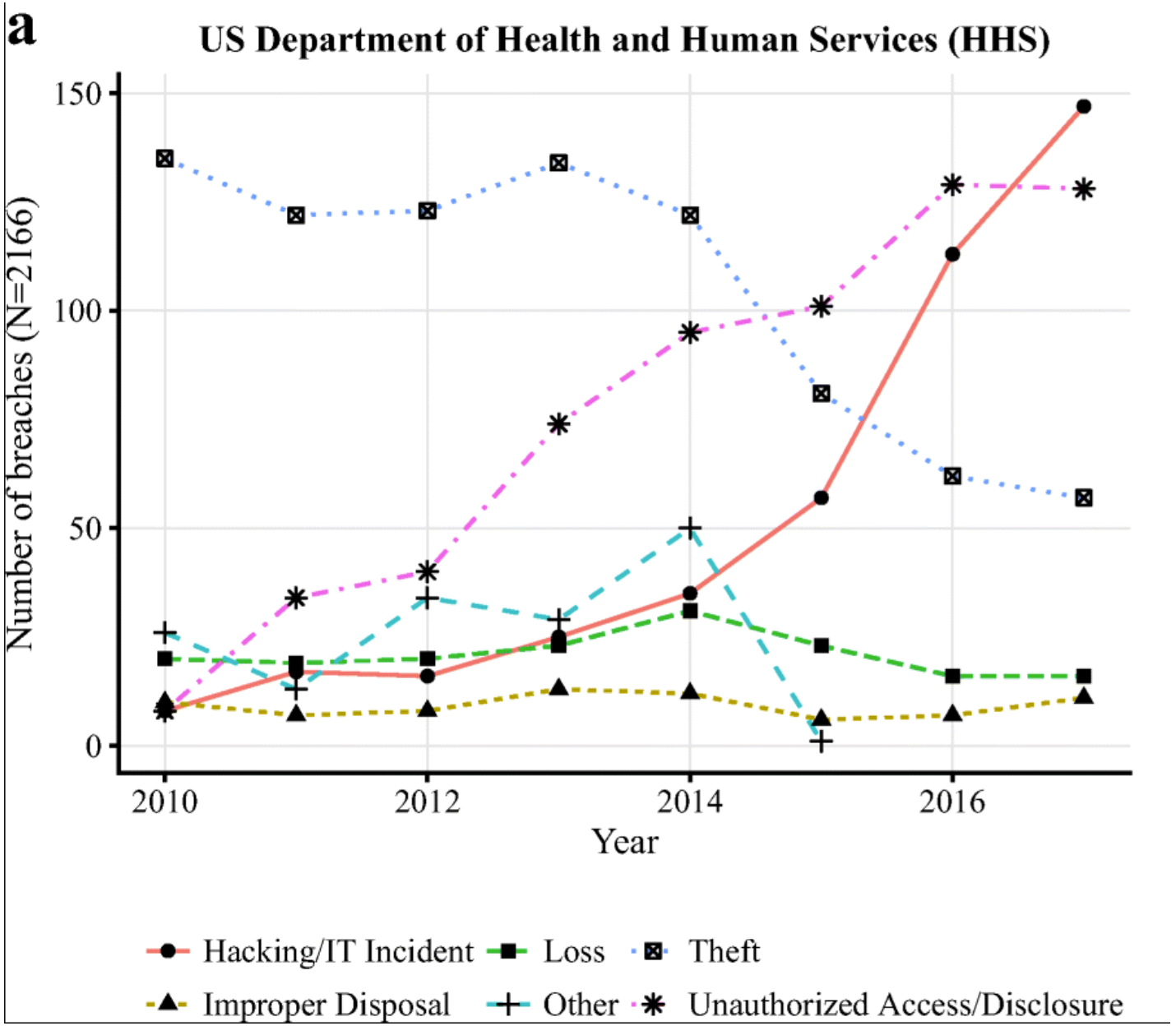


Figure 1 part a
Breakdown of healthcare breach types by year based on data provided by the US Department of Health and Human Services (HHS) including archived breaches and breaches under investigation
(2010- Apr 2018)

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

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

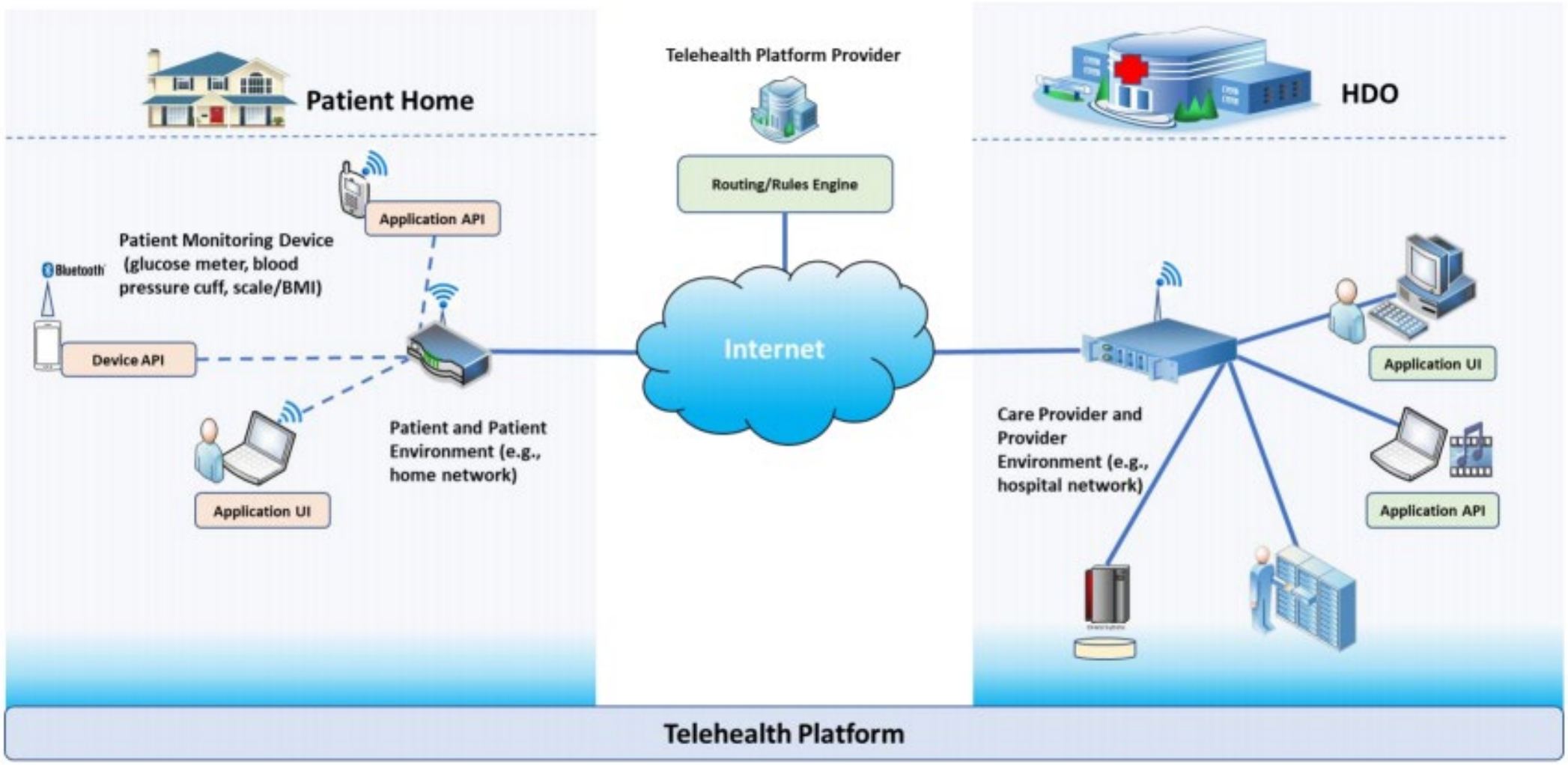
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group, aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes. The publication includes a main document, two technical volumes, and resources and templates:

- **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP):** The HICP examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats and presents (10) practices to mitigate those threats.

Cybersecurity Act of 2015, Section 405(d)

- Health Industry Cybersecurity Practices
- About the CSA 405(d) Task Group
- Cybersecurity Reports and Tools
- Get Involved

https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

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

Executive Summary

Call to Action: Cybersecurity a Priority for Patient Safety

Cybersecurity threats to health care organizations and patient safety are real. Health information technology, which provides critical life-saving functions, consists of connected, networked systems and leverages wireless technologies, leaving such systems more vulnerable to cyber-attack. Recent highly publicized ransomware attacks on hospitals, for example, necessitated diverting patients to other hospitals and led to an inability to access patient records to continue care delivery. Such cyber-attacks expose sensitive patient information and lead to substantial financial costs to regain control of hospital systems and patient data. From small, independent practitioners to large, university hospital environments, cyber-attacks on health care records, IT systems, and medical devices have infected even the most hardened systems.

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

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

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.

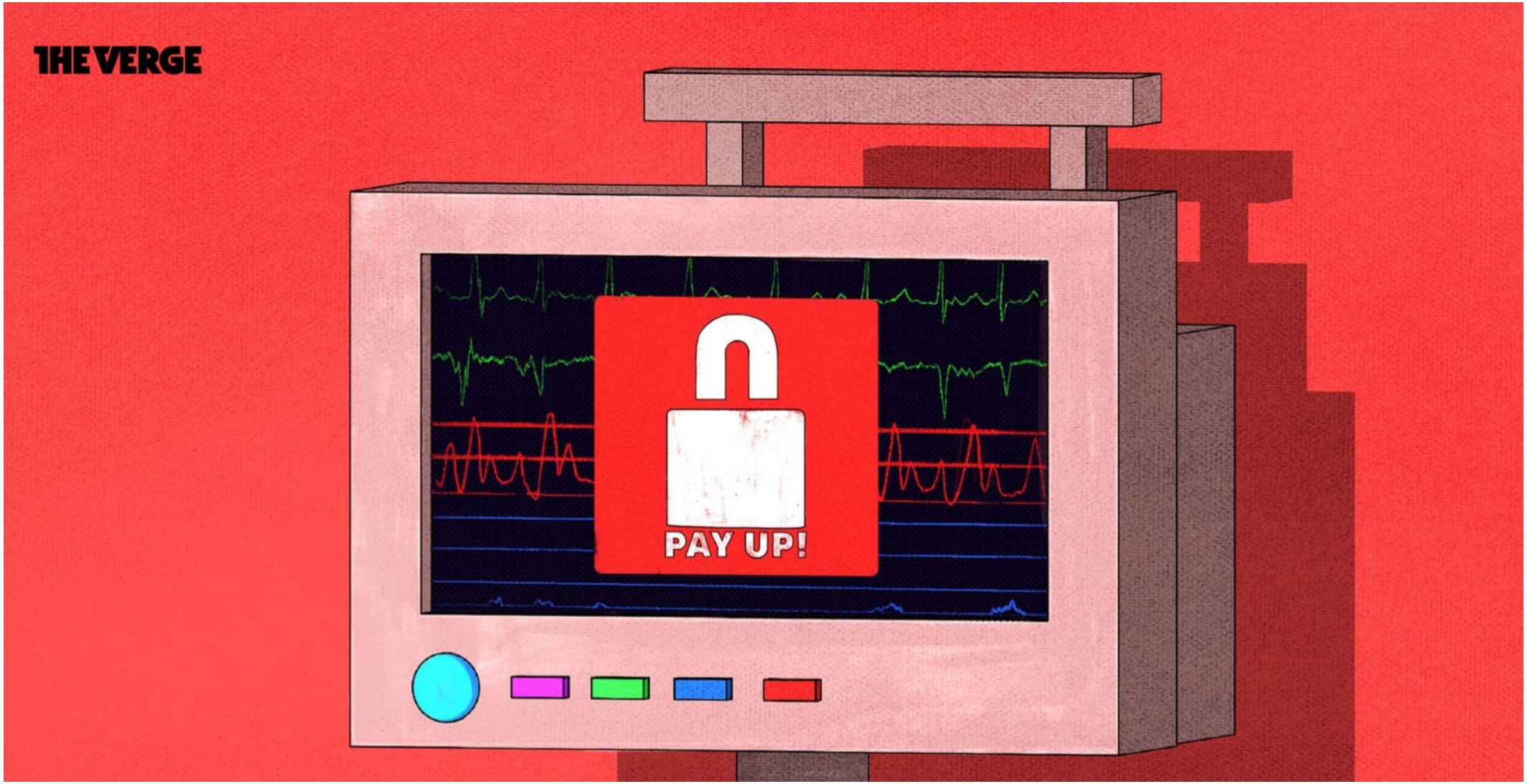
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Suggested Cybersecurity Webinar

- **NCTRC Webinar – An Overview of Cybersecurity – July 18, 2019**
  - Archive available on demand
    - https://www.telehealthresourcecenter.org/event/nctrc-webinar-an-overview-of-cybersecurity/
- **Presented by:** Jordan Berg, National Telehealth Technology Assessment Center
- **Description:** Cybersecurity is a major concern for health care and telehealth programs. This presentation will discuss the importance of Cybersecurity in Healthcare and present resources available to individuals and organizations wanting to become better versed in best practices and common threats. Core references for this presentation are the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Health Industry Cybersecurity Practices (HICP) cybersecurity report. The goal of this presentation is to provide learners with tools to be able to research, discuss, and communicate important cybersecurity ideas.

https://youtu.be/BSsIBuUAVU4



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

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

Economics > General Economics

Do Hospital Data Breaches Reduce Patient Care Quality?

Sung J. Choi, M. Eric Johnson

(Submitted on 3 Apr 2019)

Objective: To estimate the relationship between a hospital data breach and hospital quality outcome
Materials and Methods: Hospital data breaches reported to the U.S. Department of Health and Human Services breach portal and the Privacy Rights Clearinghouse database were merged with the Medicare Hospital Compare data to assemble a panel of non-federal acutecare inpatient hospitals for years 2011 to 2015. The study panel included 2,619 hospitals. Changes in 30-day AMI mortality rate following a hospital data breach were estimated using a multivariate regression model based on a difference-in-differences approach.
Results: A data breach was associated with a 0.338[95% CI, 0.101-0.576] percentage point increase in the 30-day AMI mortality rate in the year following the breach and a 0.446[95% CI, 0.164-0.729] percentage point increase two years after the breach. For comparison, the median 30-day AMI mortality rate has been decreasing about 0.4 percentage points annually since 2011 due to progress in care. The magnitude of the breach impact on hospitals' AMI mortality rates was comparable to a year's worth historical progress in reducing AMI mortality rates.
Conclusion: Hospital data breaches significantly increased the 30-day mortality rate for AMI. Data breaches may disrupt the processes of care that rely on health information technology. Financial costs to repair a breach may also divert resources away from patient care. Thus breached hospitals should carefully focus investments in security procedures, processes, and health information technology that jointly lead to better data security and improved patient outcomes.

Comments: 32 pages, 6 figures, 4 tables, presented at the Workshop on the Economics of Information Security 2017
Subjects: **General Economics (econ.GN)**; Applications (stat.AP)
Cite as: arXiv:1904.02058 **[econ.GN]**
(or arXiv:1904.02058v1 **[econ.GN]** for this version)

Submission history

From: Sung J. Choi [view email]
[v1] Wed, 3 Apr 2019 15:26:12 UTC (124 KB)

ARIZONA TELEMEDICINE PROGRAM

SOUTHWEST TRC TELEHEALTH RESOURCE · CENTER™

Thank you!

Questions?

mholcomb@telemedicine.arizona.edu

Protected Health Information

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

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

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.