yubico

Modern strong authentication and compliance for Healthcare Organizations

How the YubiKey helps Healthcare Organizations meet regulatory requirements

Contents

Authentication in Healthcare

Overcoming obstacles to digital transformation

61%

of data breaches are traced back to credentials

Over the past decade, healthcare organizations have adopted digital tools to improve patient and population health. In reaction to this digital transformation, we are seeing new and revised health regulations that are changing expectations for ensuring the security and privacy of protected health information (PHI).

While the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires "reasonable" physical, technical, and administrative safeguards for data security and authentication, the lack of standards has meant that many healthcare organizations have continued to rely on passwords.[1] However, with 61% of data breaches traced back to credentials in some way, it is clear that passwords are no longer the answer.[2]

The COVID-19 pandemic put pressure on healthcare organizations to ramp up to increased patient load, but exceptions were made to the HIPAA Security Rule to keep organizations up and running through the pandemic, which are now becoming problematic.[3] Since 2020, healthcare organizations have seen an increase in cyber attacks and data breaches. The risks of remote and virtual services, including care and clinical trials, need to be addressed for security and for compliance. As we will illustrate in this white paper, regulatory change is on the horizon—and strong multi-factor authentication is likely to be a part of this change.

Strong authentication can be challenging for healthcare organizations, including healthcare payers, providers, pharmaceutical, and service providers. Despite the myriad of regulatory and internal pressures to protect the privacy and security of PHI and the secrecy of intellectual property (IP), common obstacles to improving authentication include infrastructure complexity, shared or BYOD devices, cost, sanitation, and workflow challenges.

The YubiKey, a FIPS 140-2 validated hardware security key, has emerged as a convenient and scalable solution for modern strong authentication across a variety of healthcare situations.

$9.23 Million

average cost of breach, the most expensive industry[9]

2X

more cyberattacks on healthcare in 2020 compared to 2019[10]

28%

of attacks in healthcare were ransomware[11]

Evolving cyber attack landscape

Healthcare is one of the most highly targeted industries by cyber criminals, due in part to the high value of PHI as well as the potential for a quick ransomware payout. There is no question that the events of the global COVID-19 pandemic made the situation worse, as reflected by a 55.1% increase in breaches in 2020.[4]

The transition to remote work introduced new weaknesses, including unsecured home networks, unpatched devices, shared devices, and weak/reused passwords. In 2020, cyber attacks in healthcare rose to 239.4 million attempted attacks; of this number, there were 816 attempted attacks per endpoint—a 9,851% increase from 2019.[5]

Data breaches in any organization are costly, but in healthcare the costs can be devastating. While the healthcare industry faces the highest average cost of a data breach, $9.23 million, this cost does not reflect the impact an IT failure or ransomware threat can have on patient care.[6] Just recently, we saw Germany explore the potential link between a patient death and a ransomware event.[7] In 2018, a Finland-based private psychotherapy practice covered up a cyber attack on its patient record system. That breach led to an extortion attack two years later in which patients were directly targeted by cyber criminals (not to mention the subsequent bankruptcy and total collapse of the practice)[8]. In the pharmaceutical industry, the loss of IP can directly impact the race to market and set R&D back by years.

Cyber attacks come in many forms, from malware and DDoS attacks to phishing and ransomware. Credentials are the most sought after type of data in the initial phase of a cyber attack, with threat actors moving laterally to find sensitive and valuable data or compromise systems.

> “Unfortunately, the complexity and challenge to secure health care is daunting. We face all the threats of other industries, things like phishing, malware propagation, identity theft, insider threats and more. To that, we can add the targeting of health devices and the systems providing patient care, a large percentage of which is legacy and outdated technology. To compound the difficulty, cyber criminal adversaries appear unwilling to give us a break; they are more than willing to risk harming patients and to profit from misery.[12]
>
> **–Esmond Kane, CISO of Steward Health Care**

SolarWinds & Blackbaud attacks underscore supply chain risk

In 2020, a major threat actor backed by the Russian government penetrated thousands of organizations. It created a backdoor in the SolarWinds Orion Software, which in turn installed malware to spy on over 18,000 product customers, including hospitals and technology companies, opening up the risk for further supply chain risk.[13] 2020 also saw the hack and attempted ransomware of cloud provider Blackbaud that has been linked to over 100 healthcare data breaches and affected over 12.3 million patient records.[14]

The SolarWinds attack went undetected for months, in part due to the supply chain attack method used to move laterally between systems and gain additional privileges. Similarly, the Blackbaud attack began on February 7th 2020, but went undetected until May and uncommunicated until July 2020.[15]

Of note in the SolarWinds attack is the supposed misuse of Identity and Access Management (IAM) systems like single sign on, network logon systems, SAML/OAuth/OIDC federation systems, and the like.

With SolarWinds and Blackbaud, and many other breaches, you'll find that stolen credentials cause the initial breach. Once the attacker gains access to the victim's environment, they diversify their access to help maintain a persistent foothold.

> "It is unsettling to know that hackers are not only eager to take advantage of the pandemic crisis, but that they're feeding off of a highly profitable supply chain of stolen digital assets to do so. While hospitals are the target, the patient is ultimately the true victim of this cyber attack machine.
>
> **– David Sygula for CPO Magazine[16]**

In this whitepaper, we will take a look at existing and emerging regulations and how the YubiKey, a FIPS 140-2 validated and NIST 800-63 AAL3 authenticator, can help healthcare organizations rapidly and seamlessly deploy modern strong authentication take an immediate stand against cyber attacks while preparing for tomorrow's compliance challenges.

> For years, achieving a balance between high security and ease of use was near impossible, but new authentication technologies are finally bridging the gap. With the availability of passwordless login and security keys, it's time for the healthcare industry to step up their security options.
>
> **– Stina Ehrensvärd, Yubico CEO and Co-Founder**

Modern strong authentication with the YubiKey

The solution

YubiKey is the **only** solution that is proven to stop 100% of account takeovers in independent research.[17]

Smart Card/PIV

Out-of-the-box native integration for the Microsoft environment using Smart Card/PIV functionality based on the NIST SP 800-73 specification.

FIDO2 & FIDO U2F

Strong two-factor, multi-factor and passwordless authentication public key crypto to protect against phishing, session hijacking, man-in-the-middle, and malware attacks.

One time passcodes

Integrate Yubico OTP natively with the free YubiCloud authentication service or program unique TOTP or HOTP secrets.

Legacy multi-factor authentication solutions including mobile authentication such as SMS, OTP, and push notifications are better than just username and passwords, but are still not 100% effective against mitigating risks from evolving cyber risk vectors. In comparison, hardware security keys based on modern FIDO protocols are proven to stop successful phishing attacks and account takeovers in their tracks.

The YubiKey is a hardware security key manufactured by Yubico, that offers easy-to-use two-factor, multi-factor, and passwordless authentication at scale, helping healthcare organizations be compliant to MFA requirements across various regulations, certifications, and frameworks. Organizations receive a choice of FIPS 140-2 validated keys Overall Level 1 (Certificate #3907) and Level 2 (Certificate #3914), Physical Security Level 3, and can also avail of the YubiKey Bio Series - FIDO Edition, a gold standard in biometric authentication.

With the YubiKey, healthcare organizations can:

- Stop account takeovers and prevent man-in-the-middle attacks with superior hardware cryptographic security
- Provide unmatched simplicity for users with 4x faster logins that ensure proof of presence and possession
- Comply with existing and emerging regulations such as HIPAA, GDPR, and 21 CFR Part 11
- Support secure remote access and secure access to Electronic Health Records (EHRs)
- Support pharmaceutical use cases, including NFC for sterile environments and clean rooms, and the storage of SAFE-BioPharma certified identity credentials

By supporting multiple authentication protocols on a single YubiKey, such as OTP, OpenPGP, and strong authentication protocols such as Smart Card, FIDO U2F and FIDO2/WebAuthn, the YubiKey offers healthcare organizations the flexibility to deploy strong authentication using a single key across a variety of legacy and modern infrastructures.

To authenticate, users simply plug their security key into their desktop or laptop and touch to authentication, or tap their security key against devices such as a tablet or a phone. Where sterile environments are important, the YubiKey can be combined with a wearable to leverage NFC communication for a touchless authentication experience.

YubiKeys can be used to stop phishing attacks and account takeovers for a variety of internal and patient use cases including privileged users such as doctors, nurses and pharmacists, call center workers, hybrid and remote workers, virtual patient health, electronic prescriptions, data sharing, and virtual R&D.

Healthcare regulatory compliance

How the YubiKey for modern strong authentication addresses regulatory requirements

Only 51.2%

of healthcare organizations believe their security program is successful in meeting compliance regulations[18]

The healthcare industry is subject to strict security requirements and an increasing regulatory burden. The number of global regulations continues to increase, with new changes emerging to industry frameworks and standards as well as state, federal and global levels.

The YubiKey helps healthcare organizations comply with existing and emerging regulations with modern, strong authentication that offers highest-assurance two-factor, multi-factor, and passwordless authentication. The following sections outline the various healthcare regulations and the YubiKey capabilities that help organizations satisfy regulatory requirements related to authentication.

HIPAA

HIPAA Security Rule, HITECH, & HIPAA Safe Harbor

The Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, includes base standards for the security and privacy of protected health information (PHI), further supported by its final Security Rule in 2003, the HITECH Act (Health Information Technology for Economic and Clinical Health) of 2009, and the most recent HIPAA Safe Harbor Bill of 2021.

In the HITECH act, a data breach in healthcare is defined as the "unauthorized acquisition, access, use, or disclosure of protected health information," (Sec. 13400 1A) clearly underscoring the importance of authentication in the provisioning of access.[19] The most recent Safe Harbor Bill asks regulators to consider the NIST framework when looking at audits and fines, placing the strict NIST standards as the new goal post for authentication.[20]

Requirement	Section	YubiKey capabilities
Facility Access Controls	HIPAA 4.10	• Hardware-backed MFA access controls • Centralized authorization policies to control access • YubiKey as smart card • MFA through multiple protocols - Something you know: PIN (FIDO2, SmartCard) - Something you have: private key stored on the YubiKey • Support password / PIN for MFA (FIDO U2F, FIDO2 or OTP)
Workstation Security	HIPAA 4.12	
Access Controls	HIPAA 4.14	

Requirement	Section	YubiKey capabilities
Person or Entity Authentication	HIPAA 4.17	• Hardware-backed MFA access controls • Centralized authorization policies to control access • YubiKey as smart card • MFA through multiple protocols (Smart Card, OTP, FIDO U2F, FIDO2, OpenPGP) • Support password / PIN for MFA (FIDO U2F, FIDO2 or OTP)
Ensuring security methods to ensure appropriate authorization	HITECH 3001 3(A)(iv)	
Recognition of security practices, including the NIST Cybersecurity Framework	Safe Harbor Sec. 13412	• Multiple-protocol support • OTP, OATH, HOTP, U2F, PIV, Open PGP • 2FA and MFA options • Multi-factor cryptographic device • Hardware-based authenticator

What's next for HIPAA?

While HIPAA began with merely "reasonable" physical, technical, and administrative safeguards for data security and authentication, there has been a push to see greater specificity. In addition to the new 2021 Cybersecurity Safe Harbor Provision, there are proposed modifications to the HIPAA Privacy Rule, providing patients with greater access to data, potentially introducing new risks and vulnerabilities.[21]

The NIST (National Institute of Standards and Technology) provides guidance for HIPAA implementation, but this document dates to 2008, pre-dating many of the more recent NIST special publication (SP) requirements, including those of SP 800-63 and SP 800-53 (Security and Privacy Controls for Information Systems and Organizations). NIST is preparing to update its HIPAA guidance for the first time in 10 years.[22]

The NIST Cybersecurity Framework suggests strong authentication, including a multi-factor combination of something a user *owns*, *knows*, and *is*. NIST further clarifies these in SP 800-63, Digital Identity Guidelines. Currently, only 44% of healthcare organizations adhere to NIST.[23] YubiKey is an AAL3 certified authenticator, providing the highest level of confidence.

NIST

With HIPAA transitioning toward NIST, let's take a look specifically at the NIST cybersecurity framework standards around authentication.

Standard	NIST SP | FIPS	YubiKey capabilities	YubiKey certification level
Digital identity guidelines define authenticator assurance level (AAL)	SP 800-63	• Multiple-protocol support OTP, OATH, HOTP, FIDO U2F, PIV, Open PGP • 2FA and MFA options • Multi-factor cryptographic device • Hardware-based authenticator • Touch-button test of user presence	AAL3
Guidelines for the protection of controlled unclassified information	SP 800-171	• Hardware-backed MFA access controls • YubiKey used as smart card • Centralized authorization policies to control access	
Security and privacy controls for information systems and organizations	SP 800-53	• YubiKey used as smart card • Centralized authorization policies to control access	
Security requirements for cryptographic modules	FIPS 140-2	• Cryptographic module supports multiple protocols • YubiKey used as smart card • Touch-button test of user presence • Time or hash-based synchronous OTP • FIDO U2F, FIDO2	• Overall Level 1 #3907 • Overall Level 2 #3914 • Physical Security Level 3 #3517

21 CFR Part 11

The Code of Federal Regulations (CFR) establishes regulations on electronic records and electronic signatures (ERES) under the FDA, with Part 11 defining which controls, systems, audits, measures, signatures, and documentation are acceptable for pharmaceutical development and medical device manufacturing.[24] The regulations were updated in 2020 specifically to address the minimum requirements for systems used to process digitally signed orders.[25] Other minimum requirements related to validation and audit have been provided in supplementary guidance.[26]

Requirement	Section	YubiKey capabilities
Limit system access to authorized individuals	§ 11.10 (d) ; (k)	• Hardware-backed MFA access controls • YubiKey used as smart card • Centralized authorization policies to control access
Electronic signatures and system access, validation	§ 11.10 (a) ; (h)	• Hardware-backed MFA access controls • YubiKey used as smart card

The SUPPORT Act / EPCS

In 2018, a revised SUPPORT Act aimed to better control opioid abuse with the introduction of Section 2003, a requirement to use an EPCS (Electronic Prescription for Controlled Substances) application for the prescribing of controlled substances under Medicare Part D. The amended SUPPORT Act came into effect on January 1, 2021, with CMS delaying enforcement of penalties under an extended grace period to January 1, 2022.[27]

In addition to the SUPPORT Act at the Federal level, 24 states have State-Specific EPCS requirements, with several other states with upcoming and proposed legislation set to roll out in 2021 and beyond.[28]

Requirement	Section	YubiKey capabilities
Identity controls	85 FR 47154	• 2FA and MFA options • Multi-factor cryptographic device • Hardware-based authenticator • Touch-based test of user presence
Digital signature with cryptographic module of at least FIPS 140-2 Security Level 1	85 FR 47154 §1311.08	• Hardware-backed MFA access controls • YubiKey used as smart card • Multi-factor cryptographic device • FIPS Level 2+

Requirement	Section	YubiKey capabilities
Two-factor authentication with FIPS 140-2 Security Level 1 hard token with 2FA at minimum	85 FR 47154, §1311.115	• 2FA and MFA options • Multi-factor cryptographic device • Hardware-based authenticator • FIPS Level 2+ • Touch-button test of user presence • MFA through multiple protocols (Smart Card, OTP, FIDO U2F, FIDO2, OpenPGP)
Hard token must be FIPS 140-2 Security Level 1 and be separate from the mobile device for access	DEA Statement on Mobile Devices for EPCS[29]	• FIPS Level 2+ • Cryptographic module supports multiple protocols • YubiKey used as smart card • Touch-button test of user presence • Private key stored on the YubiKey

CURES Act Final Rule

The ONC Cures Act Final Rule (the 21st Century Cures Act), was designed to support greater access and exchange of electronic health information.[30] The following requirements apply to any Health IT Module currently looking to meet the Certified Health IT Product requirements.

Requirement	Section	YubiKey capabilities
Encrypt authentication credentials	§ 170.315(d)(12)	• Multi-factor cryptographic device • Private key stored on the YubiKey
Multi-factor authentication (MFA) consistent with NIST SP 800-63B	§ 170.315(d)(13)	• 2FA and MFA options • Multi-factor cryptographic device • Hardware-based authenticator • Validated to NIST SP 800-63-3 AAL 3 requirements • MFA through multiple protocols (Smart Card, OTP, FIDO U2F, FIDO2, OpenPGP)

GDPR

The European Union General Data Protection Regulation (GDPR) came into effect in 2018, mandating that organizations that offer goods or services (including healthcare) to EU citizens meet data protection and privacy standards, provided those healthcare organizations have more than 250 employees. GDPR fines are among the most severe—4% of global annual turnover or €20 million, whichever is higher.[31] There are no exceptions for healthcare organizations that are compliant with HIPAA.

> Authentication is key to securing computer systems and is usually the very first step in using a remote service or facility, and performing access control.
>
> **–European Union Agency for Cybersecurity (ENISA)[32]**

Requirement	Section	YubiKey capabilities
Data protection impact assessment	Article 35	• Hardware-backed MFA access controls • Centralized authorization policies to control access • Multi-factor cryptographic device
Security of processing	Article 32	
Data protection by design and by default	Article 25	

CCPA, 23 NYCRR 500 & other state laws

The California Consumer Privacy Act (CCPA) was the first US-based data privacy bill to adopt stringent measures in line with the GDPR. Followed by the California Privacy Right Act (2023) amendment, which introduces even more requirements, other states are following suit, including the recent Virginia Consumer Data Protection Act (CDPA), which comes into effect January 1, 2023.[37]

These regulations require financial institutions to implement “appropriate” and “reasonable” precautions to protect and secure data.[38]

Main Features

Hardware-backed MFA access controls

- Something you know: PIN (for FIDO2, Smart Card)
- Something you have (Private key stored on the YubiKey)

Support password / PIN for MFA (FIDO U2F, FIDO2 or OTP)

> Having strong authentication is a foundational security component of a Zero Trust architecture. Yubico and YubiKeys help fill the gap, for example, where weak passwords have been used, by providing validated, phishing-resistant security keys.
>
> **–John Kindervag, Creator of Zero Trust**

U.S. executive order on improving the Nation's cybersecurity (EO)

The recent number of attacks on critical systems has triggered increased regulatory pressure from the U.S. Federal government. On May 12 2021, the Biden administration issued an Executive Order 14028 on "Improving the Nation's Cybersecurity."[37]

This new order requires agencies and organizations in the public and private sector who work with the government, including financial services. The order includes the requirement to adopt Zero Trust frameworks within 60 days, as well as multi-factor authentication and encryption for data at rest and in flight within 180 days.[38]

The Zero Trust emphasis in the order demonstrates the high priority status the government is placing on modernizing agencies' infrastructure. Strong, modern authenticators, like the YubiKey, will be essential to reaching Zero Trust goals while providing a low-friction and secure user experience.

Main Features

Hardware-backed MFA access controls

YubiKey used as smart card

Centralized authorization policies to control access

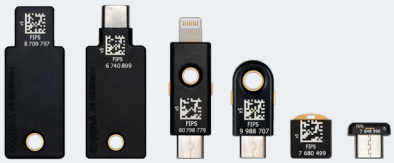
What's next in healthcare regulation?

The pace of regulatory change has accelerated in response to changes in technology and risk. While legislative change may take years to pass and move into enforcement, rapid change can come about in the form of executive order (EO). In response to the pressures of COVID-19, the growth of virtual health and virtual clinical trials, we expect to see new or revised regulations in the next several years. Keep the following regulations on your radar:

- H.R.2013 - Information Transparency & Personal Data Control Act39
- S.1842 - Protecting Personal Health Data Act40
- CURES 2.0 - Currently in concept, could require the FDA to create guidance on the use of digital endpoints and decentralized trials[41]

The YubiKey 5 Series

From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.



The YubiKey 5 FIPS Series

From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS.

The YubiKey Bio - FIPS Series

From left to right: YubiKey Bio USB-A and YubiKey Bio USB-C

> By integrating directly with the Yubico SDK, Allscripts is improving the multi-factor authentication (MFA) experience that is needed to comply with the electronic prescription of a controlled substance (EPCS).
>
> **–Steve Pascht, Allscripts Senior Solutions Manager**

YubiKeys offer a bridge to passwordless for healthcare organizations

It is clear from the cyber attack landscape that passwords are no longer the answer. It is also clear that healthcare regulations are recognizing this fact, with a clear move toward strong authentication such as FIDO2—true passwordless authentication. However, going passwordless is a journey, not an overnight transition.

With the YubiKey, healthcare organizations can implement FIDO2 passwordless, smart card passwordless or a hybrid strategy, depending on the infrastructure and use cases that need to be addressed. As the passwordless ecosystem continues to expand, YubiKeys are perfectly designed to help financial organizations bridge the transitory period from modern strong MFA to passwordless. YubiKeys support the broadest set of authentication protocols, enabling a single security key to work across a wide range of applications and services, regardless of where healthcare organizations are in their strong authentication and passwordless journey.

Yubico offers the fastest way to meet today's complex compliance and security requirements, while accelerating your journey to passwordless. Take a stand against cyberattacks and future-proof your compliance stance with the YubiKey.

CASE STUDY

How Allscripts achieved EPCS compliance with the YubiKey

Due to the complex compliance requirements and fast-moving nature of hospitals or other healthcare environments, it's important that doctors, nurses, and medical staff have quick, yet secure, access to critical systems and information. However, mobile devices are a source of privacy risk in healthcare, responsible for up to 25% of breaches in previous years.

Mobile phones are not purpose-built for security. They are multi-purpose computing devices that, by nature, have a larger attack surface. An external, single-purpose authentication device like the YubiKey significantly minimizes the level of risk exposure to malware or phishing attacks.

Allscripts, a leader in healthcare information technology solutions, is actively working with the Yubico Android SDK to make YubiKey support available in its Allscripts Sunrise™ Mobile and Allscripts Professional™ EHR Mobile and Desktop.

"By integrating directly with the Yubico SDK, Allscripts is improving the multi-factor authentication (MFA) experience that is needed to comply with the electronic prescription of a controlled substance (EPCS)," said Steve Pascht, Allscripts Senior Solutions Manager. "It's easier for providers to use hard tokens on mobile and desktop platforms by simply plugging in—and eventually tapping—the YubiKey without having to read, remember, re-type, or copy and paste OTP codes when prescribing controlled substances."

YubiKey authentication is up to four times faster than copying and pasting one-time codes. Not only is this a more preferred and enjoyable user experience, but it has also been shown to reduce support costs by up to 92%.[42]

Summary

Due to the growing threat of cyber attacks, healthcare regulations are moving to adopt strong zero trust frameworks, with all signs pointing to strong authentication in line with NIST SP 800-63.

Today, globally accepted standards such as FIDO2/WebAuthn are helping healthcare organizations and their supply chains to combat the threats of cyber attacks such as phishing, ransomware, and account takeovers.

Easy, efficient, strong authentication is finally a reality with the YubiKey. Designed to be cost effective, user friendly, and portable, the YubiKey provides a modern, strong authentication solution for the most highly sensitive patient information, for the strict requirements of digital identity verification in sterile environments, and EPCS requirements for e-prescribing.

Trust the YubiKey to secure your healthcare organization and supply chain.

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088

Sources

[1] Enzoic, Recommendations for HIPAA Password Compliance, (March 23, 2020), https://securityboulevard.com/2020/03/recommendations-for-hipaa-password-compliance/

[2] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

[3] Amanda Lennon, COVID-19 and HIPAA Enforcement Discretion Leaves Healthcare Organizations Vulnerable to Ransomware Attacks, (April 1, 2021), https://www.carbonblack.com/blog/covid-19-and-hipaa-enforcement-discretion-leaves-healthcare-organizations-vulnerable-to-ransomware-attacks/

[4] Bitglass, Healthcare Breach Report 2021, (Accessed June 10, 2021), https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q1HealthcareBreachReport2021.pdf

[5] Samantha Mayowa, The State of Healthcare Cybersecurity: VMware Carbon Black Explores the Surge in Cyber Threats, (February 3, 2021), https://www.carbonblack.com/blog/the-state-of-healthcare-cybersecurity/

[6] IBM, 2021 Cost of Data Breach Report, (Accessed May 13, 2021), https://www.ibm.com/security/data-breach

[7] Reuters, Prosecutors open homicide case after cyber-attack on German hospital, (September 18, 2020), https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital

[8] Computer Weekly, Hacked Finnish Therapy Business Collapses, (February 2021) https://www.computerweekly.com/news/252496227/Hacked-Finnish-therapy-business-collapses

[9] IBM, 2021 Cost of Data Breach Report, (Accessed May 13, 2021), https://www.ibm.com/security/data-breach

[10] IBM, X-Force threat Intelligence Index 2021, (Accessed June 9, 2021), https://www.ibm.com/downloads/cas/M1X3B7QG

[11] IBM, X-Force threat Intelligence Index 2021, (Accessed June 9, 2021), https://www.ibm.com/downloads/cas/M1X3B7QG

[12] CISCO, "Health Care Security In Focus," (Accessed May 17, 2021), https://www.cisco.com/c/dam/en/us/products/collateral/security/threats-year-report.pdf#page=28

[13] Kevin Poulsen et. al., Solar Winds Hack Victims: From Tech Companies to a Hospital and University, (December 21, 2020), https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402

[14] Paul Bischoff, Ransomware attacks on US healthcare organizations cost $20.8bn in 2020, (March 10, 2021), https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

[15] Paul Clolery, The Hack of Blackbaud: Damage is Still Being Assessed, (August 6, 2020), https://www.thenonprofittimes.com/npt_articles/the-hack-of-blackbaud-damage-is-still-being-assessed/

[16] David Sygula, Inside the Cyber Attack "Machine": What Hospitals Need to Know about the Dark Web and Post-Pandemic Threats, (April 22, 2021), https://www.cpomagazine.com/cyber-security/inside-the-cyber-attack-machine-what-hospitals-need-to-know-about-the-dark-web-and-post-pandemic-threats/

[17] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[18] Cisco, Security Outcomes Study: Healthcare Sector (Accessed May 14, 2021), https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-outcomes-study-healthcare-mini-report.pdf

[19] Public Law 111-5, (February 17, 2009) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

[20] Mike Semel, Implement NIST CSF for a HIPAA Safe Harbor, (March 10, 2021), https://www.rapidfiretools.com/blog/2021/03/10/implement-nist-csf-for-hipaa-safe-harbor/

[21] HHS, Extension of the Public Comment Period for Proposed Modifications to the HIPAA Privacy Rule, (March 9, 2019), https://www.hhs.gov/about/news/2021/03/09/extension-public-comment-period-proposed-modifications-hipaa-privacy-rule.html

[22] NIST, SP 800-66 Rev. 2 (draft), (April 29, 2021), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

[23] Cynergistek, 2020 Annual Report, (September 17, 2020), https://insights.cynergistek.com/reports/2020-annual-report

[24] US FDA, 21CFR11, (April 1, 2020), https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1&subpartNode=21:1.0.1.1.8.2

[25] US FDA, CFR - Code of Federal Regulations Title 21, (April 1, 2020), https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=1311.55

[26] US FDA, Guidance for Industry Part 11, Electronic Records, (August 2003), https://www.fda.gov/media/75414/download

[27] CMS, Final Rule, (December 1, 2020), https://www.cms.gov/newsroom/fact-sheets/final-policy-payment-and-quality-provisions-changes-medicare-physician-fee-schedule-calendar-year-1

[28] Josh Vogt, What States Require EPCS & How Your Practice Can Stay Compliant, (Accessed June 9, 2021), https://blogs.meditab.com/discover-the-essentials-of-mandatory-epcs-compliance

[29] US Department of Justice, Use of Mobile Devices in the Issuance of EPCS, (August 16, 2018), https://www.deadiversion.usdoj.gov/GDP/(DEA-DC-8)%20Use%20of%20Mobile%20Devices%20in%20the%20Issuance%20of%20EPCS.pdf

[30] ONC, ONC's Cures Act Final Rule, (Accessed June 10, 2021), https://www.healthit.gov/curesrule/

[31] European Commission, Data Protection, (Accessed June 10, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

[32] ENISA, Privacy and Data Protection by Design - from policy to engineering, (January 12, 2015), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[33] Moritt Hock & Hamroff LLP, Virginia Becomes the Second State to Pass a Comprehensive Privacy Law, (March 24, 2021), https://www.jdsupra.com/legalnews/virginia-becomes-the-second-state-to-2607391/

[34] Intersoft Consulting, General Data Protection Regulation, (Accessed May 19, 2021), https://gdpr-info.eu/art-32-gdpr/; National Law Review, CPRA Security Risk Assessments & Privacy Compliance, (November 6, 2020), https://www.natlawreview.com/article/cpra-security-risk-assessments-privacy-compliance

[35] Matthew M. Shatzkes, Julia K. Kadish, What Virginia's New Privacy Law Means for Organization in the Healthcare Industry, (March 8, 2021), https://www.natlawreview.com/article/what-virginia-s-new-privacy-law-means-organizations-healthcare-industry

[36] Kirk Nahra, How emerging privacy laws are impacting the health care industry, (January 28, 2020), https://iapp.org/news/a/how-emerging-privacy-laws-are-impacting-the-health-care-industry/

[37] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[38] David Treece, Quick Take: Executive Order on Improving the Nation's Cybersecurity, (May 13, 2021), https://www.yubico.com/blog/quick-take-executive-order-on-improving-the-nations-cybersecurity/

[39] Congress.gov, H.R. 2013, (April 1, 2019), https://www.congress.gov/bill/116th-congress/house-bill/2013/text

[40] Congress.gov, S.1842, (June 13, 2019), https://www.congress.gov/bill/116th-congress/senate-bill/1842

[41] Kat Jercich, Cures 2.0 could be 'well on the way' by spring, say DeGette and Upton, (December 8, 2020), https://upton.house.gov/uploadedfiles/cures_2.0_concept_paper_final.pdf

[42] Yubico, Google defends against account takeovers and reduces IT costs, https://www.yubico.com/resources/reference-customers/google/

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.

© 2021 Yubico