

HIPAA: Proactive Security & Compliance Best Practices

Webinar

Q4, 2021




Conversation Set Up

According to [Black Book Research](#), 90% of the healthcare staff working remotely during the COVID-19 outbreak did not receive any security guidelines or data privacy training before going remote.

At the same time, in 2020 the number of Healthcare industry cyber attacks in the U.S. increased by 45%. Some countries like Canada and Australia experienced cyber attack increases between 100% - 250%. *As of September 2021, cyber-attack frequency and severity is not slowing down.*

In August 2021 there were 707 healthcare data breaches reported for the previous 12-month period, up from 465 for the same time last year. HIPAA compliance was created to help protect customer health records and information, but many organizations struggle with data privacy and security.

In today's session we will discuss healthcare industry attack trends, and proactive IT and security best practices for addressing cyber threats and HIPAA compliance.

A man with glasses and a beard is sitting at a desk, looking at a computer monitor. A woman is standing next to him, leaning over his shoulder and pointing at the screen. The monitor displays a line graph with a blue line and a red line, and some text. The background is blurred, showing other people and office equipment.

Since January 2021, 38 attacks on health care providers or systems have disrupted patient care at roughly 963 locations, compared with 560 sites being impacted in 80 separate incidents from all of 2020."

- Brett Callow, Threat Analyst, Emsisoft

Arstechnica.com 2021

Why Healthcare?

The largest industry in the U.S. @ 17.8% of the GDP - \$3.6T. 784K Companies within the Industry.

Growing Market. Global Spend is Estimated @ \$10T by 2022. CAGR is 7.3%.

Vulnerable Supply Chain. Business Associates now account for 43% of all breaches in 2021.

Value of Data. Personal Health Records and Information Fetch Big \$ the Dark Web.

Patient records can sell between \$1 and \$1,000 due to the amount of information found in the documents, including date of birth, credit card information, Social Security number, address and email. These records are used to commit pharmaceutical and medical fraud on the Dark Web and internationally.

Xceptional.com



“There has been a major increase in the number of cyberattacks on business associates of HIPAA covered entities, which now account for 43% of all reported healthcare data breaches. In the first 6 months of 2021, there were 141 data breaches reported by business associates of HIPAA-covered entities.”

- HIPAA Journal, September 2021

Healthcare Industry Realities

Staff:

- Mentally Tired
- Emotionally Tired
- Overworked
- Talent Shortage

IT, InfoSec, Operations:

- Legacy & Unpatched Systems
- Legacy and Unpatched Applications
- Growth of Internet Connected Devices (IoT)
- Growing Threat Landscape, Facilities, Clinics, TeleHealth
- Understaffed IT Departments
- Understaffed Infosec Departments
- Understaffed Operations
- Unsecured 3rd Party Partners

<https://healthitsecurity.com/news/87-health-orgs-lack-security-personnel-for-effective-cyber-posture>

Xceptional.com



“Managing regulatory change was reported as the top compliance challenge in 2020. 34% of companies report outsourcing some or all of their compliance, up from 28% in 2019.”

- Thomson Reuters Cost of Compliance 2020 Report.

The Rate of Change: Reginfo.gov



September 22, 2021



Average loss per ransomware attack reported on SARs increased from \$417,000 in 2018 to \$783,000 in 2020. (FinCEN / FBI)

Regulatory Pressure Points:

1. Increased integration and improved operational resiliency, including cyber risk management
2. Outdated risk assessment and resiliency frameworks
3. Closer partnership between the board and business functions to strategically align initiatives
4. Focus on modern technology resilience across platforms, data and applications
5. Expanded cyber and vulnerability threats resulting from increased use of digital platforms, including rapid cloud adoption and software deployment
6. Regulatory focus on proprietary data, customer data, core processes, and exposure from third party vendors and partners
7. Availability of new technologies and tooling; increased focus on IT asset management and the need for a complete and accurate view of IT assets
8. Enhanced integration of cyber risk management with enterprise risk management

Top Technology risks to manage



Software development



Obsolete technology



Security of systems and data



People and skills



Third party technology and services



Failed technology strategy



Services and availability



Emerging technology



Data quality and management



Regulations and compliance

Compliance Realities In Healthcare

Healthcare spends about \$39 billion annually on the administrative facets of regulatory compliance.

***Hospitals with 161 beds pay on average \$7.6M in compliance administrative costs per year.**

Estimated annual costs of regulatory compliance for the average hospital is \$47K per bed.

The number of regulations for Acute Care providers has grown to 629 – 288 more than 2017.

A report by the Ponemon Institute found that the average cost of compliance for an organization was \$5.5 million. Meanwhile, the average cost of noncompliance was over \$14.5 million.

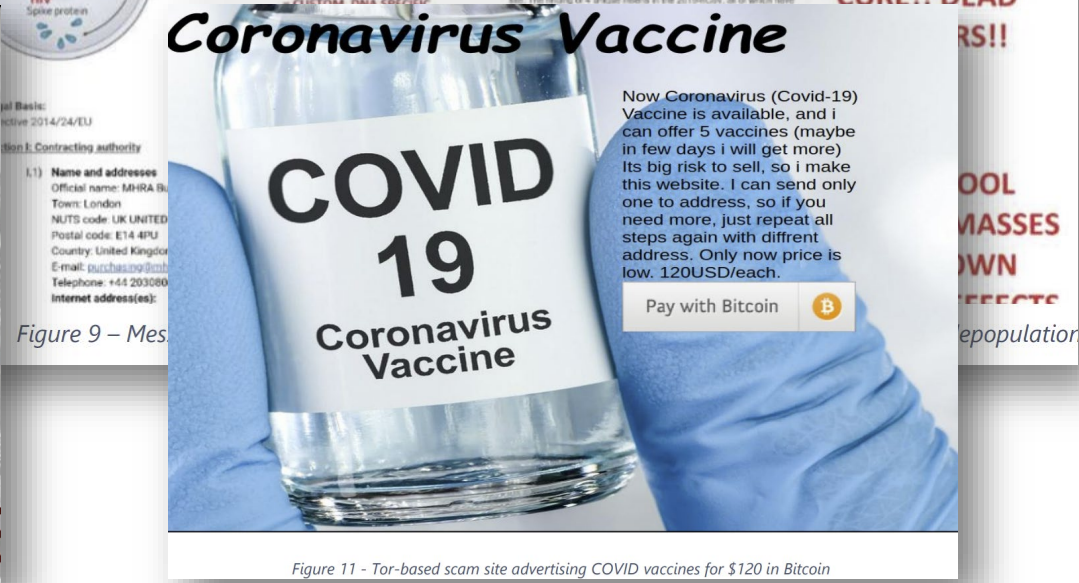
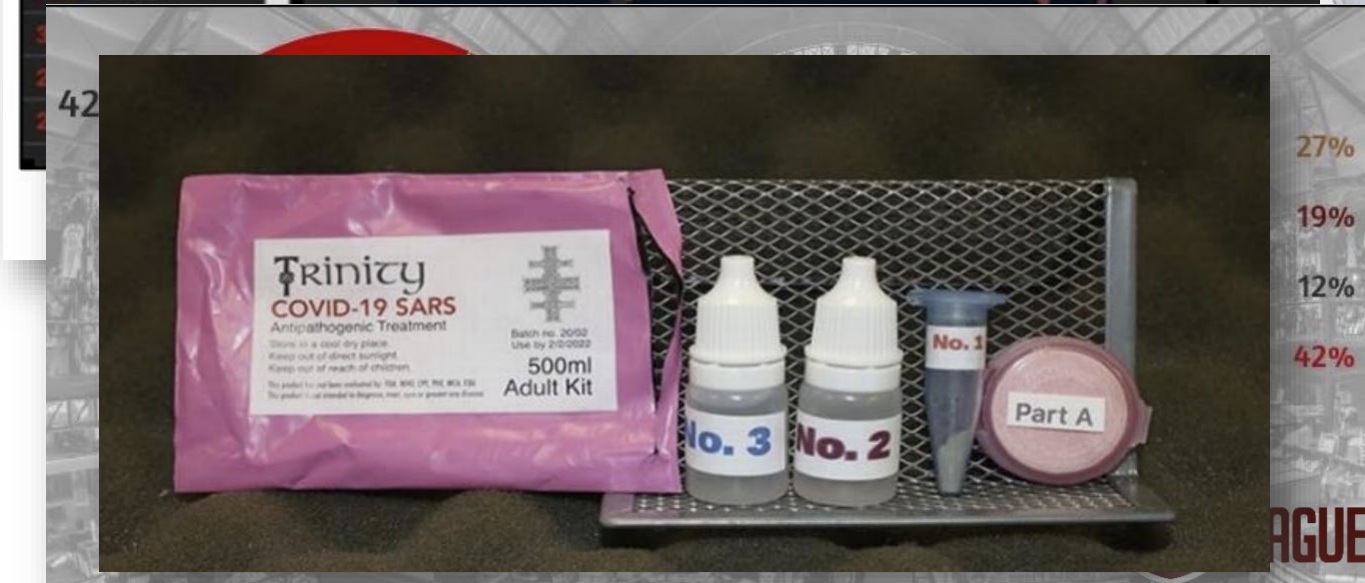
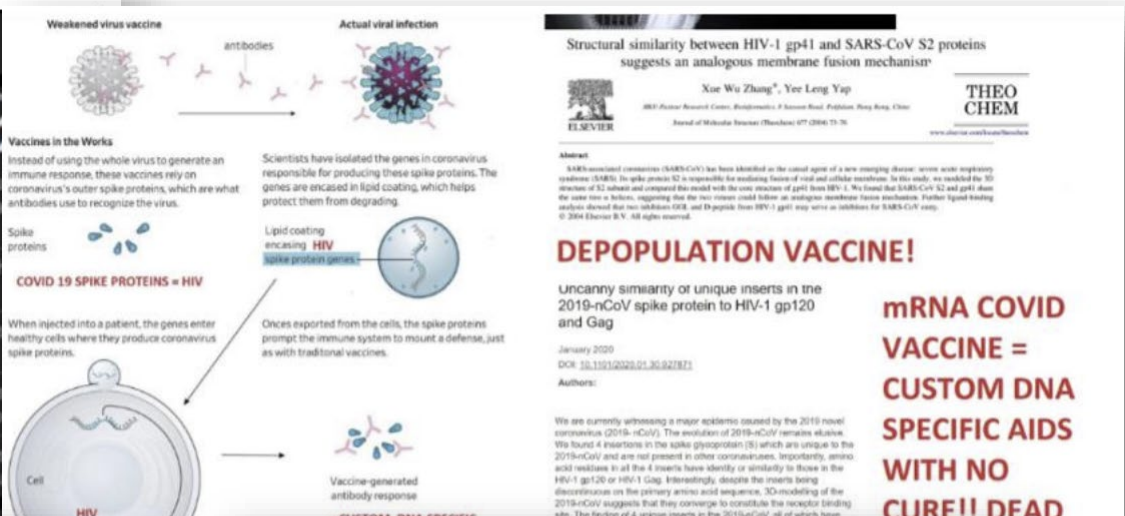
exceptional.com



Growing Number of State & International Privacy Regulations

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California.

2020 Healthcare Focused Dark Web Ads, Ransomware

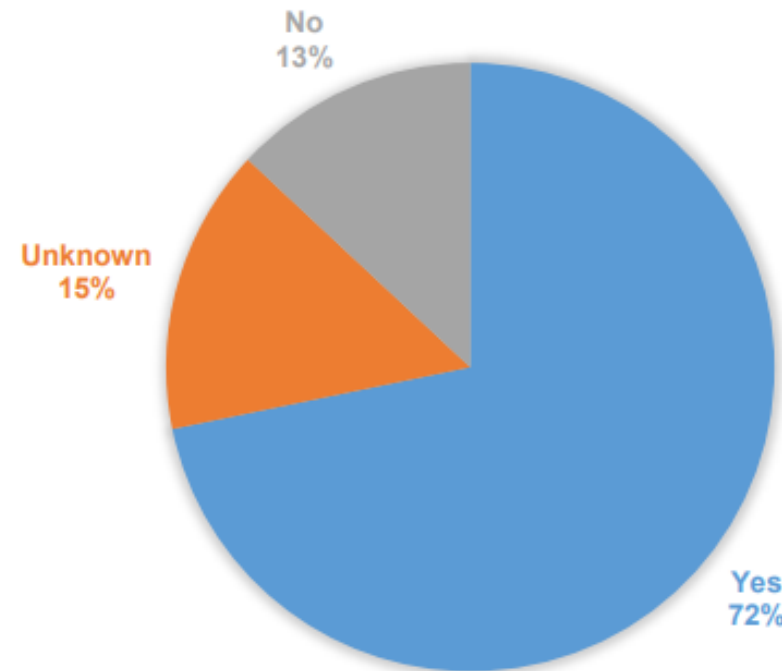


2021 Ransomware Attacks



- Looking back at a total of **48 ransomware incidents in the United States healthcare sector** tracked by HC3 this year, for **at least 72%** of the ransomware incidents, victim data was leaked.
- This involved either full file dumps, screenshots, or samples.
- Based on HC3 observations of ransomware blogs, data leaks ranged from just a few screenshots to as large as Terabytes of data from the victims.

U.S. HPH RANSOMWARE INCIDENTS 2021: WAS DATA LEAKED?




SECURITY

Dark Web Ar...

Update to R... Adds Netwo...

Federal French resea... ransomware variant... allow it to automatic...



Li... at... bi...
The... again...
Doze... wors... which...
It's... had... down...

Ransomware gang plans to call victim's business partners about attacks



By [Lawrence Abrams](#)

March 6, 2021 12:47 PM



by ransomware last year
defense after

es Ransomware reness and

resist, and report attacks

Prism and Financial Intelligence today
n efforts to combat ransomware scams
ey laundering and sanctions regulations
Financial Intelligence may have
nts. Efforts to detect and report
om deploying malicious software to
s accountable for their crimes.

ools, hospitals, and businesses of all
nue to use its powerful tools to counter

Attack Trends 24-36 Months Ago



P = Phishing Attack
R = Ransomware Attack
V = Vendor, Supply Chain Attack

The financial impact of these attacks are significant!

How One Ransomware Attack Cost Erie County Medical Center \$10 Million



NEWS
42,000 patients impacted by 2016 breach of Michigan provider

by [Jessica Davis](#) | June 04, 2018
A hacker told Holland Eye Surgery and Laser Center in March that they had accessed a patient list, but an investigation revealed that



NEWS
Phishing hack on Ohio provider breaches data of 42,000 patients

by [Jessica Davis](#) | May 29, 2018
A hacker hit some email accounts of Aultman Health Foundation with a phishing attack in February, but officials didn't discover the



NEWS
Data of 500k patients compromised in LifeBridge Health breach

by [Beth Jones Sanborn](#) | May 23, 2018
Discovered on March 18, the health system was infected with malware that infected its EMR server, patient registration and billing



NEWS
Ransomware attack breaches 40,800 patient records in Hawaii

by [Jessica Davis](#) | September 13, 2018
The Fetal Diagnostic Institute of the Pacific was able to restore data from backups, and with help from a cybersecurity firm wipe the



NEWS
Phishing attack breaches 38,000 patient records at Legacy Health

by [Jessica Davis](#) | August 22, 2018
The hackers went undetected for several weeks at the Portland, Oregon-based health system.



NEWS
417,000 Augusta University Health patient records breached nearly one year ago

by [Jessica Davis](#) | August 17, 2018
The Georgia provider was hit by two cyberattacks in September 2017, but did not explain when the breach was discovered.



NEWS
DoD IG finds massive security flaws in Army, Navy EHR

by [Jessica Davis](#) | May 08, 2018
Inspector general says Defense Health Agency sites failed to consistently implement technical, physical and administrative



NEWS
205,000 patient records exposed on misconfigured FTP server

by [Jessica Davis](#) | May 18, 2018
MediEvolve, a practice management software vendor, left its FTP server open to the public without the need for a login.



NEWS
OCR investigating Banner Health for breach of 3.7 million records

by [Jessica Davis](#) | March 21, 2018
The Arizona health system is cooperating with the investigation but expects to receive negative findings and a potential fine.



NEWS
Canadian pharmacist fined for routinely accessing health records of acquaintances

by [Lynne Minion](#) | August 13, 2018
She snooped in the EHRs of nearly four dozen people over two years.



NEWS
1.4M records breached in UnityPoint Health phishing attack

by [Jessica Davis](#) | July 31, 2018
This is the second breach for the health system this year, and the biggest health data breach of 2018 in the U.S.



NEWS
Third-party vendor error exposes data of 19K patients for 2 months

by [Jessica Davis](#) | August 02, 2018
Orlando Orthopaedic's transcriptionist vendor misconfigured access to a database during a software upgrade. The health center waited



NEWS
Ransomware breaches data of 85,000 patients

by [Jessica Davis](#) | April 26, 2018
Hackers hit the IT vendor of three Center for Orthopaedic Specialists locations in February, which locked out users and prevented patient



NEWS
UnityPoint Health System hit with cyberattack affecting 16,000 patients

by [Beth Jones Sanborn](#) | April 20, 2018
Hospital is advising patients to monitor their



NEWS
California medical device manufacturer reports breach of 30,000 consumers

by [Jessica Davis](#) | April 17, 2018
Inogen reports a hacker accessed an



NEWS
Ransomware, malware attack breaches 45,000 patient records

by [Jessica Davis](#) | July 26, 2018



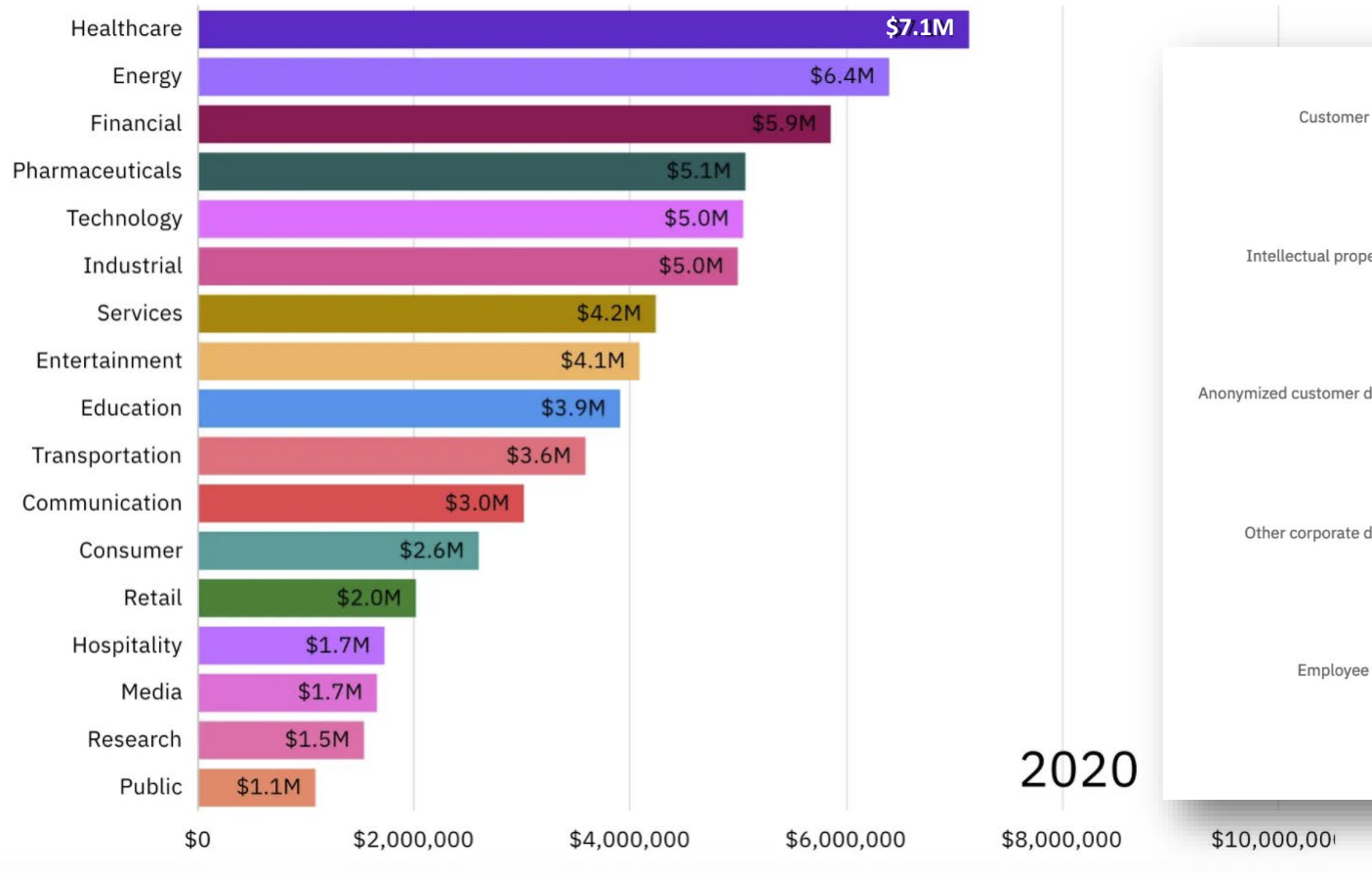
NEWS
LabCorp's network breach puts millions of records at risk

by [Jessica Davis](#) | July 17, 2018



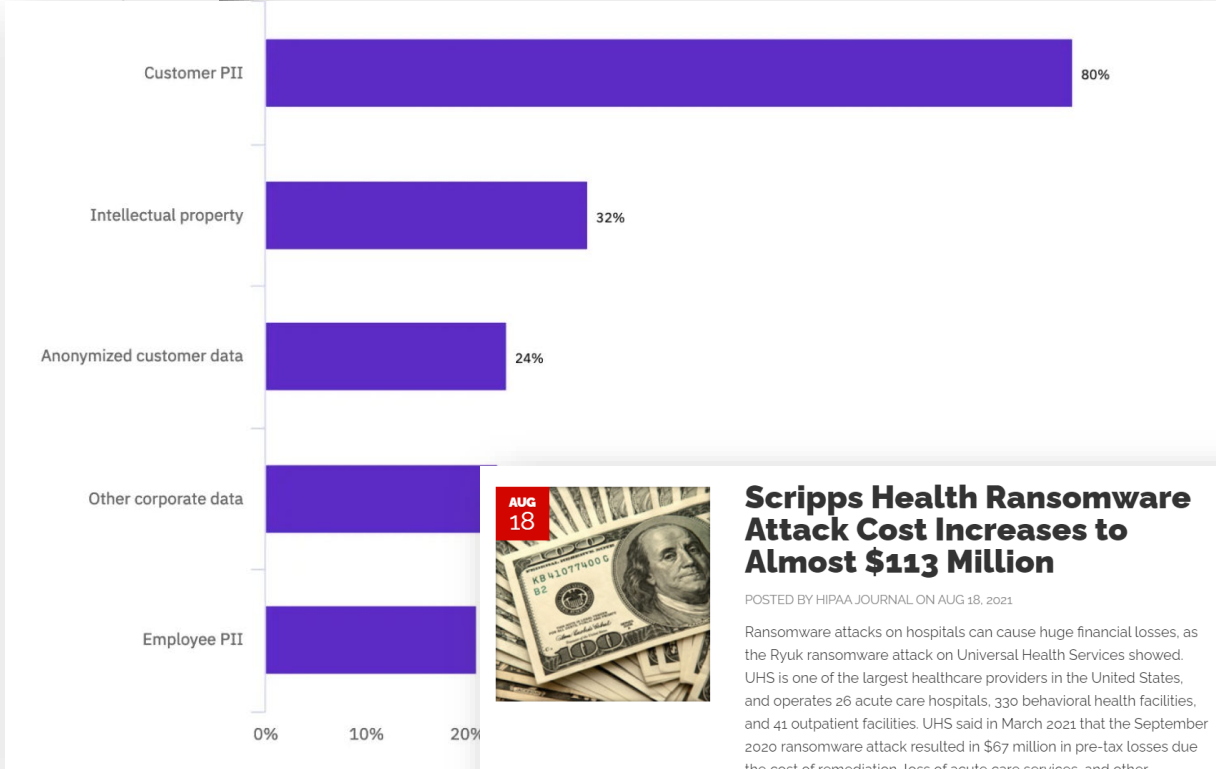
NEWS
Hackers breach 1.5M Singapore patient records, including the prime minister's

Ave Cost of a Data Breach by Industry



2020

Top Data Types Stolen



Scripps Health Ransomware Attack Cost Increases to Almost \$113 Million

POSTED BY HIPAA JOURNAL ON AUG 18, 2021

Ransomware attacks on hospitals can cause huge financial losses, as the Ryuk ransomware attack on Universal Health Services showed. UHS is one of the largest healthcare providers in the United States, and operates 26 acute care hospitals, 330 behavioral health facilities, and 41 outpatient facilities. UHS said in March 2021 that the September 2020 ransomware attack resulted in \$67 million in pre-tax losses due to the cost of remediation, loss of acute care services, and other expenses incurred due to the attack. While the losses suffered by UHS were significant, the ransomware attack on Scripps Health has proven to be far more expensive. Scripps Health is a California-based nonprofit operator of 5 hospitals and 19 outpatient facilities in the state. In the May 2021 ransomware attack, Scripps Health lost access to information systems at two of its hospitals, staff couldn't access the electronic medical record system, and its offsite backup servers were also affected. Without access to critical IT systems, Scripps Health was forced to re-route stroke and heart attack patients from four...

<https://digitalguardian.com/blog/what-does-data-breach-cost-2020>

HIPAA Risk Assessment (Title II) 245 Controls

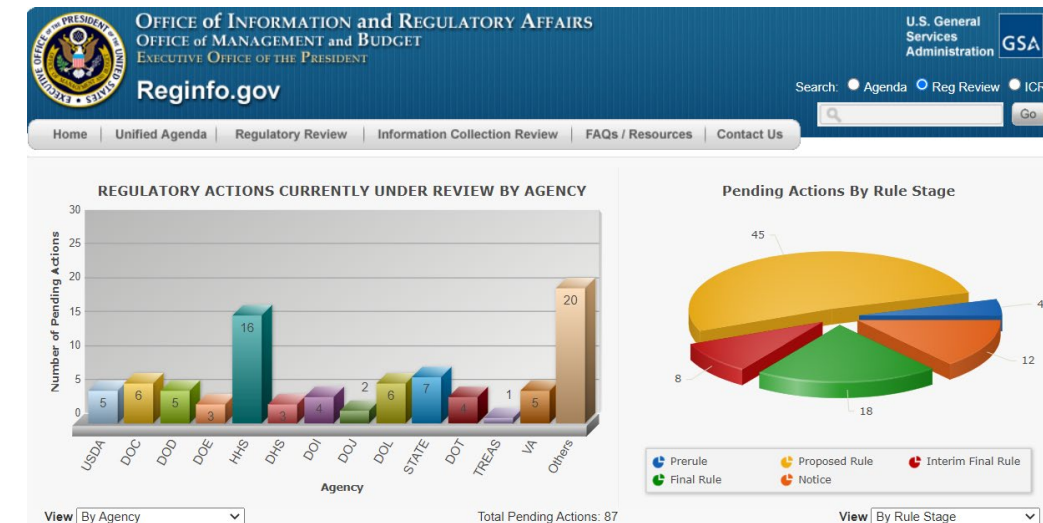
Measures an organization's ability to meet the HIPAA standards and requirements set forth by Congress and the Department of Health and Human Services (HHS) around electronic health data (**electronic Protected Health Information – ePHI**)

Privacy Rule (both paper and electronic PHI)

- 2 Privacy Safeguards: Use and Disclosures.....**89 Controls**

Security Rule (ePHI – only)

- Administrative Safeguards**73 Controls**
- **Technical Safeguards45 Controls**
- Physical Safeguards**38 Controls**



HIPAA Realities: Growing Penalties



HIPAA Violation Type	Civil Penalty (MIN)	Civil Penalty (MAX)
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	\$100 - \$50,000 per violation, with an annual maximum of \$25,000 for repeat violations	\$59,522 per violation, with an annual maximum of \$1,789,651
HIPAA violation due to reasonable cause and not due to willful neglect	\$1,000 - \$50,000 per violation, with an annual maximum of \$100,000 for repeat violations	\$59,522 per violation, with an annual maximum of \$1,789,651
HIPAA violation due to willful neglect but violation is corrected within the required time period	\$10,000 - \$50,000 per violation, with an annual maximum of \$250,000 for repeat violations	\$59,522 per violation, with an annual maximum of \$1,789,651
HIPAA violation is due to willful neglect and is not corrected	\$59,522 per violation, with an annual maximum of \$1,789,651	\$59,522 per violation, with an annual maximum of \$1,789,651

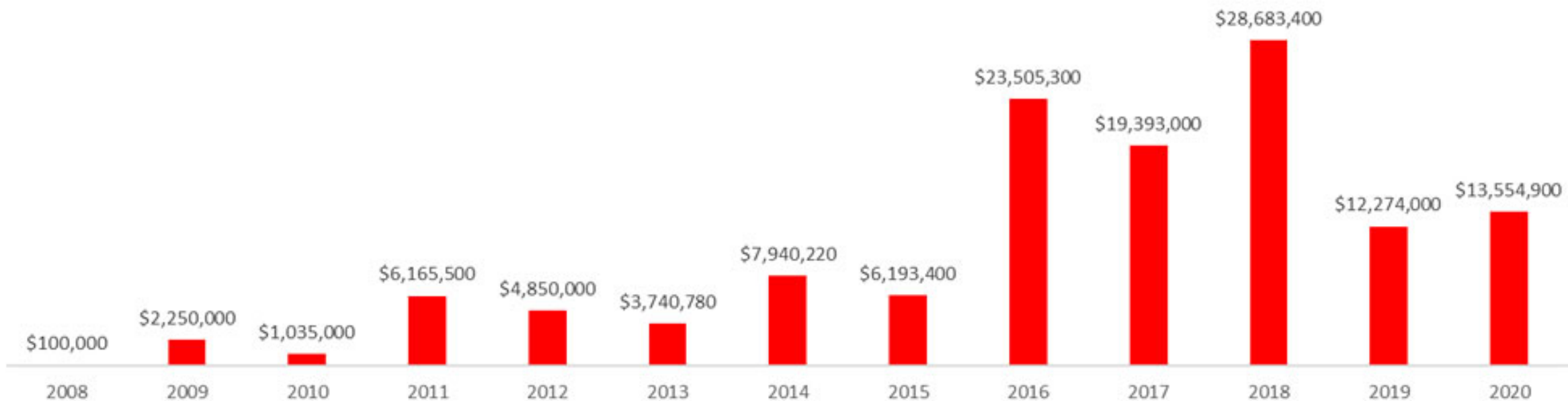
<https://www.govinfo.gov/content/pkg/FR-2020-01-17/pdf/2020-00738.pdf>

[https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement#:~:text=Civil%20violations&text=The%20secretary%20is%20prohibited%20from,extended%20at%20HHS'%20discretion\).](https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement#:~:text=Civil%20violations&text=The%20secretary%20is%20prohibited%20from,extended%20at%20HHS'%20discretion).)

PCI Violation Month	Merchant Level 1	Merchant Level 2
1 to 3	\$10,000 monthly	\$5,000 monthly
4 to 6	\$50,000 monthly	\$25,000 monthly
7 and on	\$100,000 monthly	\$50,000 monthly

OCR PENALTIES FOR HIPAA VIOLATIONS

HIPAA SETTLEMENTS AND CIVIL MONETARY PENALTIES



Proactive Cyber & IT Best Practices



TRENDS TO RECOGNIZE

- Hacking the Human Works
- Phishing & Social Engineering Attacks, Losses Are Growing YOY
- Ransomware & Malware Attacks Are Pervasive
- Scans & Attacks Are Automated 24/7/365
- Once Breached, Infected, Attacks Increase
- No One is Too Small For Criminals, Hackers To Attack

HOW TO BEGIN

- The 4 Ps: People, Program, Patching, passwords,
- Identify Crown Jewels
- Educate Employees
- Understand Your Maturity, Risks, Vulnerabilities
- Discover Your Assets, Who Has Access to Your Systems
- Patch, Update Systems, Applications, Websites
- Harden & Monitor Systems, Applications, Websites

EVOLVE THE PROGRAM

- People (Train, Educate, Phish, Incentivize)
- Data (Encrypt Customer, Business Info)
- Platforms, Systems (Scan, Patch, Update, Remediate)
- Brand, Enterprise (Pen Test, Risk Assessment, Remediation, Logging, Monitoring, Alerting, Incident Response, Password & Vulnerability Management)
- Partners, Vendors (Assessment, Score Card, Rank, Remediate)

FIND A TRUSTED PARTNER

- End Point Detection & Response (Anti-Malware, Anti-Ransomware)
- Managed Threat Detection, Alerting, & Response (SIEM, SOC)
- Security and Risk Assessments
- Security as a Service
- Compliance as a Service

Where to Begin?



Begin with the 4 P's: <https://resources.xceptional.com/webinars>

- ☐ **People** (Security Education, Training, Awareness, Internet Usage, Phishing Simulations)
- ☐ **Program** (Data Privacy, *SOC-SIEM, Logging/Monitoring, Policies, Procedures, Resources)
- ☐ **Patching, Scanning** (Vulnerability Management Program - Planned, Automated)
- ☐ **Passwords** (Unique Phrases w Special Characters, Vault)
 - ✓ **Data Privacy, Data Encryption** (At Rest, In Transit)
 - ✓ **Security Operations, SIEM, Scanning & Monitoring**
 - ✓ **Backups** (Full-Off Network)
 - ✓ **Limit and Lock Down Administrative and System Access Control/Write**
 - ✓ **Limit, Block Network Access** (RDP, etc), email file extension delivery
- ✓ **End Point Detection & Response: Modern Anti-Malware, Ransomware, Encryption on End Points**
- ✓ **Updated BCDR Plans, Solutions** (Ransomware, Social Engineering)
- ✓ **IoT, IT Inventory, Assessment & Pen Testing**
- ✓ **Business Process Assessments**

Compliance Solutions Map



Company Size	Industries	Regulatory Requirement, Business Driver	Common Cyber Threats, Attacks	Potential Security, Compliance Solutions
Small, Medium, Large	Covered Entities: Hospitals, Clinics, Group Practices, Independent Dr. Offices, Labs, etc	PCI Compliance, Letter from Processor, HIPAA Compliance, HITRUST Certification, HHS Notice	Data Breach, Malware or Ransomware Attack, Business Email Compromise, Social Engineering (Phishing, Vishing, Physical) Attack, 3 rd Party Partner Vendor Breach	Security Operations Center SIEM Scanning & Monitoring, Encryption, Anti-Ransomware Software, Compliance as a Service, Policies-Procedures-Services-Solutions Bundled as MRC, Vendor Risk Assessments, Quarterly ASV Scanning
Small, Medium, Large	Business Associates: Manufacturing, Bio, Business Services, Supplies,	FDA, EPA, SSAE, ISO, SOC 2, HIPAA, Other Federal & Industry Compliance, Letter from Covered Entity	DDoS Attack, Data Breach, Malware or Ransomware Attack, Business Email Compromise, Business Process Compromise, Social Engineering (Phishing, Vishing, Physical) Attack, 3 rd Party Vendor Data Breach	Security Operations Center SIEM Scanning & Monitoring, Anti-Ransomware Software, Encryption, Compliance as a Service, Policies-Procedures-Services-Solutions Bundled as MRC



Cisco Compliance Solution for HIPAA Security
Rule Design and Implementation Guide
A Cisco Validated Design



Figure 2-1 Cisco HIPAA Solution Framework

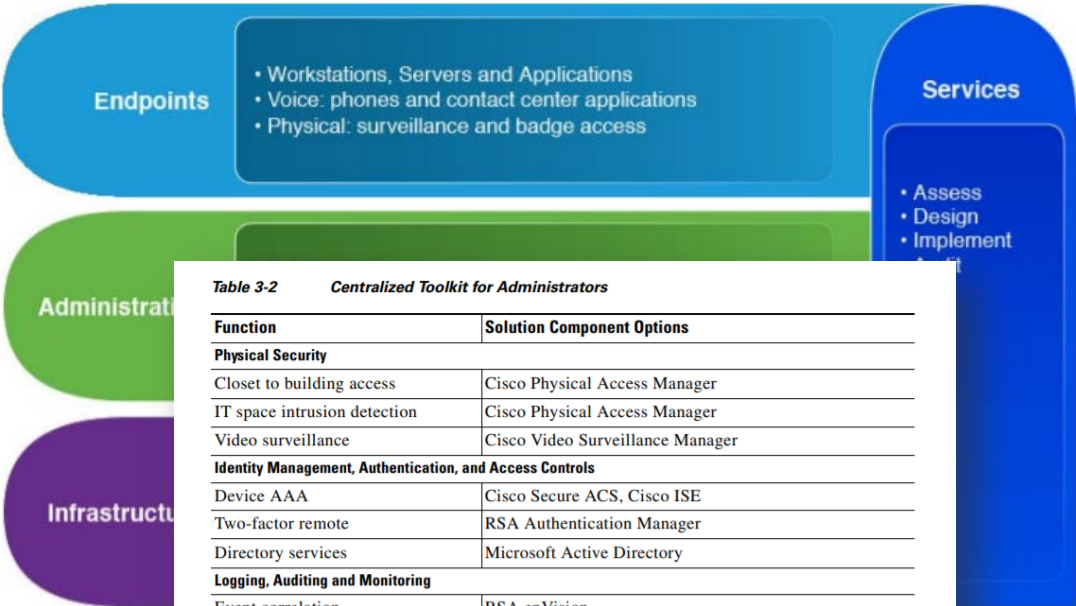


Table 3-2 Centralized Toolkit for Administrators

Function	Solution Component Options
Physical Security	
Closest to building access	Cisco Physical Access Manager
IT space intrusion detection	Cisco Physical Access Manager
Video surveillance	Cisco Video Surveillance Manager
Identity Management, Authentication, and Access Controls	
Device AAA	Cisco Secure ACS, Cisco ISE
Two-factor remote	RSA Authentication Manager
Directory services	Microsoft Active Directory
Logging, Auditing and Monitoring	
Event correlation	RSA enVision
Policy enforcement	Cisco Prime LAN Management Solution (LMS)
Corporate policy	RSA Archer
Virtualization	EMC Unified Infrastructure Manager, VMware vSphere
Encryption	
Storage	Cisco Key Manager, RSA Data Protection Manager
Remote access/VPN	Cisco Security Manager, Cisco AnyConnect VPN
Network Management	
Device configuration	Cisco Prime LMS
Security configuration	Cisco Security Manager
Wireless configuration	Cisco WCS

Cisco HIPAA Control Mapping

Healthcare Services & Corresponding Compliance Controls Located at Facility



Hospital/Clinic Service Types	Controls Recommended	Relevant Solution Products
Electronic medical records (EMR) systems	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Wired and wireless medical devices	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Imaging systems	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Wireless tablets and roll-around carts	Data encryption/decryption Auto-log-off controls Passwords	Cisco ISR, Cisco ASA, Cisco IPS appliance, Cisco Unified Wireless
Hospital/clinic LAN/WAN	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS Appliance
Patient registration workstations Nurse station workstations	Authentication controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Internet demarcation	Data encryption/decryption Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS Appliance

Cisco HIPAA Safeguard Area Mapping

Mapping Cisco to HIPAA Safeguards – Verizon Research



The Healthcare Security Requirements revolve around HIPAA Part 164 Part C. HIPAA Part 164 Subpart C is made up of nine sections.

Three of the sections are administrative and are not part of this assessment. **The remaining six sections (Security Standards: General Rules; Administrative Safeguards; Physical Safeguards; Technical Safeguards; Organizational Requirements; and Policies and Procedures and Documentation Requirements) consist of 52 Security Safeguards.**

Verizon performed an initial assessment to determine whether the safeguards could be met by using specific technology components provided by Cisco. Of the **52** Safeguards in the current healthcare requirements, Verizon identified **29 Safeguards as not applicable** in the context of this Assessment, because the Safeguard was either explicit and demanding direct (non-technology related) controls, or general but not allowing for the reasonable use of technology as a compensating control in the fulfillment of the Safeguard.

Of the remaining 23 Safeguard Areas in the current healthcare requirements, Verizon has further identified **8 Safeguards that call for universal security control requirements** that are foundational across Cisco's products and present in all network devices and systems that make up Cisco's Healthcare Reference Architecture.

Safeguard Areas where Cisco Security Controls are Not-Applicable	Safeguard Areas where Cisco Security Controls are Universally Applicable	Safeguard Areas where Cisco Security Controls are Specifically Applicable
29	8	15

Cisco Zero Trust Technology Portfolio

Portfolio enhancements that address cyber hygiene and program maturity



Product	Capability	Program Maturity				
		Basic	Intermediate	Good	Proactive	Advanced
1	2	3	4	5		
ESA/WSA	Advanced threat protection capabilities to detect, block and remediate threats					
Umbrella	Advanced defense and intelligence against threats					
Duo	Establish user trust w/multi-factor auth, SSO for SaaS and device visibility					
Cyber Vision	Threat detection/intelligence for cyber threats in the industrial networks					
AnyConnect	Remote access to network with visibility and posture compliance via agent					
SDA/ISE/TrustSec	Wired, wireless, VPN access policy with network segmentation					
Tetration	Threat detection/intelligence for threats in the private/hybrid clouds					
AMP/Threat Grid	Threat detection/intelligence with host visibility and remediation					
Stealthwatch	Threat detection with internal network and cloud visibility via flow sensors					
Threat Response	Threat visibility and rapid containment with intel-driven incident response					
Firepower	Network access, segmentation and threat detection with in-line insertions					

How We Help

Architecture, Design, Implementation, Run, Manage, Maintain



ceptional CARE

- Remote and Onsite Managed Services Support
- 24 x 7 Monitoring and Management of Desktop, Network, Phones, and Applications
- Multiple Support Levels to Fit Your Business, Budget
- Virtual CIO: Quarterly Technology Reviews and Reporting. Includes Strategic IT Planning, Updates to Plans, Standards, Maintenance, and Support Levels

ceptional CONNECT

- Design, Deployment, and Management of Telepresence and Video Solutions
- Voice, Video, and Web-based Conferencing
- Real Time Communications on all Devices
- Cloud, Onsite, and Hybrid Communications Solutions

ceptional CLOUD

- Strategic enterprise-class Data Center and Hosting Services. IT Software, Services, Applications, Email, and Network Solutions (Hosting, IaaS)
- Storage Solutions
- Backup & Recovery Solutions (BaaS)
- Compliance as a Service Solutions (CaaS)
- Virtualization

ceptional NETWORKS

- Networking Solutions Driving Technology and Business Operations
- Routers/Switches
- Wireless Mobility Solutions
- Security Solutions and Security as a Service
- WAN Optimization

Support and Monitoring Services

- 24x7 Monitoring and Alerting
- Managed Detection & Response (SIEM/SOC)
- Unlimited Helpdesk Support 6:00 a.m. – 6:00 p.m. M-F
- End Point Detection & Response with Anti-Virus and Patching
- Password Vault and Document Repository
- IT Asset Management
- Desktop/Email/Server Backups
- Mobile Device Management
- Single Sign On with Multifactor Authentication

Benefits

- Comprehensive Blanket IT Support, Security & CMMC Managed Services
- Predictable Cost Per User/Asset
- Access to Dedicated Engineers

IT Management, Consulting & Compliance Services

- Virtual CIO/CISO Strategy and Planning
- Hardware/Software Architecture, Design, Implementation, Resale
- Quarterly Security Assessments
- HIPAA Compliance Manager
- Performance Tuning
- End-User Security Training and Phishing Tests

HIPAA:

- ✓ Compliance Manager HIPAA One-time Set Up
- ✓ Annual Subscription
- ✓ HIPAA Compliance Manager Software
- ✓ Quarterly Scans
- ✓ Assessment Report Delivery
- ✓ 1 Hour Report Review/Recommendations Session

Reports & Assets Included:

- ✓ HIPAA Privacy Rule Worksheet
- ✓ HIPAA Breach Notification Rule Worksheet
- ✓ HIPAA Auditor Checklist
- ✓ HIPAA Policies and Procedures
- ✓ HIPAA Management Plan
- ✓ HIPAA Risk Analysis
- ✓ HIPAA Evidence of Compliance
- ✓ HIPAA Risk Analysis Update
- ✓ HIPAA Change Summary Report
- ✓ HIPAA Risk Management Plan Update
- ✓ HIPAA External Vulnerability Scan Detail
- ✓ Additional Supporting Documents & Worksheets



Wrap Up



Most healthcare executives or suppliers we speak to are seeking ways to reduce cyber attack risks, improve employee safety and productivity, while looking for highly efficient and cost-effective ways to address regulatory compliance while serving and supporting customers and patients.

The amount of time, energy, effort, and resources required to align IT systems and business processes with regulatory compliance is significant.

But you are not alone.

As a leading, award winning provider of Managed IT Services, Networking, and Security Solutions, Xceptional is committed to helping customers reduce risks and align their IT systems and applications to address regulatory compliance. We work collaboratively with clients to deploy effective and efficient IT solutions that support the current needs of their business, employees, and customers!

Embrace the Xceptional experience and [visit our website](#) or [contact us](#) today!



Thank You!

Visit our [resources page](#) to access our free eBooks and research!

Request a [complimentary network](#) or [security assessment](#) email us at info@xceptional.com

xceptional.com | 858-225-6230