HEALTH SECTOR COORDINATING COUNCIL

Joint Cybersecurity Working Group

CYBERSECURITY IN THE HEALTHCARE SECTOR

for the Confidentiality Coalition of the
Healthcare Leadership Council

Briefing
July 15, 2021

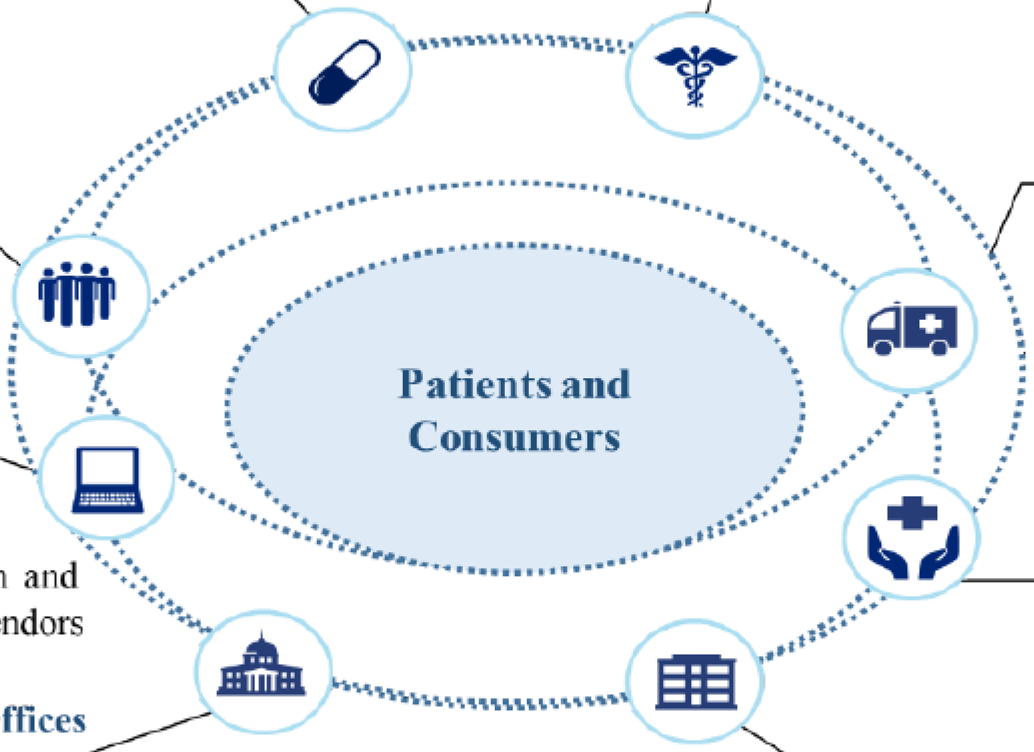
Greg Garcia
Executive Director

Critical Infrastructure

Systems and assets, whether physical or virtual, so vital to the United States that the[ir] incapacitation or destruction …would have a debilitating impact on security, … economic security, … public health or safety, or any combination of those matters.

§1016(e) of the USA Patriot Act of 2001
(42 U.S.C. §5195c(e))

Figure 2 Health Care Ecosystem



Laboratories, Blood & Pharmaceuticals

Pharmaceutical Manufacturers
Drug Store Chains
Pharmacists' Associations
Public and Private Laboratory Associations
Blood Banks

Medical Materials

Medical Equipment & Supply Manufacturing & Distribution
Medical Device Manufacturers

Health Information Technology

Medical Research Institutions
Information Standards Bodies
Electronic Medical Record System and Other Clinical Medical System Vendors

Federal Response & Program Offices

Coordinated Response Activities Under Emergency Support Function 8
Government Coordinating Council
Federal Partners (e.g., HHS, DoD, other sector partners)

Direct Patient Care

Healthcare Systems
Professional Associations
Medical Facilities
Emergency Medical Services
Consumer Devices \ BYOD

Mass Fatality Management Services

Cemetery, Cremation, Morgue, and Funeral Homes
Mass Fatality Support Services (e.g., coroners, medical examiners, forensic examiners, & psychological support personnel)

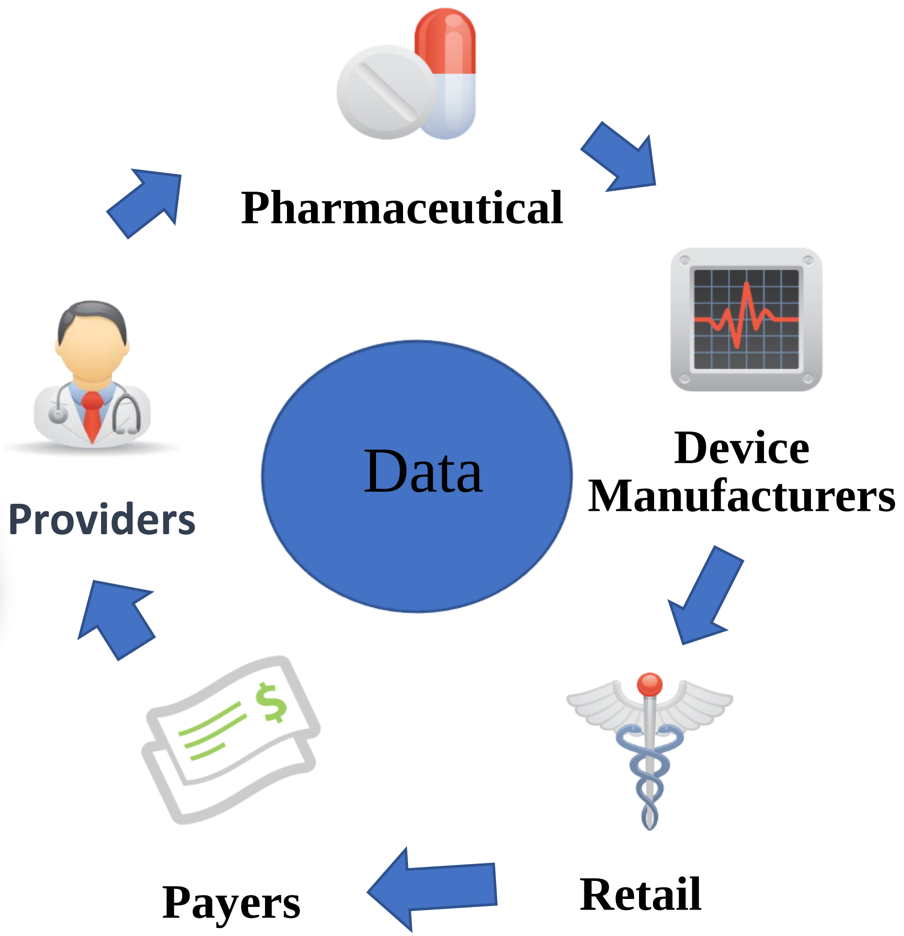
Health Plans and Payers

Health Insurance Companies & Plans
Local and State Health Departments
State Emergency Health Organizations

Public Health

Governmental Public Health Services
Public Health Networks

The Healthcare Ecosystem – Connected, Digitized and Portable



Pharmaceutical

Device Manufacturers

Retail

Payers

Providers

Data

A Snapshot of Healthcare Cyber Attacks in 2020

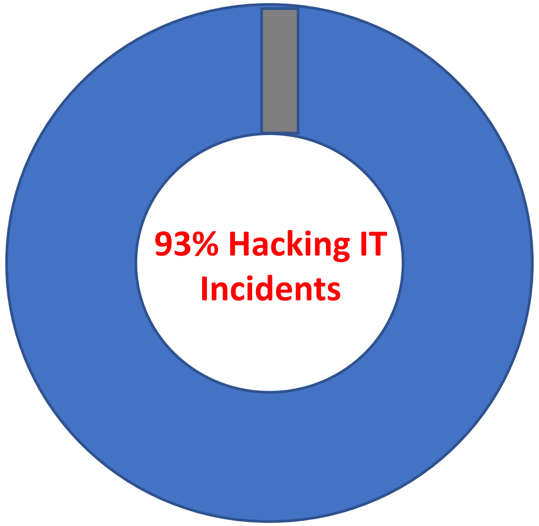
Another banner year for cybercriminals

- 599 HEALTHCARE BREACHES – 55% INCREASE OVER 2019
- HACKING AND IT INCIDENTS CONSTITUTED 93% OF HEALTHCARE BREACHES
- THE AVERAGE COST PER BREACHED RECORD INCREASED FROM $429 IN 2019 TO $500 IN 2020
- THE AVERAGE HEALTHCARE FIRM TOOK ABOUT 236 DAYS TO RECOVER FROM AN ATTACK
- 1M HEALTHCARE RECORDS BREACHED EACH MONTH LAST YEAR

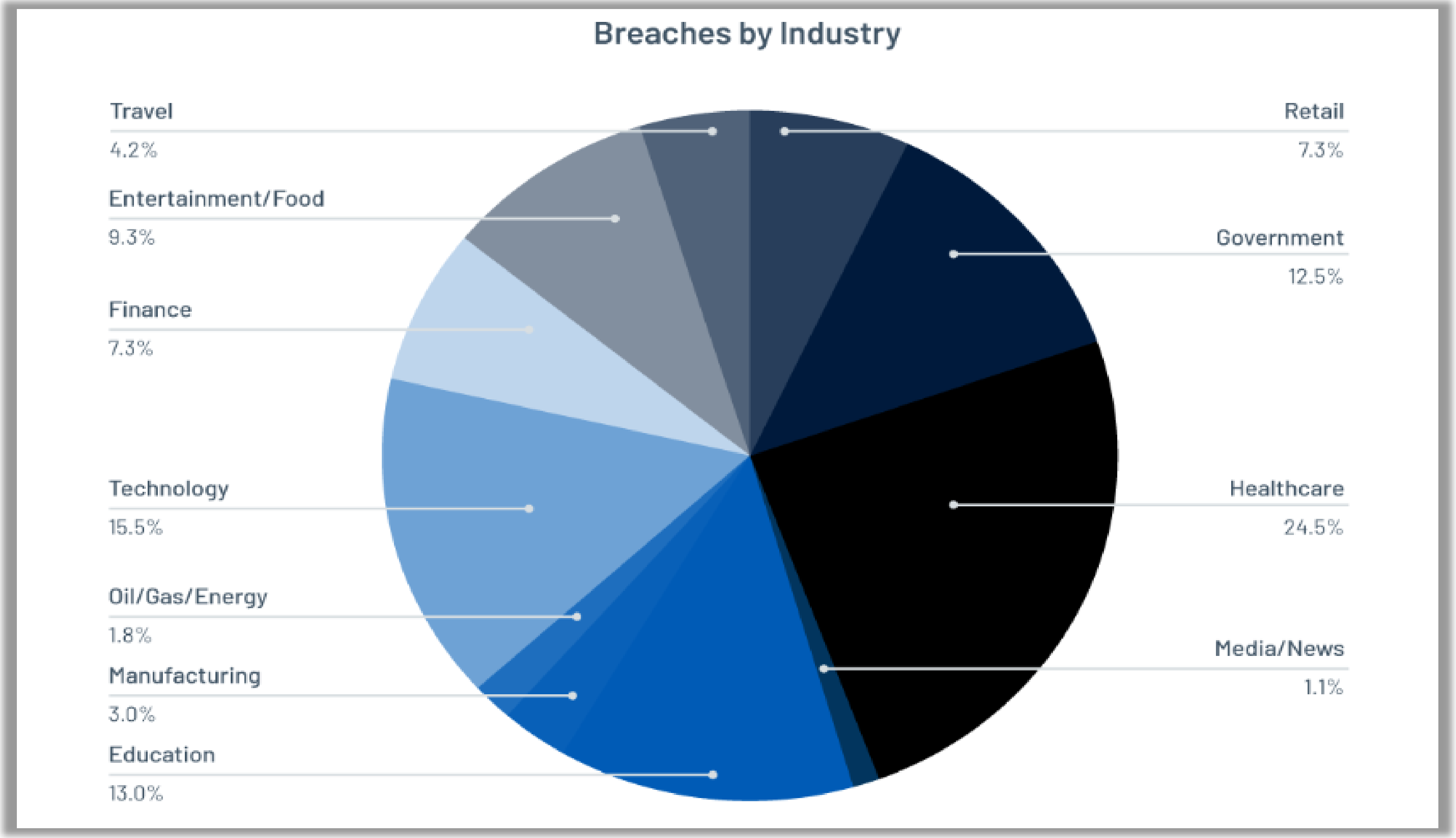
Healthcare Data Breaches in 2020

- TOP EIGHT BREACHES REPORTED TO HHS INVOLVED 500,000 RECORDS OR MORE
  - OVER 6.5 MILLION RECORDS TOTAL WERE REPORTED
- 75% OF ALL RECORDS EXPOSED IN THE SECOND HALF OF 2020 WERE DUE TO COMPROMISED BUSINESS ASSOCIATES.
- SPECIFIC TYPES OF HEALTHCARE ORGANIZATIONS TARGETED:
  - HOSPITAL SYSTEMS
  - LIFE SCIENCE LABS
  - RESEARCH LABS
  - REHABILITATION FACILITIES
  - GENERIC HEALTHCARE ORGANIZATIONS

OF THE 26 MILLION RECORDS BREACHED IN 2020, 93% WERE ATTRIBUTED TO MALICIOUS HACKING INCIDENTS, RATHER THAN OTHER CAUSES SUCH AS UNAUTHORIZED DISCLOSURE, IMPROPER DISPOSAL, THEFT OR LOSS.

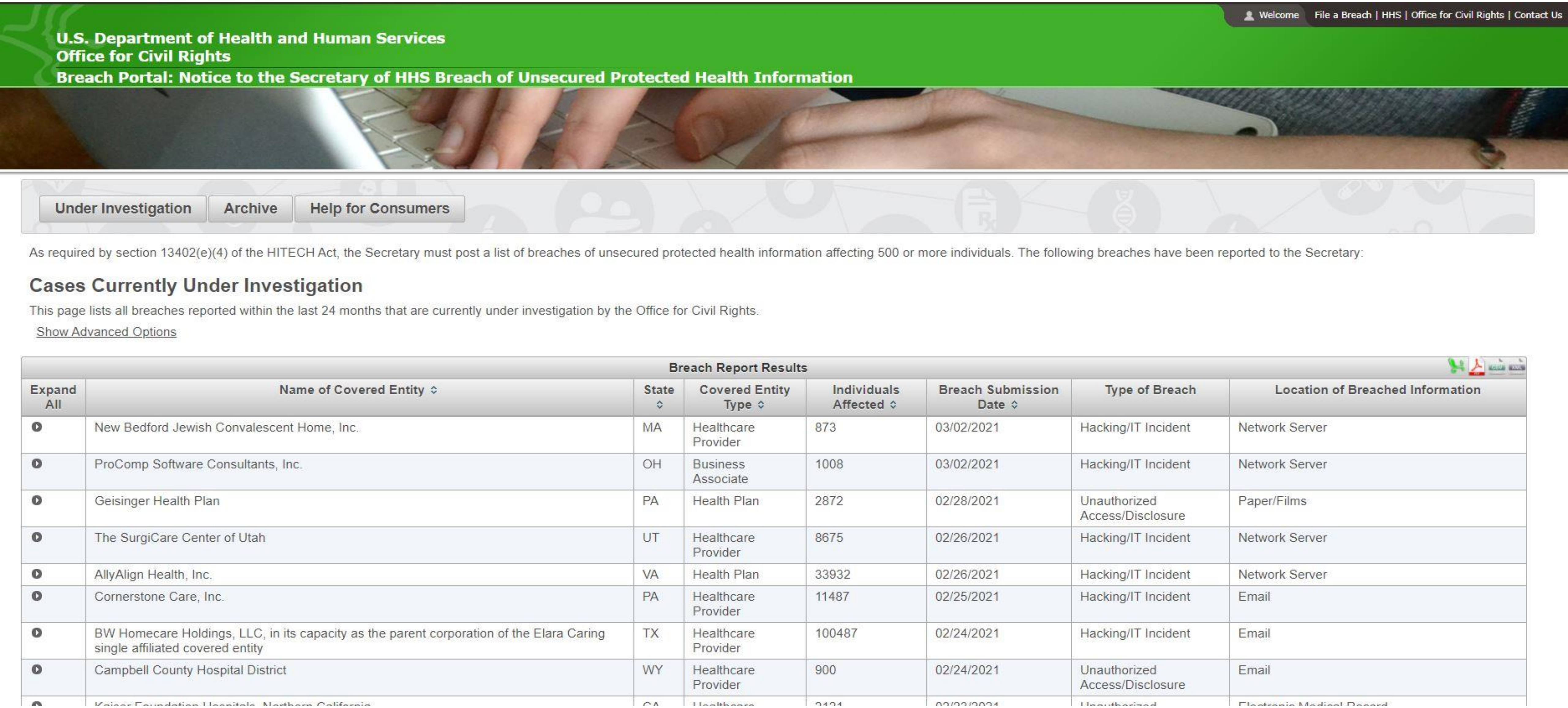


Healthcare Data Breaches and Other Sectors



Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HHS “Wall of Shame”



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

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

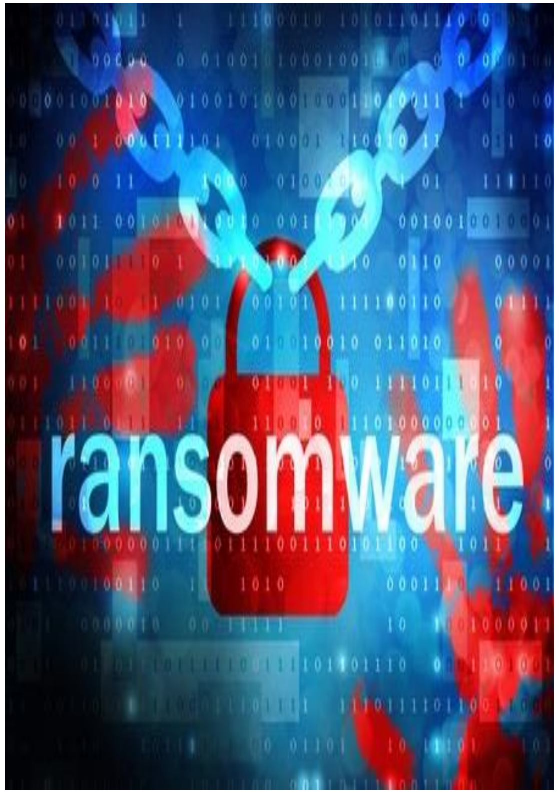
Breach Report Results

Expand All	Name of Covered Entity ⇕	State ⇕	Covered Entity Type ⇕	Individuals Affected ⇕	Breach Submission Date ⇕	Type of Breach	Location of Breached Information
●	New Bedford Jewish Convalescent Home, Inc.	MA	Healthcare Provider	873	03/02/2021	Hacking/IT Incident	Network Server
●	ProComp Software Consultants, Inc.	OH	Business Associate	1008	03/02/2021	Hacking/IT Incident	Network Server
●	Geisinger Health Plan	PA	Health Plan	2872	02/28/2021	Unauthorized Access/Disclosure	Paper/Films
●	The SurgiCare Center of Utah	UT	Healthcare Provider	8675	02/26/2021	Hacking/IT Incident	Network Server
●	AllyAlign Health, Inc.	VA	Health Plan	33932	02/26/2021	Hacking/IT Incident	Network Server
●	Cornerstone Care, Inc.	PA	Healthcare Provider	11487	02/25/2021	Hacking/IT Incident	Email
●	BW Homecare Holdings, LLC, in its capacity as the parent corporation of the Elara Caring single affiliated covered entity	TX	Healthcare Provider	100487	02/24/2021	Hacking/IT Incident	Email
●	Campbell County Hospital District	WY	Healthcare Provider	900	02/24/2021	Unauthorized Access/Disclosure	Email
●	Kaiser Foundation Hospitals, Northern California	CA	Healthcare	2121	02/22/2021	Unauthorized	Electronic Medical Record

… AND ALMOST 600 MORE

Healthcare Ransomware in 2020

- 560 HEALTHCARE ORGANIZATIONS IMPACTED BY RANSOMWARE – MORE THAN 1 PER DAY
- CLINICAL WORKFLOW DISRUPTED
- PAYMENT SYSTEMS DOWN
- AMBULANCES REROUTED
- RADIATION TREATMENTS FOR CANCER PATIENTS DELAYED
- MEDICAL RECORDS INACCESSIBLE AND SOME PERMANENTLY LOST
- HUNDREDS OF STAFF FURLOUGHED
- PHI AND OTHER SENSITIVE DATA STOLEN AND PUBLISHED ONLINE

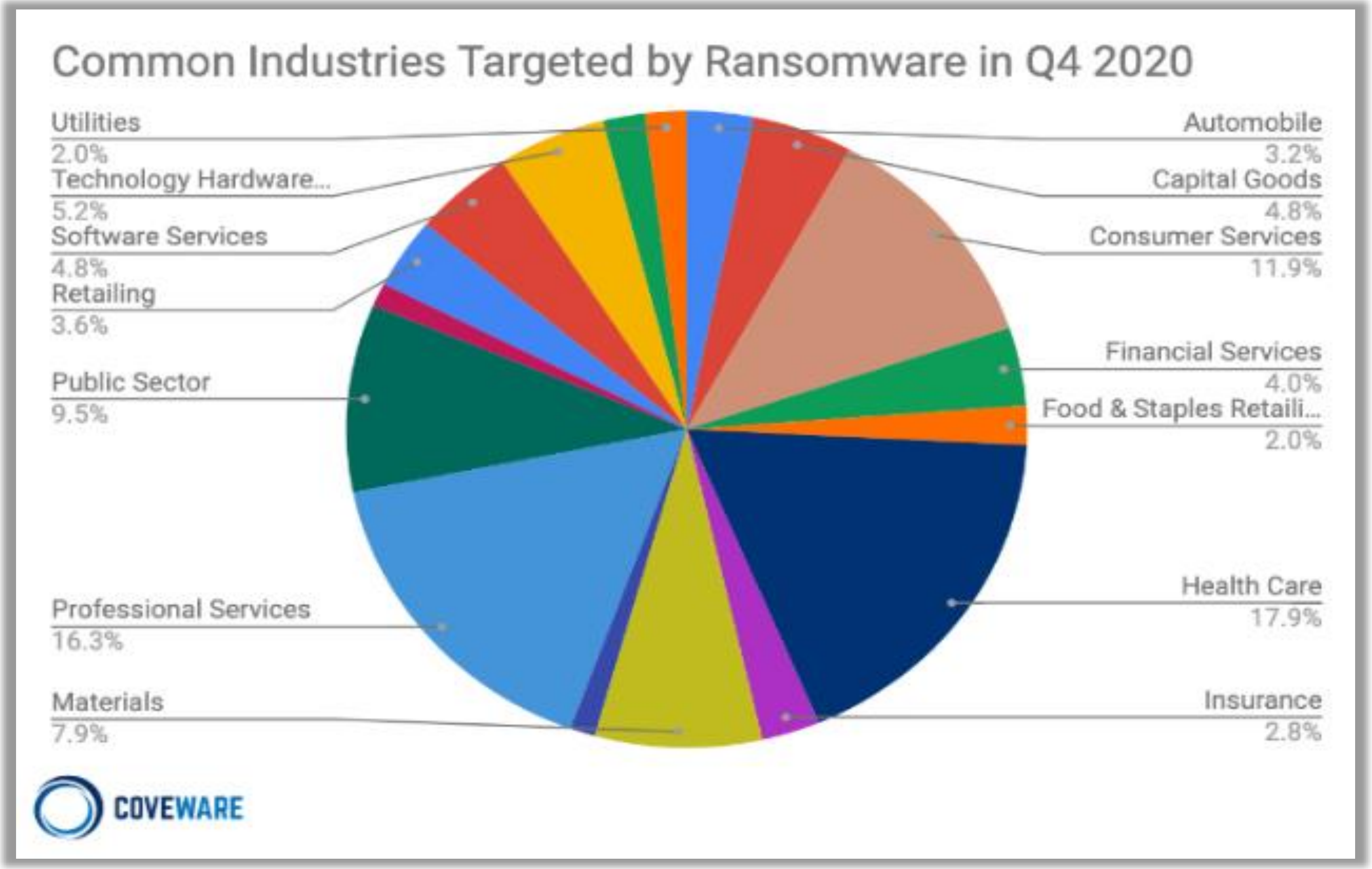


RESULTING RANSOMWARE RISK:

PATIENT HARM
LOSS OF QUALITY OF CARE

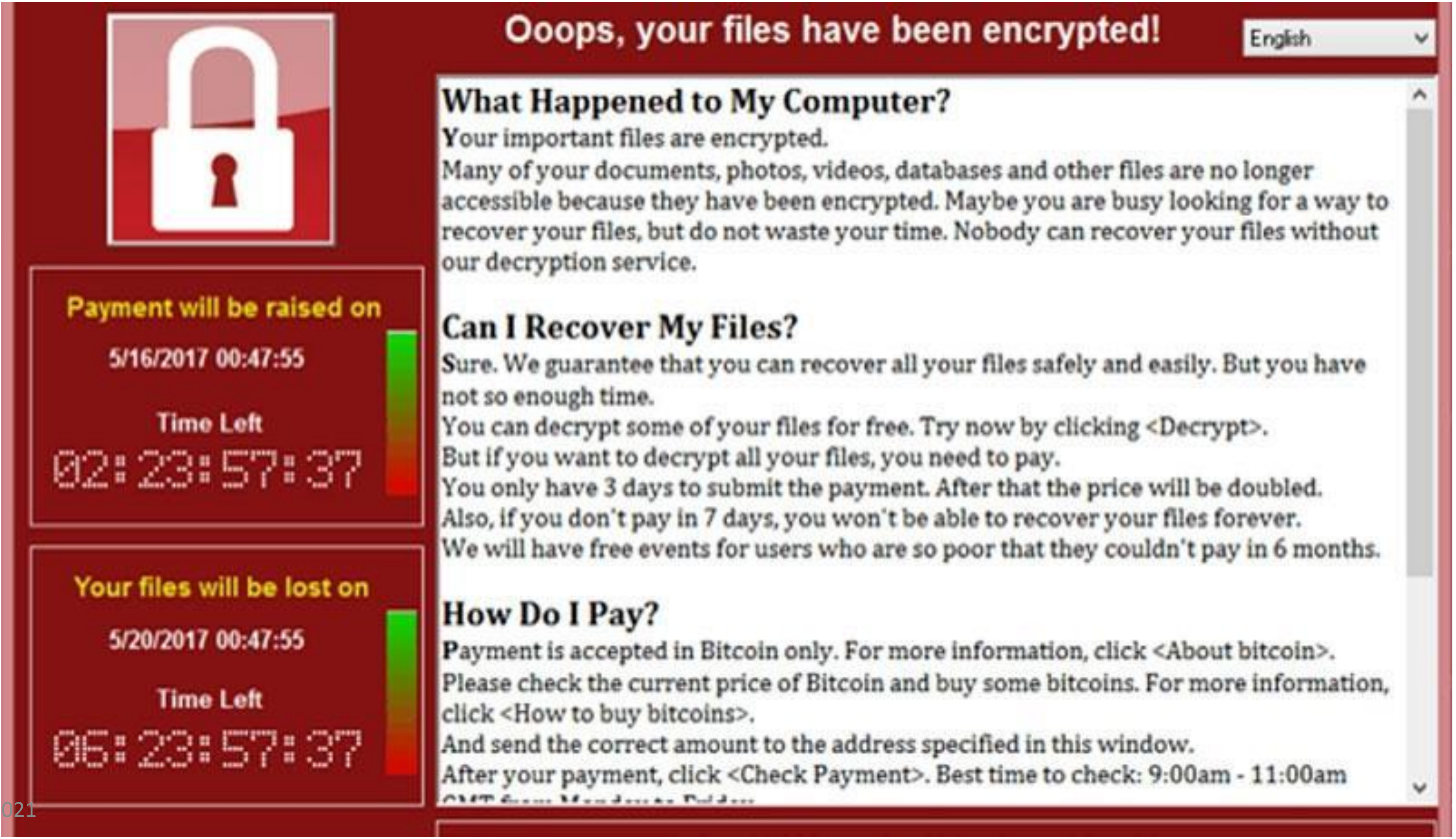
INCREASED BURN RATE
REDUCED OPERATIONAL EFFICIENCY

Healthcare Ransomware and Other Sectors



Source: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

Ransomware Attack Method



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

2020-21 OCR BREACH ACTION

ENTITY	WHEN	BREACH	IMPACT (# PEOPLE)	PENALTY ($M)
EXCELLUS HEALTH PLAN	JANUARY 2021	HACKED IT SYSTEM	9.3 MILLION	$5.1m
PREMERA	SEPTEMBER 2020	HACKED IT SYSTEM	10.4 MILLION	$6.85m
LIFESPAN HEALTH SYSTEM	JULY 2020	THEFT OF UNENCRYPTED LAPTOP		$1.04m

BREACHES UNDER OCR INVESTIGATION – 3/2020 – 3/2021: 522

BREACHES UNDER OCR INVESTIGATION IN MARYLAND: 15 – SAMPLES BELOW

ENTITY	WHEN	BREACH	IMPACT (# PEOPLE)	PENALTY ($M)
MEDSTAR HEALTH	9/25/2020	HACKED NETWORK SERVER	668	TBD
ADVENTIST HEALTH	9/11/2020	HACKED NETWORK SERVER	13,041	TBD
UNIVERSITY MARYLAND	7/24/2020	HACKED EMAIL	33,896	TBD
KAISER PERMANENTE	5/22/2020	UNAUTHORIZED ACCESS EMR	2756	TBD
MAGELLAN HEALTH MAGELLAN PHARMACY MAGELLAN IMAGING	6/12/20	HACKED EMAIL	50,410 33,040 22,560	TBD

Medical Device Risks

A patient bed has an average of 15 medical devices.
A 500 bed hospital could have **7,500 devices** . Most of them **connect to the network**.

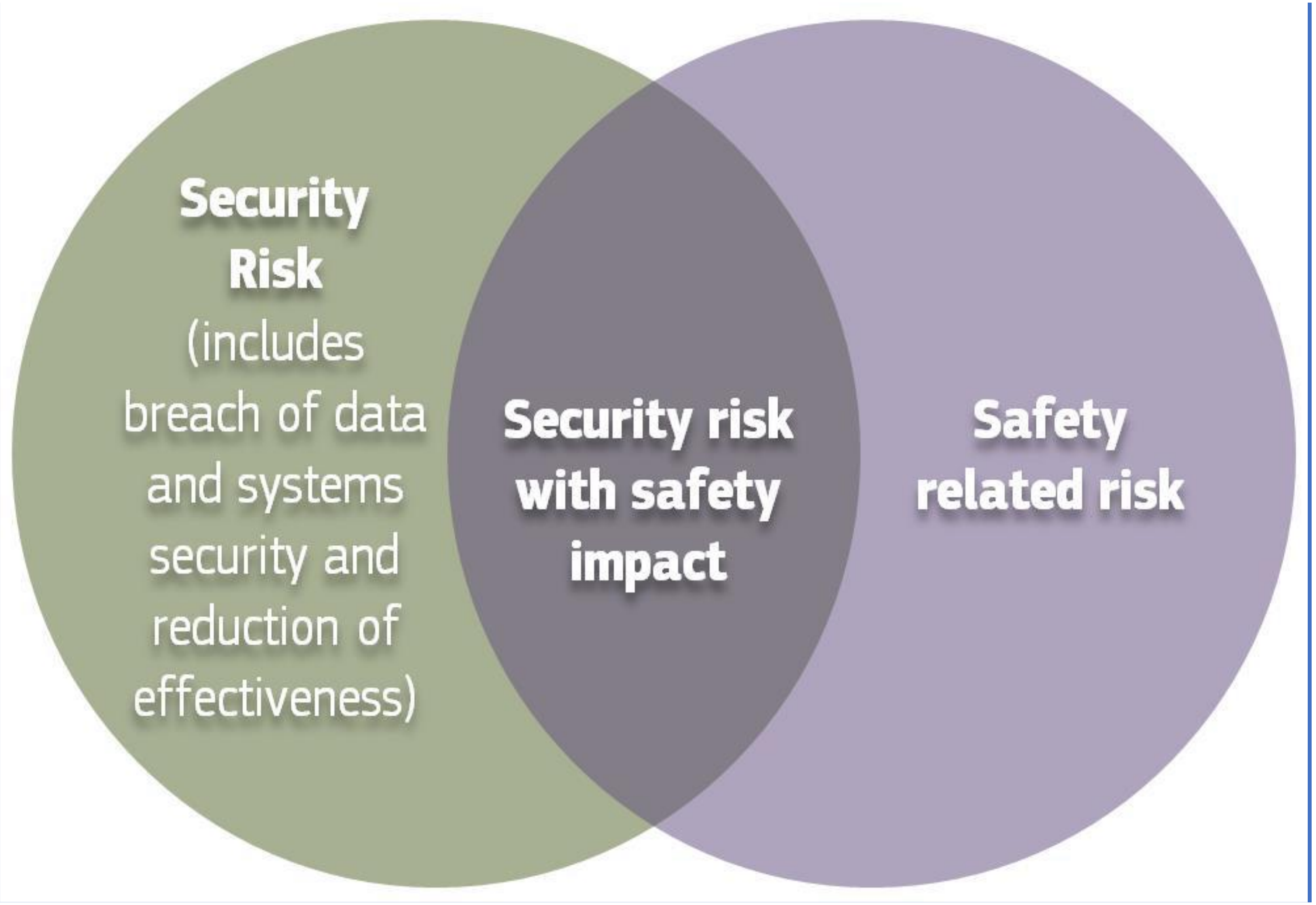
- Most hospitals have ‘networked’ medical devices over 8-10 years old.
- The security-related components in these devices pose a cyber risk
  - The operating systems & microcontrollers no longer receive maintenance or security patches from the component vendor. i.e “Not Supported by Vendor”
  - Often have common passwords set by the manufacturer that cannot be changed.
  - Often have unencrypted hard drives
- Time and cost to update these devices is very expensive

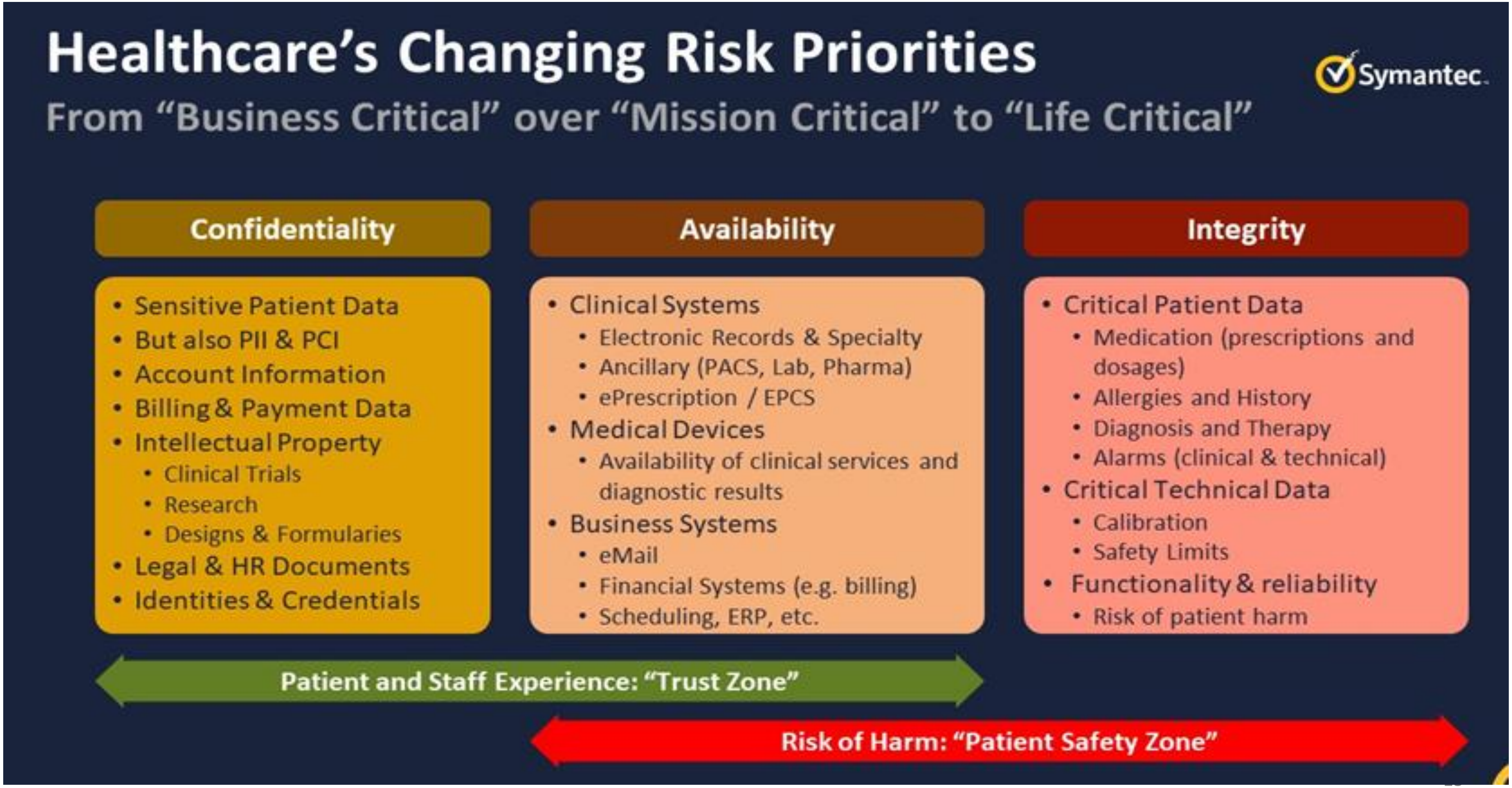
Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Medical Device Security and Management Must be Balanced

Balance between weak security… that could, for example, allow malicious modification of the operation of an implanted cardiac device and…

Restrictive security …
that could, for example, prevent medical personnel from accessing an implanted cardiac device without restrictions


Security Risk (includes breach of data and systems security and reduction of effectiveness)
Security risk with safety impact
Safety related risk



Healthcare's Changing Risk Priorities

Symantec.

From "Business Critical" over "Mission Critical" to "Life Critical"

Confidentiality

- Sensitive Patient Data
- But also PII & PCI
- Account Information
- Billing & Payment Data
- Intellectual Property
  - Clinical Trials
  - Research
  - Designs & Formularies
- Legal & HR Documents
- Identities & Credentials

Availability

- Clinical Systems
  - Electronic Records & Specialty
  - Ancillary (PACS, Lab, Pharma)
  - ePrescription / EPCS
- Medical Devices
  - Availability of clinical services and diagnostic results
- Business Systems
  - eMail
  - Financial Systems (e.g. billing)
  - Scheduling, ERP, etc.

Integrity

- Critical Patient Data
  - Medication (prescriptions and dosages)
  - Allergies and History
  - Diagnosis and Therapy
  - Alarms (clinical & technical)
- Critical Technical Data
  - Calibration
  - Safety Limits
- Functionality & reliability
  - Risk of patient harm

Patient and Staff Experience: "Trust Zone"

Risk of Harm: "Patient Safety Zone"

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

Prescription for Cyber Health

2017 Health Care Industry Cybersecurity (HCIC) Task Force – Six Imperatives and 105 Action Items

1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT
3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
4. Increase healthcare industry readiness through improved cybersecurity awareness and education
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks and exposure
6. Improve information sharing of industry threats, risks, and mitigations

How the Health Sector Collaborates to Addresses HCIC Recommendations

Health Sector Coordinating Council (HSCC)

- The cross-sector coordinating body representing one of 16 critical infrastructure sectors organized under Presidential Executive Order (PPD-21)
- As a “Critical Infrastructure Partnership Advisory Council”, exempted from Federal Advisory Committee Act requirements to protect ongoing sensitive deliberations with government
- A trust-community partnership convening companies, non-profits and industry associations across six subsectors
- ***Mission: to identify cyber and physical risks to the security and resiliency of the sector, and develop planning guidance in a 3-year Sector Specific Plan and implementing task groups for mitigating those risks***
- Focused on longer-term critical infrastructure policy and strategy, complementing the operational Health Information Sharing and Analysis Center

HSCC Joint Cybersecurity Working Group

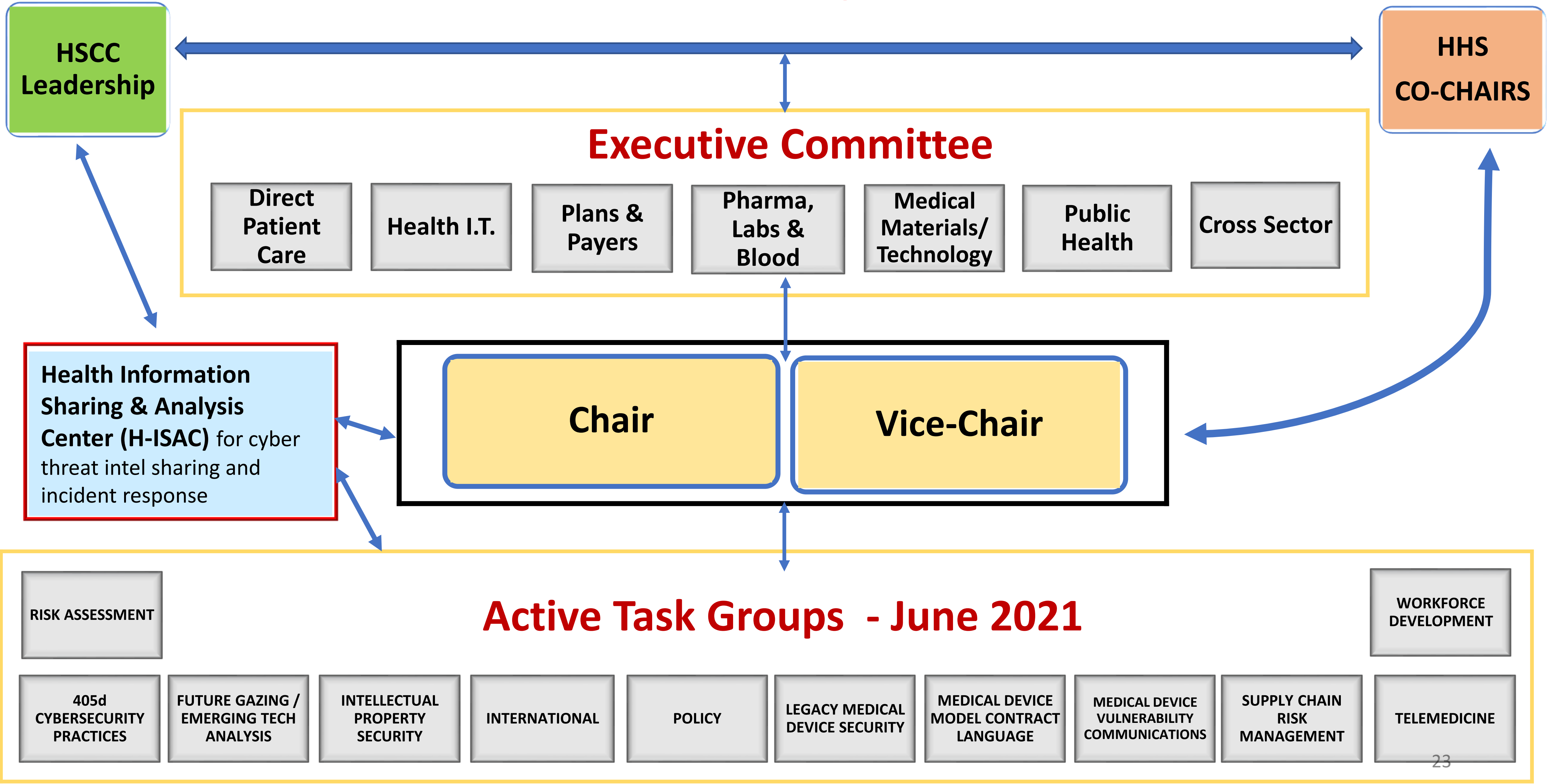
- Largest standing Working Group under the HSCC umbrella
- Identifies and develops strategic, cross-sector solutions to cybersecurity threats and vulnerabilities affecting the security and resiliency of the healthcare sector
- 277 voting industry member organizations, which includes 42 industry associations and professional societies across the 6 health subsectors;
- 15 federal, state, local and Canadian government agencies;
- 45 non-voting SME Advisors, and 657 total member-organization personnel
- 12 outcome-oriented task groups meet regularly through the year; Full CWG meets twice a year around the country
- Works closely on joint initiatives with:
    - HHS offices of Assistant Secretary for Preparedness and Response
    - Chief Information Officer
    - FDA

Organizational Membership Subsector Distribution

- Direct Patient Care: **39.1%**
- Health Information Technology: **10.0%**
- Health Plans and Payers: **3.9%**
- Mass fatality and Management Services: **0**
- Medical Materials: **10.8%**
- Laboratories, Blood, Pharmaceuticals: **4.7%**
- Public Health: **3.6%**
- Cross-sector: **8.6%**
- Government (Fed, State, County, Local): **10.5%**
- Non-Voting Advisors: **12.5%**

Governance

Cybersecurity Working Group Structure



HSCC Leadership

HHS CO-CHAIRS

Executive Committee

- Direct Patient Care
- Health I.T.
- Plans & Payers
- Pharma, Labs & Blood
- Medical Materials/ Technology
- Public Health
- Cross Sector

Health Information Sharing & Analysis Center (H-ISAC) for cyber threat intel sharing and incident response

Chair

Vice-Chair

Active Task Groups - June 2021

- RISK ASSESSMENT
- WORKFORCE DEVELOPMENT
- 405d CYBERSECURITY PRACTICES
- FUTURE GAZING / EMERGING TECH ANALYSIS
- INTELLECTUAL PROPERTY SECURITY
- INTERNATIONAL
- POLICY
- LEGACY MEDICAL DEVICE SECURITY
- MEDICAL DEVICE MODEL CONTRACT LANGUAGE
- MEDICAL DEVICE VULNERABILITY COMMUNICATIONS
- SUPPLY CHAIN RISK MANAGEMENT
- TELEMEDICINE

2021 Executive Committee

CHAIR: Terence (Terry) Rice Vice President, Information Risk Management and CISO, Merck. End of Term: Dec. 2021

VICE CHAIR: Theresa Meadows, SVP & CIO, Cook Children's Healthcare System. End of Term: Dec. 2021

Erik Decker, AVP - Chief Information Security Officer Intermountain Healthcare End of Term: Dec. 2021

Leslie A. Saxon, MD, Executive Director, USC Center for Body Computing. End of Term: Dec. 2023

Marilyn Zigmund Luke, Vice President, Special Projects America's Health Insurance Plans. End of Term: Dec. 2022

Michael McNeil, Senior Vice President, Global CISO, McKesson. End of Term: Dec. 2022

Greg Barnes, CISO Amgen. End of Term: Dec. 2021

Sri Bharadwaj, Vice President, Digital Innovation, Franciscan Health. End of Term: Dec. 2021

Denise Anderson, President, Health-ISAC. End of Term: Dec. 2021

Mark Jarrett, Chief Quality Officer, Senior Vice President & Associate Chief Medical Officer, Northwell Health. End of Term: Dec. 2022

JOINT CYBERSECURITY WORKING GROUP GOVERNMENT CO-CHAIRS

Suzanne Schwartz

Director
Office of Strategic Partnerships & Technology Innovation (OST)
Center for Devices and Radiological Health
U.S. Food and Drug Administration

Bob Bastani

Senior Cyber Security Advisor
Security, Intel, and Information Management Division
Office of the Assistant Secretary for Preparedness & Response
U.S. Department of Health and Human Services

Julie Chua

Director, Governance, Risk, Compliance (GRC)
HHS Office of the Chief Information Officer

Objectives –
Implementing the HCIC Recommendations

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Task Group Status as of June 2021

- 405(d) – HEALTH INDUSTRY CYBERSECURITY PRACTICEs
  - Released HICP Wave 1 Supplements (Quick Start and Matrix); continuing with Wave 2 and 3 supplements development
- FUTURE GAZING
  - Preparing White Paper on Artificial Intelligence
- HEALTH TECHNOLOGY RISK ANALYSIS
  - Preparing White Paper on Artificial Intelligence
- IP DATA PROTECTION
  - Published Health Industry Cybersecurity Protection of Innovation Capital Guide May 2020; to disband after HIC-PIC marketing initiatives
- INTERNATIONAL
  - Hosting webinars on health-cyber international coordination
- LEGACY MEDICAL DEVICES
  - Ongoing – Publication expected Q2 / late Q1
- MODEL CONTRACTS
  - Ongoing – Publication expected Q2
- VULNERABILITY COMMUNICATIONS
  - Ongoing - Publication this year
- POLICY
  - Activates as needed for policy proposals and response
- RISK ASSESSMENT
  - Finalized NIST Cyber Framework Implementation guide; under review by HHS for co-branding
- SUPPLY CHAIN
  - Published HIC-SCRiM v2 on September 22; Assessing options for next initiative
- TELEMEDICINE
  - Published in April "Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)"
- WORKFORCE DEVELOPMENT
  - Preparing series of cybersecurity training videos for clinicians and healthcare students

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

2019-2021 Guidance Publications

SEE: https://healthsectorcouncil.org/hscc-recommendations/

June 2021	Letter to President Biden on Healthcare Cybersecurity Strategy
April 2021	Health Industry Cybersecurity – Securing Telehealth and Telemedicine
September 2020	Health Industry Cybersecurity Supply Chain Risk Management
June 2020	Health Sector Return-to-Work (R2W) Guidance
May 2020	Health Industry Cybersecurity Tactical Crisis Response
May 2020	Health Industry Cybersecurity Protection of Innovation Capital
March 2020	Health Industry Cybersecurity Information Sharing Best Practices
March 2020	Management Checklist for Teleworking Surge During COVID-19
October 2019	Health Industry Cybersecurity Matrix of Information Sharing Organizations
June 2019	Health Industry Cybersecurity Workforce Guide
January 2019	Medical Device and Health IT Joint Security Plan (JSP)
January 2019	Health Industry Cybersecurity Practices (HICP)

Deliverables on Deck

- **Health Industry NIST Cybersecurity Framework Implementation Guide – Expected Q3**

- **Legacy Medical Device Cybersecurity Management Guide – Expected Late Q3**

- **Medical Device Model Cybersecurity Contract Language – Expected Late Q3**

2021 Priorities

- Coordinated incident response protocols
- Multi-tier supply chain security
- Clarified shared responsibility among MDMs and HDO for cybersecurity
- Security preparedness for remote, digital and emerging health technologies
- More capable clinical workforce in basic cybersecurity responsibilities
- Broad adoption of cyber security practices across provider ecosystem
- Structured and reliable partnership with government in healthcare cyber operations and policy
- Update 5-year plan of the 2016 Healthcare and Public Health Sector Specific Plan

Patient Safety Requires Cyber Safety

HEALTH SECTOR COORDINATING COUNCIL
Joint Cybersecurity Working Group

Greg Garcia

Executive Director

Greg.Garcia@HealthSectorCouncil.org

Allison Burke

Program Operations Lead

Allison.Burke@HealthSectorCouncil.org

https://HealthSectorCouncil.org