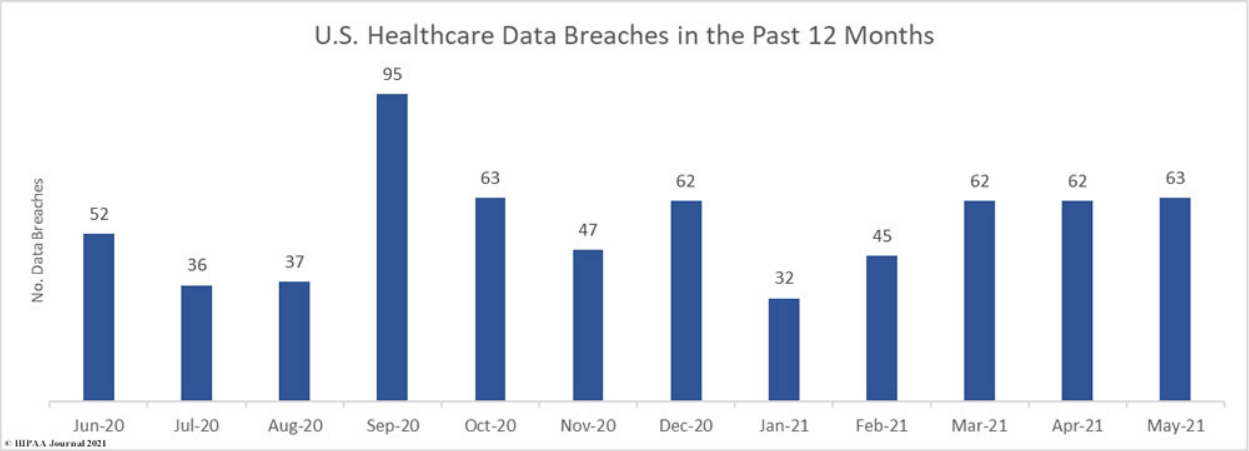
Investment Thesis Report: Healthcare Cybersecurity

August 2021

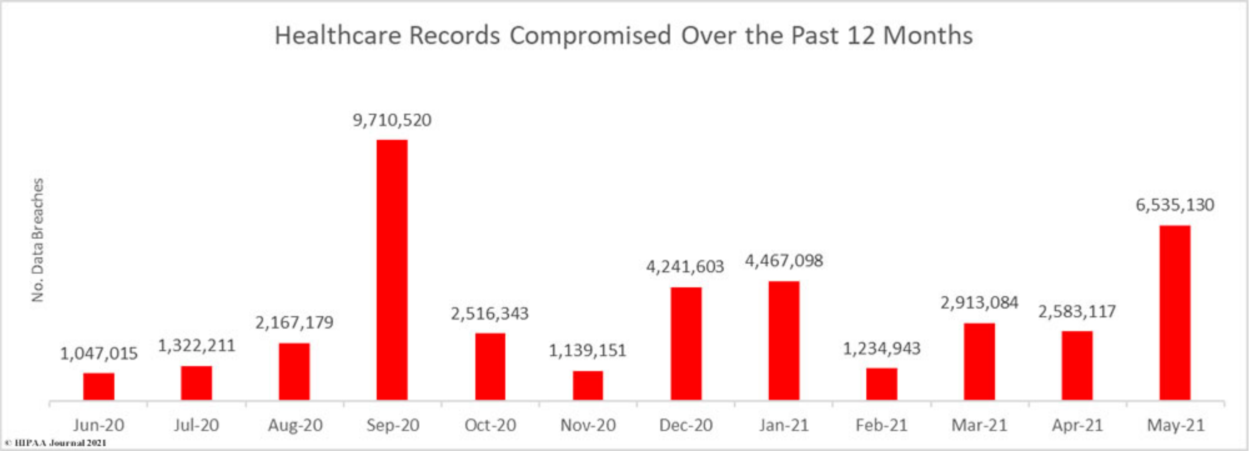
FCA VENTURE PARTNERS

Executive Summary

Healthcare uses cybersecurity to protect the electronic information and assets of hospitals, healthcare systems, medical homes, clinics, medical centers, and telehealth software. These protections are put in place to protect from illegal access, use, and disclosure of medical data and computerized materials. Cybersecurity in the healthcare industry and in other industries attempt to accomplish three goals called the CIA Triad: confidentiality, integrity, and availability.[1] In 2020 alone there were at least 560 attacks on healthcare facilities throughout 80 separate incidents. In addition, ransomware attacks are only expected to increase in 2021.[2] Ransomware is the most common and one of the most harmful cyberattacks. It is defined as a type of malicious software (malware) that threatens to publish or block access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim does not pay in time, the data could be gone forever.[3] With 264 attacks through May of 2021, we are well on our way to beating last year's numbers. So far 17,733,372 healthcare records have now been exposed or impermissibly disclosed in 2021 and almost 40 million records (39.87M) have been breached in the past 12 months.[4] Each individual record



does not represent one individual. One patient could have many records tied to their name. The increasing number of cyberattacks on the healthcare industry presents a unique opportunity for startups and companies to take advantage and solve a major problem affecting the industry at large.



© HIPAA Journal 2021

Healthcare’s Reliance on Technology

Cybersecurity has become vitally important to the healthcare industry as modernization and the advent of cheaper computing capabilities has led to the transfer of large amounts of information and systems to electronic platforms. Because of this transition over time, healthcare systems, hospitals, clinics, and other health organizations have become solely reliant on these technologies to run and operate their businesses. Some of the major systems that have become completely electronic are EHR systems, e-prescribing systems, practice management support systems, clinical decision support systems, radiology information systems, patient payment systems, and computerized physician order entry systems. In addition to these systems, many of the machines and tools used in these facilities are all included on the Internet of things. These include smart elevators, smart heating, ventilation and air conditioning systems, infusion pumps, remote patient monitoring, and other devices.[1]

Vulnerability of Telehealth and Telemedicine

Moreover, as telehealth and telemedicine continue to increase in popularity and availability, the importance and reliance on cybersecurity and these electronic systems only deepens. As COVID-19 has put stresses and restrictions on the healthcare industry, the need and use of telehealth has only increased. Although these events were just what telehealth and telemedicine needed to jumpstart their industry, the importance of cybersecurity and the protection of information has greatly increased. During the last year and a half, the Department of Health and Human Services released many restrictions and laws in communication apps, which have allowed telehealth services to begin to thrive. But with these regulations relaxed, comes more opportunity for cyberattacks and eavesdropping on private information and payments.[5]

Affected Parties

Patients

Patients are most vulnerable through their records and information that are stored in the healthcare systems, hospitals, and other databases that can be stolen or deleted. Patients need to know how to safely communicate and share information to their providers. They also need to be informed on how their providers store, use, and protect their information. Moreover, as telehealth becomes more popular and used throughout the public, patients need to make sure their connections with their providers are secure and that their providers have adequate security written into the software of the systems they are using.[1]

Workforce

Healthcare's workforce can be at the frontline of cyberattacks and cybersecurity in the industry. Each worker that deals with patient information and access to a database needs to have training on how to protect themselves and their patient's information from being illegally accessed. They also need to be aware of the threats and entry points of hackers and cyber criminals and know when and where to report these threats.[1]

C-Suite Executives

Many organizations will hire a chief information security officer (CISO) to make major cybersecurity decisions. They mainly work on strategy and coordination of the programs while leaving implementation and day to day operation of the programs to specific members of the cybersecurity team. The more time, effort, energy, and resources the c-level executives invest into cybersecurity and the protection of their electronic assets, information, and systems, the greater the top-down focus will be throughout each organization.[1]

Types of Cyberattacks

There are multiple types of cyberattacks that can all uniquely affect health organizations. The attacks include ransomware, data breaches, DDoS attacks, insider threats, business email compromise, and fraud scams.[6]

Ransomware

Ransomware attacks usually infect systems through phishing emails containing malicious links, a user clinking on a malicious link, and by viewing an advertisement containing malware (malvertising). Because of quickly evolving tactics, techniques, and procedures health organizations are having a tough time defending against these attacks and increasing the ease in which anyone with any level of technical skill can launch a cyberattack.[7] In addition to ransomware, hackers can also steal and/or just delete information. Credential sweepers steal usernames, passwords, and other tokens and wipers delete entire drives that can become unrecoverable.[1]

Data Breaches

Data breaches are becoming incredibly common in the healthcare sector. According to the Ponemon Institute and Verizon Data Breach Investigations Report, the healthcare industry has more breaches of data than any other industry. Data breaches can be caused by credential-stealing malware, providing patient data either accidentally or purposely, and misplaced devises and laptops. These attacks are increasing in number because the incentives to attack medical databases are higher than any other databases because Personal Health Information (PHI) is more valuable on the black market than either credit card information or Personally Identifiable Information (PII).

The reason behind PHI being more valuable than PII is that PHI cannot be changed unlike credit card and social security numbers which can.[8]

DDoS Attacks

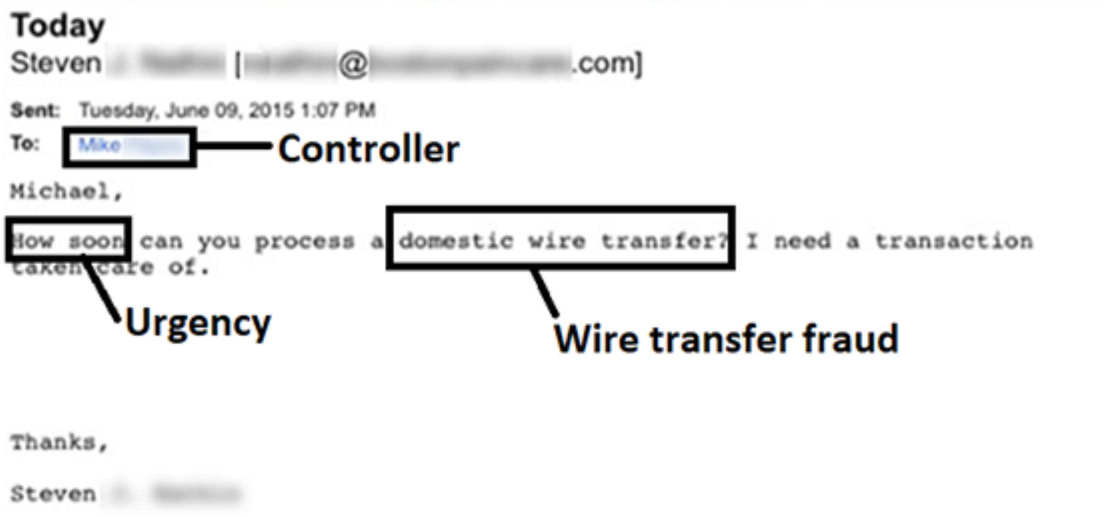
Distributed denial of service (DDoS) attacks are used by cybercriminals to overwhelm systems to make them not operational. When these attacks happen networks and systems can be shut down for weeks, not allowing the healthcare organization workforce to access the internet, information, records, prescriptions, or send or receive emails. These attacks come from hacktivists that are angered by a certain health organizations actions that victimize a certain individual or group of individuals that have been affected by some social, political, ideological, or financial discrepancy. These attacks can be opportunistic, purposeful, or even accidental.[9]

Insider Threats

In almost every case in the healthcare industry, cybersecurity teams can become so focused on external threats they can forget that insiders can pose an incredible vulnerability in their organization. An insider can pose a unique threat as they would most likely have legitimate access to the systems and networks of information to patients which would be able to bypass cybersecurity defenses including intrusion detection devices or physical security. In addition, they could have knowledge of weaknesses in the system or how the network works and is set up. These intentional criminals can provide codes or gain profit by selling PHI or PII information. The insider threat can also come accidently by a workforce member accidently clicking on a malicious link or losing a device.[10]

Business Email Compromise

Business Email Compromise, also known as the “Billion Dollar Scam” by the Federal Bureau of Investigation (FBI), are scams that come through the form of phony emails that trick the receiver to transfer money into a fraudulent account. Scammers send these emails to their targets posing as an important and powerful individual in the company like the CEO or CFO. These individuals usually do extensive research in attempting to replicate the language and styling of these executives and send the malicious emails to a select group of people that usually deal with the finances which allows the scammers to escape email filtering.[11]



Today
Steven [redacted] [[redacted]@[redacted].com]

Sent: Tuesday, June 09, 2015 1:07 PM
To: Mike [redacted]

Michael,

How soon can you process a domestic wire transfer? I need a transaction taken care of.

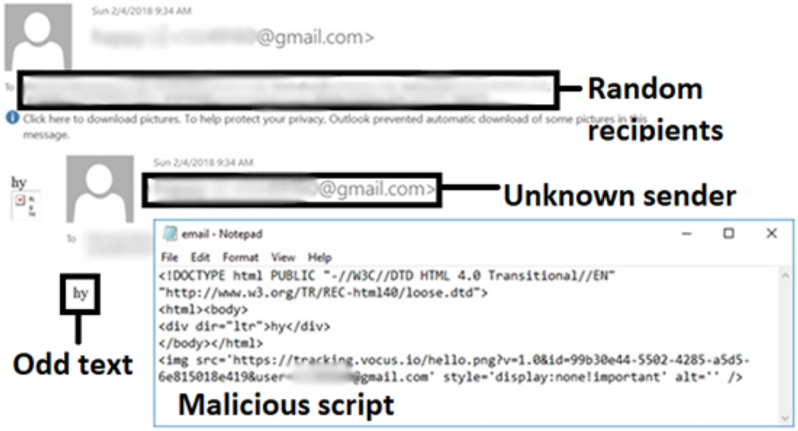
Thanks,

Steven [redacted]

Example of whaling email, source: HIMSS Cybersecurity Community

Phishing

Phishing is defined as a method of identity theft that relies on individuals unwittingly volunteering personal details or information that can be used for malicious purposes. It is often carried out through the creation of a fraudulent website, email, or text appearing to represent a legitimate firm.[12] Phishing is the most widely used initial point of compromise for cyberattacks. A user or group of users are targeted either randomly or specifically and are convinced into giving away sensitive information or clicking on a malicious link or attachment. As stated above, phishing is mostly used through email but can also be by way of websites, texts (Smishing), social media, phone calls, and other similar pathways. Some ways to tell that an email is malicious includes poor spelling and grammar (although not always), too good to be true claims, and language that conveys a sense of urgency or which preys on an individual's fear or greed. Alternatively, an online scam artist may send a spear-phishing email to a specific employee within an organization or to a specific department or unit within an organization. Unlike general phishing emails, spear-phishing emails are tailored to the targeted recipients. Spear-phishing tends to be more effective. Another form of spear-phishing is called whaling in which a cybercriminal will target a big fish like a C-suite level executive.[1]



Sun 2/4/2018 9:34 AM

[redacted]@gmail.com>

To [redacted]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

hy

Sun 2/4/2018 9:34 AM

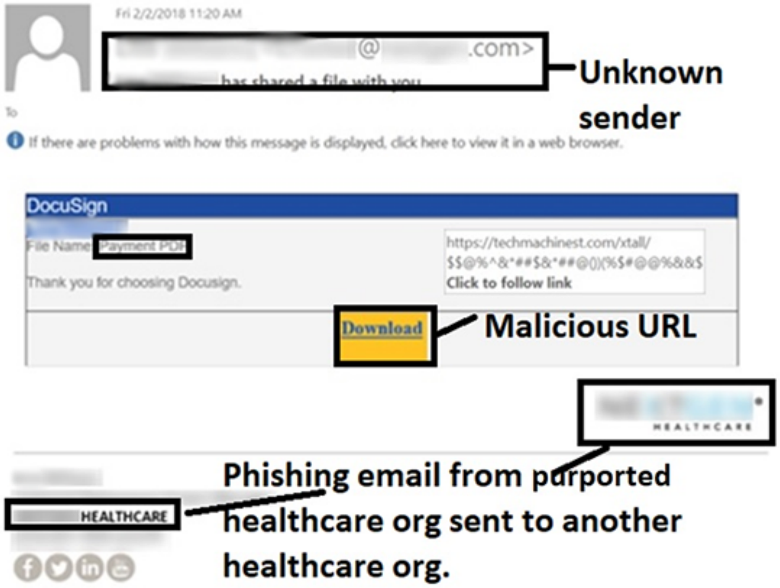
[redacted]@gmail.com>

To [redacted]

hy

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"
"http://www.w3.org/TR/REC-html40/loose.dtd">
<html><body>
<div dir="ltr">hy</div>
</body></html>
<img src='https://tracking.vocus.io/hello.png?v=1.0&id=99b30e44-5502-4285-a5d5-
6e815018e419&user=[redacted]@gmail.com' style='display:none!important' alt='' />
```

Example of general phishing email, source: HIMSS Cybersecurity Community



Fri 2/2/2018 11:20 AM

[redacted]@[redacted].com>

[redacted] has shared a file with you

To

If there are problems with how this message is displayed, click here to view it in a web browser.

DocuSign

File Name Payment PDF

Thank you for choosing Docusign.

https://techmachinest.com/xtall/
$$@%^&*##$&*##@()(%$#@@%&&$
Click to follow link

[redacted] HEALTHCARE

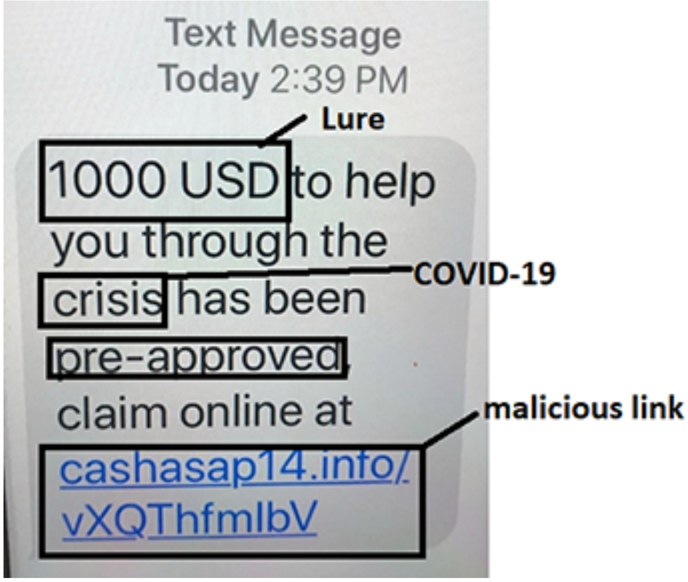
[redacted] HEALTHCARE

Unknown sender

Malicious URL

Phishing email from purported healthcare org sent to another healthcare org.

Example of spear-phishing email, source: HIMSS Cybersecurity Community



Text Message
Today 2:39 PM

1000 USD to help you through the crisis has been pre-approved, claim online at cashasap14.info/vXQThfmlbV

Lure

COVID-19

malicious link

Example of SMiShing, source: HIMSS Cybersecurity Community

Illegal Use of PHI

Patients' Personal health Information (PHI) can be stolen by cybercriminals and sold on the dark web. PHI records include the following information:

- Names
- Dates, except year
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers
- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Any unique identifying number or code[13]

As stated above, these records and sets of information are much more valuable than plain personal information like credit cards and social security because they cannot be changed. Gary Cantrell, head of investigations at the HHS Office of Inspector General, said hackers tend to steal medical records because they are like "a treasure trove of all this information about you." They contain a patient's full name, address history, financial information, and social security numbers—which is enough information for hackers to take out a loan or set up a line of credit under patients' names, according to Computerworld. Hackers also focus on medical records because hospitals and health care organizations are often easy to hack.[14] Once these criminals get the information they are looking for, there are multiple uses for it. The most popular use of this information is to sell if for a profit on the black market. The selling price of these PHI records can go for upwards of $1000. The buyers of these records use the information to create fake IDs to purchase medical equipment or drugs, or to file a false insurance claim. When these records are stolen it can create havoc for the patient. It can take years, even decades to manage the effects it has on one’s credit records, personal finances, and medical legitimacy.

Risk Assessments and Security Controls

Risk assessments and gauges are incredibly important to healthcare organizations. These assessments can be crucial in deciding what controls need to be put in place and how much of a risk there is to the information and assets of these organizations. Risk must be gauged based upon factors such as probability of occurrence, impact on the organization, as well as the prioritization of the risk. Risk assessments should be conducted or reviewed regularly and at least once per year.[1]

Security controls are the main defenses of any system or database that holds assets, information, or runs computer systems of healthcare organizations and other businesses. One should have both basic and advanced defenses. The basic defenses protect against weaker threats that do not have the wherewithal to break into the systems and are an organization’s first line of defense. Advanced security controls protect against the main threats of cyberattacks and are the most secure measures in cybersecurity. An organization should have a defense-in-depth strategy in their cybersecurity. Meaning that if one control fails another will automatically back it, creating a multilayer defense of important data and information. A robust incident response plan is necessary for cybersecurity in healthcare so that any security incidents that occur are either blocked or tackled in a timely and expeditious manner.[1]

Listed below is a grid listing basic and advanced security controls.[1]

Basic Security Controls	**Advanced Security Controls**
Anti-virus	Anti-theft devices
Backup and restoration of files/data	Business continuity and disaster recovery plan
Data loss prevention	Digital forensics
Email gateway	Multi-factor authentication
Encryption at rest	Network segmentation
Encryption for archived files/data	Penetration testing
Encryption in transit	Threat intelligence sharing (also called information sharing)
Firewall	Vulnerability scans
Incident response plan	
Intrusion detection and prevention system	
Mobile device management	

Policies and procedures
Secure disposal
Security awareness training
Vulnerability management program/patch management program
Web gateway

HIPAA Laws and Regulations

The Health Insurance Portability and Accountability Act (HIPAA) is a federal requirement in the U.S. which applies to covered entities and business associates. HIPAA is comprised of three major rules: the HIPAA Privacy Rule, Security Rule and Breach Notification Rule.[1]

The HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164, sets forth permitted and required uses and disclosures of protected health information. The protected health information may exist in any form, including on paper, film and in electronic form. Protected health information is a form of individually identifiable health information.[1]

The HIPAA Security Rule, 45 CFR Part 160 and Part 164, Subparts A and C, sets forth requirements for electronic protected health information. In other words, the confidentiality, integrity and availability of electronic protected health information must be maintained by covered entities and their business associates.[1]

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.[1]

HIPAA covers health plans, healthcare clearinghouses, and healthcare providers who electronically transmit health information connected with transactions for which the U.S. Department of Health and Human Services has standards. Covered entities include physician practices, ambulatory surgical centers, hospitals, long-term care facilities, health plans, healthcare clearinghouses, and others. Business associates perform functions or services on behalf of covered entities. Business associates may create, receive, transmit, or maintain protected health information on behalf of the covered entity. Examples of business associates include accountants, attorneys, cloud service providers, document storage companies, third party billing services and others.[1]

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. The severity of the breach is judged based on these things:

I. The extent to which the risk to the protected health information has been mitigated.

II. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.

III. The unauthorized person who used the protected health information or to whom the disclosure was made.[1]

The three exceptions to the definition of a breach are:

I. The covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

II. The inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized healthcare arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

III. The unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.[1]

In addition, covered entities must establish business associate agreements with their business associates. HIPAA is enforced by the U.S. Department of Health and Human Services Office for Civil Rights (OCR). OCR has the authority to interpret and enforce HIPAA. Accordingly, it is best for to keep up with guidance from OCR as it relates to the interpretation and enforcement of HIPAA.

Companies in Healthcare Cybersecurity

To remedy the threats of cybercriminals, many companies have been created and funded specifically to provide cybersecurity to healthcare organizations. These companies range from startups to publicly traded companies and have a wide range of offerings. Most companies that work in healthcare cybersecurity specialize in the Healthcare space like Clearwater and Health Linkages, but others like Battelle serve the healthcare industry alongside other industries. Some of the services that the following companies provide include data encryption and protection, blockchain encryption and safety, integrated artificial intelligence, and much more.[15]

Companies to Watch

BATTELLE

Develops and translates the latest advances in prevention, treatment, and analytics into better outcomes for people everywhere.

Headquarters: Columbus, Ohio

Provides a suite of cyber security services for medical devices with expertise in cybersecurity, medical device design and development, and user experience

Not only provide security to health organizations but also to government entities including industries from homeland security to energy development; provide commercial offerings and lab management

private nonprofit applied science and technology development company
(Crunchbase)
5781 employees (LinkedIn)

United States
https://www.battelle.org/

bitglass

Enables enterprises to embrace the cloud while ensuring data secuirty and regulatory compliance by securing data across any cloud app and any device. [16]

Headquarters: Campbell, CA

Provide multiple cloud app protection including everything from Office 365 to Dropbox; provide app security, encryption, cloud and mobile security management, shadow IT discovery

Developing Secure Access Service Edge (SASE) technology, in which organizations can extend consistent security to all enterprise resources from a single control point.

Raised \$150.1M since 2013
\$70M Series D lead by Quadrille Capital
\$45M Series C (Crunchbase)
166 employees (LinkedIn)

United States
https://www.bitglass.com/

ClearDATA

SECURE · HEALTHCARE · CLOUD

Managed cloud provider for healthcare and life sciences security. Advanced healthcare PHI security and HIPAA compliance services for AWS environments.

Headquarters: Austin, TX

Platform allows automated safeguards, remediations, and line of sight to real-time compliance reporting, assists your team in the identification, management and use of PHI/PII

Is partnered with Amazon, Google, Azure and more to provide automated safeguards; have 70+ cloud services and 230+ technical controls

\$80.4M raised since 2012
\$26M Series E lead by Humana (Crunchbase)
\$12M Series D lead by Flare Capital Partners
202 employees (LinkedIn)

United States
https://www.cleardata.com/

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Healthcare compliance and cyber risk management solutions. Empowering health organizations to manage healthcare's evolving cybersecurity risks, compliance requirements, and ensure patient safety.

Headquarters: Nashville, TN

Software, Managed Services, and Consulting to Avoid Preventable Breaches, Protect Patients and Their Data, Meet Regulatory Requirements, and Optimize Cybersecurity Investments

Provide consulting and cybersecurity management to a diverse group of small and large firms; rated first for risk analysis risk management past 4 years

Founded 2010, private (Crunchbase)
85 employees (LinkedIn)

United States
https://clearwatercompliance.com/

CyberMaxx.

Prevents, detects and responds to cybersecurity attacks for healthcare organizations; expands capabilities to avoid cyberattacks and mitigate loss

Headquarters: Nashville, TN

Proactive defense, response, and prevention of cyber-attacks; ensure endpoint security, handle containment, and remediation; around the clock security monitoring and cloud computing

Provide services to over 1000 healthcare facilities and 40% of major hospital systems in the US; tailormade experiences for each organization that is custom fit for each system

$30M raised since 2001
$20M funding from Relyens Group (Crunchbase)
33 employees (LinkedIn)

United States
https://www.cybermaxx.com/

CyberMDX

Suite that is a comprehensive solution set that addresses Biomedical Engineers, IT Security, IT Networking, Complinace, and C-Suite Managmnet.

Headquarters:
New York, NY

Provides 360-degree visibility by network inspection using Layer7 medical protocol expertise and AI; assesses the risk of each medical device, factoring in exposures, attack potential, operational criticality.

?

Have a layered architecture and approach for asset inventory and tracking, ricks assessment and preventive care, detection and response, and compliance and governance

$

$30M raised since 2017
$20M Series B lead by Sham (Crunchbase)
$10M Series A lead by Pitango and Qure Ventures
63 employees (LinkedIn)

United States
https://www.cybermdx.com/

CYLERA™

Provides network security solutions powered by machine learning to provide zero-day protection from malware and exploits, especially focused on the medical device space.

Headquarters:
New York, NY

Provide platform that encompasses all of a health system's cybersecurity portals and protection; can analyze, edit, and report on all one's information

?

Through their all-encompassing platform, they provide asset management, risk analysis, smart segmentation, threat defense, operational analytics, and government and compliance

$

$17M raised since 2017
$10M Series A lead by Concord Health Partners (Crunchbase)
31 employees (LinkedIn)

United States
https://www.cylera.com/

CYNERGISTEK®

Cybersecurity and information management dedicated to serving the healthcare industry. Helping organizations achieve privacy, security, compliance, and document output goals.

Headquarters:
Austin, TX

Provide security risk assessment, privacy program assessment, compromise assessment, and medical device security assessment

?

Cybersecurity consulting offers services that assess risks, build cyber resilience, and validate controls; have ongoing program management

$

Publicly traded company
Ticker: CTEK (Crunchbase)
94 employees (LinkedIn)

United States
https://cynergistek.com/

Cynerio

Provider of healthcare IoT cybersecurity and asset management solutions; pre-empting threats with automated risk reduction and attack prevention tools.

Headquarters:
New York, NY

Provide medical device IoMT, enterprise IoT, OT systems, information security, biomedical engineering, and executive cybersecurity management

?

Uses an in-house threat intelligence team that utilizes an AI system to deliver real-time alerts on new vulnerabilities and step-by-step mitigation and remediation plans.

$

$37M raised since 2001
$30M Series B lead by ALIVE Israel HealthTech Fund (Crunchbase)
51 employees (LinkedIn)

United States
https://www.cynerio.com/

DataMotion

Enabling providers to communicate more efficiently across the care continuum and with their patients. Secure messaging and connectivity solutions for secure and compliant exchange of (PHI).

Headquarters:
Florham Park, N.J

ADT Notifications, Secure messaging, Secure clinical information exchanges, payment plans, secure data transfer

?

In addition to healthcare cybersecurity, they provide finiacial services in simplifying client interactions, public sector communication security, and mobile file sharing app

$

$3.3M raised since 2000
$2M Series B lead by Raghu Sugavanam (Crunchbase)
42 employees (LinkedIn)

United States
https://datamotion.com/

Fortified
HEALTH SECURITY

Healthcare organization with effective solutions to mitigate cybersecurity and compliance risks. Services include assisting with compliance with state and federal regulations.

Headquarters:
Franklin, TN

Offer purpose-built strategies, services, and tools like advisory services, Healthcare Security Operations Center, and Threat Assessment & Incident Response

?

Stress that their completive advantage is that they focus on healthcare specifically making them better equipped to serve healthcare organizations

$

Privately held, no funding (Crunchbase)
67 employees (LinkedIn)

United States
https://fortifiedhealthsecurity.com/

imperva

Provide healthcare security to safeguard sensitive patient data, secure medical applications and devices; also provide cybersecurity for finiacial services, telecom, and retail

Headquarters:
Redwood Shores, CA

Provide active data monitoring, web application firewall, and cloud data security; ensures compliance with healthcare regulations

?

Protect the data of over 6,000 global customers from cyberattacks through all stages of their digital transformation across many industries including healthcare, financial services, telecom, and retail

$

$94.4M raised since 2003
$22M Venture round (Crunchbase)
$13M Series B led by ForgePoint Capital
1513 employees (LinkedIn)

United States
https://www.imperva.com/

imprivata®

Healthcare IT security solutions company enabling healthcare to access, communicate, and transact patient information, securely and conveniently.

Headquarters:
Lexington, MA

Provide services of identity protection and authentication, enterprise single sign on, mobile IAM, positive patient ID, risk analytics and intelligence, and secure healthcare communications

?

They have a tailored approach that provides two major broad based services of advisory and management that they can edit and customize based on the client

$

$45M raised since 2002
Acquired by Thoma Bravo (Crunchbase)
612 employees (LinkedIn)

United States
https://www.imprivata.com/

Ostendio

Cloud-based cybersecurity and information management platform; alllows healthcare providers to show information security compliance to multiple industry standards and regulations.

Headquarters: Arlington, VA

Provides a one-stop-shop platform that delivers risk management, training, assessment, asset management, validation, document management, incident management, and breach response

Their MyVCM is an integrated cybersecurity platform that works in conjunction with all business operations to deliver perpetual security that's always on, always secure, and always auditable.

$957K raised since 2014
Series A led by Osage Venture Partners (Crunchbase)
26 employees (LinkedIn)

United States
https://www.ostendio.com/

PROTENUS

Protect patient data security with alerts to suspicious activity in the electronic health record (EHR). Mitigate risk and public exposure, reinforce trust enterprise-wide, and enhance patient privacy.

Headquarters: Baltimore, MD

Provide services including patient privacy protection that reduces privacy violation through AI and drug diversion surveillance that tracks movement of substances and identifies misuse and abuse

This is an active niche in the market. Maize Analytics, a provider of healthcare data governance solutions and similar to Protenus, was recently sold to SecureLink system[17]

$57.2M Raised since 2014
$21M Series D (Crunchbase)
105 employees (LinkedIn)

United States
https://www.protenus.com/

Opportunities in Healthcare Cybersecurity

As 2021 continues, the number of cyber attacks and hacks will continue to increase. And as health organizations gradually become aware of these threats, two specific occurrences will happen. The first is that healthcare organizations will begin to hire healthcare cybersecurity companies to protect their data, information, and systems. The second is as security increases so will the skills of cybercriminals thus increasing the threat and abilities of these hackers. Through these two events over the broadscale of the healthcare industry, many opportunities will open for startups to emerge in the healthcare cybersecurity space. And as startups emerge, therein creates the opportunities for venture capital funds to invest and profit off their successes.

Works Cited

1. https://www.himss.org/resources/cybersecurity-healthcare
2. https://www.hipaajournal.com/at-least-560-u-s-healthcare-facilities-were-impacted-by-ransomware-attacks-in-2020/
3. https://www.proofpoint.com/us/threat-reference/ransomware
4. https://www.hipaajournal.com/may-2021-healthcare-data-breach-report/
5. https://academic.oup.com/jamia/article/28/3/671/6039104
6. https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/
7. https://www.cisecurity.org/blog/ransomware-in-the-healthcare-sector/
8. https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/
9. https://www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/
10. https://www.cisecurity.org/blog/insider-threats-in-the-healthcare-sector/
11. https://www.cisecurity.org/blog/business-email-compromise-in-the-healthcare-sector/
12. https://www.investopedia.com/terms/p/phishing.asp
13. https://www.hipaajournal.com/considered-phi-hipaa/
14. https://www.advisory.com/en/daily-briefing/2019/03/01/hackers
15. https://cybersecurityventures.com/healthcare-cybersecurity-companies-list/
16. https://security.healthcaretechoutlook.com/vendors/top-healthcare-cybersecurity-companies-2018.html
17. http://www.brentwoodcap.com/maize-analytics-is-acquired-by-securelink/

FCA | VENTURE PARTNERS

FCA Venture Partners is a venture capital firm investing in early-stage healthcare technology and technology-enabled healthcare services companies that improve patient care, reduce costs, and increase efficiency. FCA manages over $100M and invests across the Series Seed to Series B stages. Our firm brings portfolio companies valuable healthcare insights, connections, and board-level experience to accelerate growth and build disruptive and sustainable businesses. Based in Nashville, the epicenter of healthcare innovation, with a strategic network in Charlotte and Winston-Salem, NC, our team has a decades-long track record including more than 60 investments in the rapidly changing healthcare industry.