

ARIZONA
TELEMEDICINE
PROGRAM



Securing Telemedicine Communications

Michael Holcomb, BS
Associate Director, Information Technology



<https://www.youtube.com/watch?v=bPVaOIJ6ln0>

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



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.

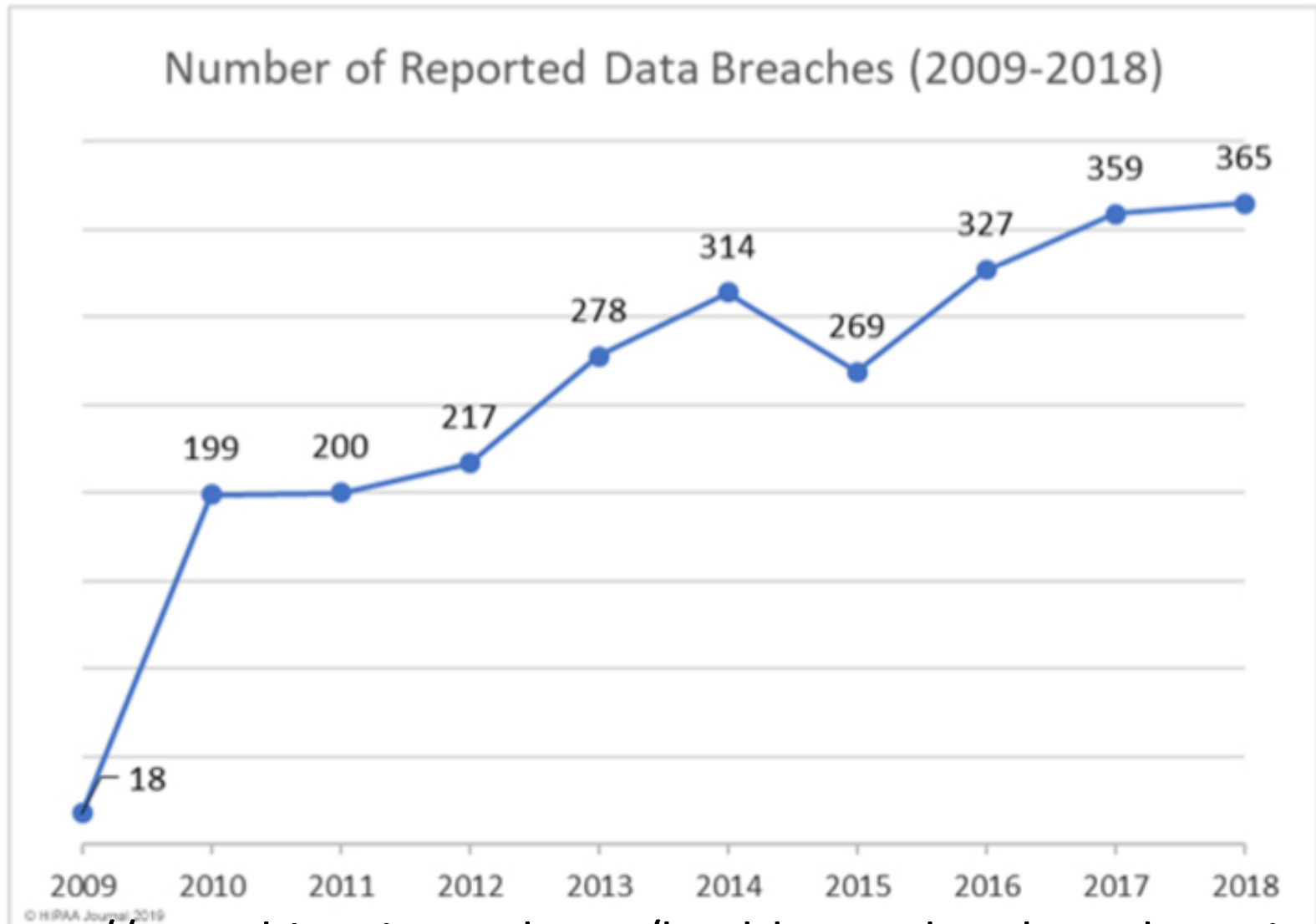
Project Description: Securing Telehealth Remote Patient Monitoring Ecosystem

5

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

Healthcare data breaches are now being reported at a rate of more than one per day.

Healthcare
Data
Breaches
Affecting
500+
Patients



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

LATEST HEALTH DATA BREACHES NEWS

The 10 Biggest Healthcare Data Breaches of 2019, So Far

Hackers have hit the ground running in 2019, with sophisticated cyberattacks impacting millions of individuals; phishing and vendors continue to be a major pain point.

<https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far>

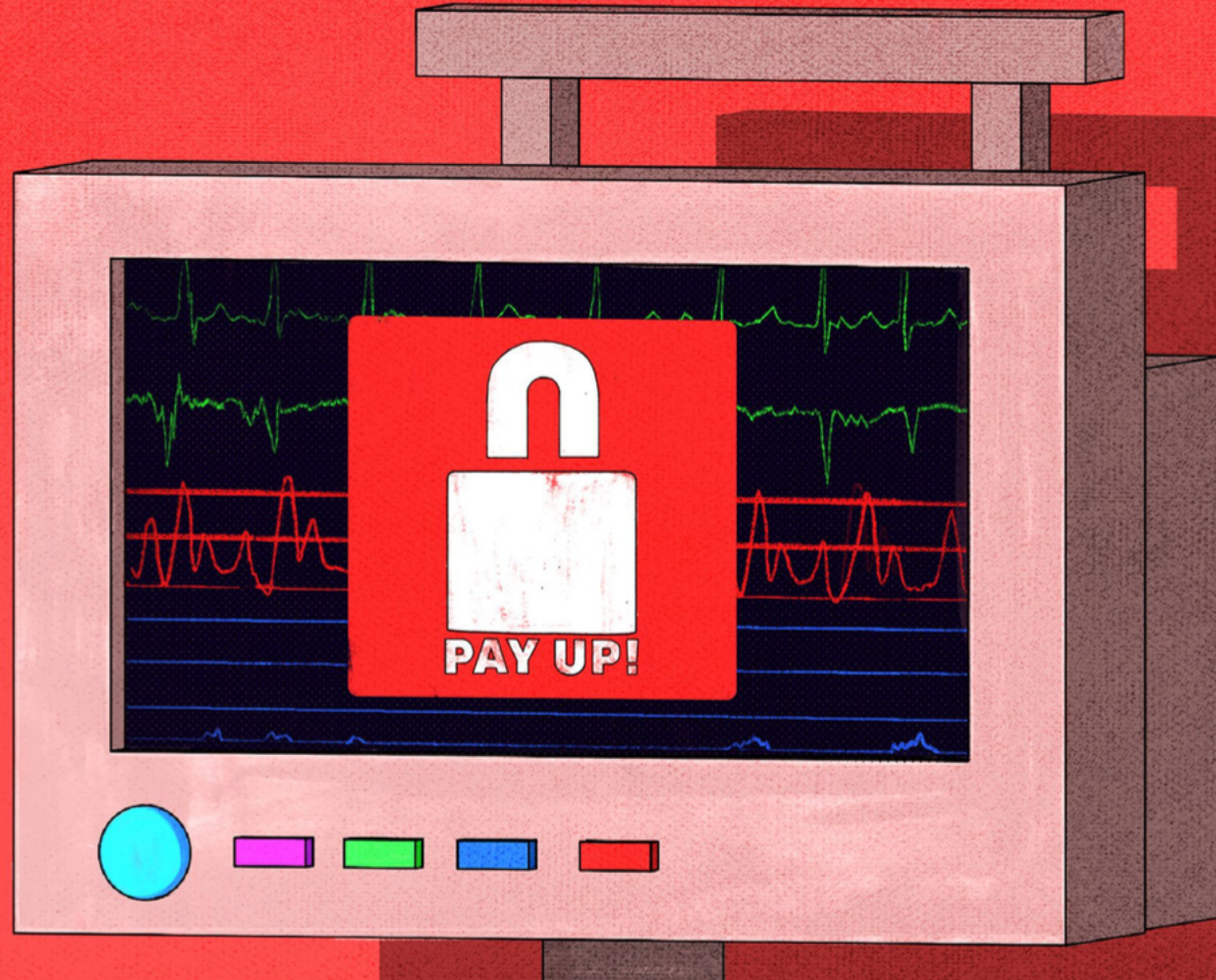
Evaluation of Causes of Protected Health Information Breaches

- 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



<https://youtu.be/BSsIBuUAVU4>

THE VERGE



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

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)

Download:

- [PDF](#)
- [Other formats](#)

(license)

Current browse context:

econ.GN

[< prev](#) | [next >](#)

[new](#) | [recent](#) | [1904](#)

Change to browse by:

[econ](#)

[q-fin](#)

[q-fin.EC](#)

[stat](#)

[stat.AP](#)

References & Citations

- [NASA ADS](#)

[Google Scholar](#)

Bookmark





Public Health Emergency

Public Health and Medical Emergency Support for a Nation Prepared

Search...



PHE Home > Preparedness > Planning > Aligning Health Care Industry Cybersecurity Approaches > Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

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:

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



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.



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.



NIST Cybersecurity Framework



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

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.

ARIZONA
TELEMEDICINE
PROGRAM



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.