yubico

HEALTHCARE WHITE PAPER: JAN 2021

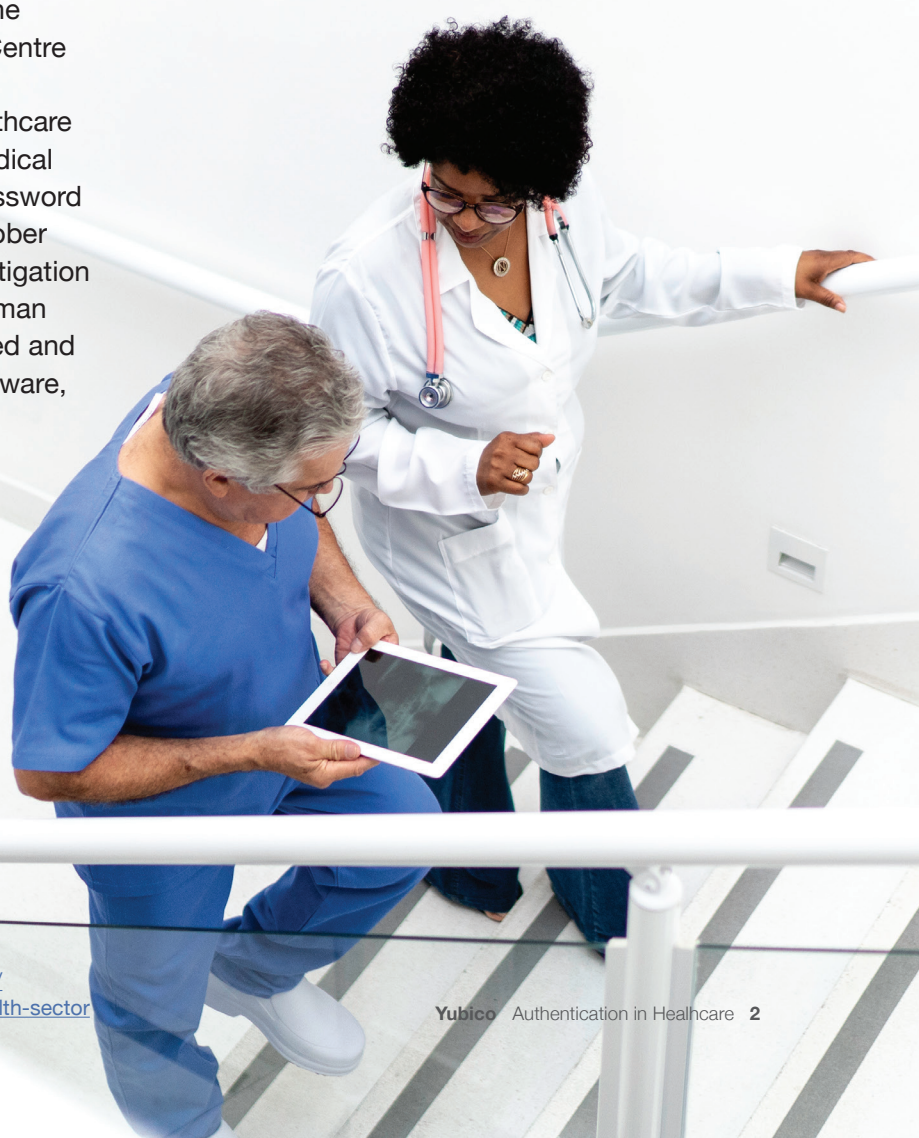
Best practices for strong authentication in healthcare using the YubiKey

The need for strong authentication in healthcare

Since early 2020, the healthcare industry has undergone a significant digital transformation. Whether it's remote work, increased e-health adoption such as electronic prescriptions, telemedicine, and electronic payments, or even virtual collaboration on vital drug and vaccine research, healthcare organizations are transforming to improve patient outcomes.

At the same time, the healthcare industry has also seen an increase in cyber attacks. On May 20 2020, the United States Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), and the United Kingdom's National Cyber Security Centre (NCSC) released a joint alert on advanced persistent threat (APT) groups targeting healthcare bodies, pharmaceutical companies, and medical research organizations using large-scale password spraying campaigns.[1] More recently, on October 28, 2020, CISA, the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) released an alert on increased and imminent cybercrime threat, namely ransomware, to U.S. hospitals and healthcare providers.[2]

Credential phishing attacks, the primary vehicles for successful account takeovers, can have damaging effects including leveraging the credentials to deliver ransomware and providing unauthorized access to e-health systems and data such as patient records, personal information and credit card data. Any successful account takeover can result in non-compliance with industry regulations such as Health Insurance Portability and Accountability Act (HIPAA), and Electronic Prescriptions for Controlled Substances (EPCS) which can carry significant penalties.



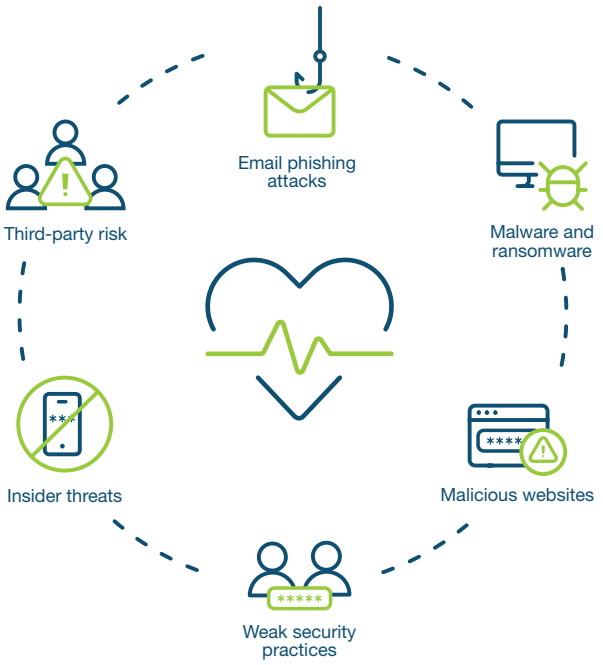
[1] https://us-cert.cisa.gov/ncas/alerts/AA20126A

[2] https://us-cert.cisa.gov/ncas/current-activity/2020/10/28/ransomware-activity-targeting-healthcare-and-public-health-sector

Common cyber threats and vulnerabilities across the healthcare industry

Common cybersecurity threats and vulnerabilities targeted at healthcare organizations can lead to account takeovers, if strong authentication isn't deployed.

- **Email phishing attacks:**
  Seemingly legitimate, but malicious emails are sent to users to obtain usernames and passwords. Spear-phishing emails, which can often be effective, are highly tailored toward the individual being targeted.
- **Malware and ransomware:**
  As defenses against common malware payload delivery mechanisms have improved such as email attachment filtering, criminals have increasingly turned to phishing and account takeovers as the first step in multi-phase attacks. Cyber criminals use malware, including ransomware, to take over individual devices, servers or even entire networks to steal data, credentials, etc. In a ransomware attack, users are typically prevented from accessing their system or files until a ransom is paid or credentials divulged.
- **Malicious websites:**
  Cyber criminals create websites similar to reputable sites in order to install malware to steal usernames and passwords, that are then commonly delivered via email phishing attacks.
- **Weak security practices:**
  Employees can leave organizations susceptible to attack through poor security hygiene including weak passwords, shared passwords, and reuse of passwords across multiple accounts including personal accounts.
- **Insider threats:**
  The 2020 Verizon Data Breach Investigations Report lists internal actors as the second highest cause of breaches in healthcare (48%), not far behind external threat actors (51%).[3] In areas such as call centers, where agents are trusted with access to highly sensitive data, insider threats pose significant risk. It is crucial that mobile devices not be used for authentication in such environments where protected health or personal information can be captured with a camera and sold to malicious actors.
- **Third-party risk:**
  Many healthcare providers outsource services such as catering, payroll, and web development to third-party and even fourth-party vendors. These vendors often have access to shared sensitive information, which can be vulnerable to attack if not properly secured.



[3] 2020 Verizon Data Breach Investigations Report

What is strong authentication?

With the industry moving toward a zero trust security framework where nothing is trusted inside or outside the perimeter, and instead all connections must be verified before granting access, authentication becomes a key component of any zero trust architecture. EPCS regulations at the federal and various state levels mandate using two-factor authentication and strong access controls to help mitigate security risks. While HIPAA did not include a similar mandate when it was written, the reality of today's threat landscape is that strong authentication has become a necessity to meet the "reasonable and appropropriate security measures" required by the law. But many organizations are still using weak legacy authentication mechanisms, such as username and password, and SMS/email authentication. Others are using higher-security options internally such as smart cards with NFC readers which doesn't meet the portability needs of today's mobile workforce and potentially leaves them exposed externally. However, the healthcare industry's typically complex and legacy infrastructure in combination with remote work technology has led to varied two-factor authentication (2FA) and multi-factor authentication (MFA) usage.

But what exactly is strong authentication and how can it protect against account takeovers?

Strong authentication has two main qualities:

- It does not rely solely on shared secrets process or protocol (symmetric keys) at any point: This includes passwords, OTP, SMS codes, and recovery questions.
- It robustly repels credential phishing, Man-in-the-middle attacks (MitM) and impersonation: Strong authentication assumes some attacks will reach the end user and the authentication mechanism will prevent the attack from being successful.

Among the varied authentication protocols, only smart card and modern FIDO U2F and FIDO2/WebAuthn protocols are in fact strong authentication. In addition, it's also important to consider usability and scalability of MFA solutions. Poor user experiences, and low portability and scalability, can introduce lack of adoption and drive up cost.

Not all authentication is created equal

Username and password	Basic 2FA: SMS, email, mobile	YubiKey: strong authentication
Deployed everywhere	Not purpose-built for security	Purpose-built for security
Known usability gaps	Uses existing technology stacks that are vulnerable to network and software attacks	No network connection, stored data, or client software required
Costly and hard to sustain	Common target for credential phishing	Highly phishing resistant
Common target for credential phishing		

Better security and usability with the YubiKey

To reduce the risk of phishing attacks and to stop account takeovers Yubico provides the YubiKey—a hardware security key that provides strong multi-factor authentication at scale. It is the only solution that is proven to stop account takeovers 100% in independent research.[4] 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 better security compared to username/passwords and mobile-based authenticators, as well as high portability and usability. It also lowers administrative overhead with broader platform support compared to traditional smart card solutions.

The YubiKey as a highly portable root of trust works across multiple devices such as desktops, laptops, mobile, tablets and notebooks without requiring a battery or internet connection. The YubiKey can also be used for strong authentication to any healthcare system or device that has USB and NFC capabilities, making it ideal to secure healthcare infrastructure and computing systems that clinicians use.

With the YubiKey for strong authentication:

- Frontline healthcare workers and clinicians like doctors and nurses can simply tap/touch to securely and quickly sign in to EHR systems, shared workstations, and e-prescribing for access to patient records, and be more productive in their day-to-day jobs—even remotely.
- Healthcare providers can stay compliant to industry regulations and improve business efficiencies by eliminating password related IT support costs, remain in compliance with industry regulations, and serve more patients more quickly.
- Patients can gain secure access to their online health information and e-prescriptions and also get peace of mind that their personal data and health records stay protected against cybercriminals.

[4] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Best practices for strong authentication using the YubiKey

1. **Compliance with HIPAA, HITECH and EPCS**
   HIPAA requires appropriate safeguards for protecting electronic protected health information (ePHI). Lost or stolen ePHI data, or unauthorized access to ePHI makes healthcare organizations liable to fines, and any breach must be reported under Health Information Technology for Economic and Clinical Health Act (HITECH) rules. EPCS requires confirmation of the identity of providers, and identity verification in order to sign prescriptions.

   Per Drug Enforcement Agency (DEA) guidelines, any state that permits the use of e-prescribing will follow DEA guidelines for EPCS regardless if there is state legislation in place. DEA guidelines around the electronic prescription of controlled substances state that any hardware devices being used for authentication must meet Federal Information Processing Standard (FIPS) 140-2 Security Level 1.

   YubiKeys are FIPS 140-2 validated to meet the highest authentication assurance level 3 requirements (AAL3) of NIST SP800-63B guidelines. Using YubiKeys for strong MFA helps healthcare organizations conform with EPCS requirements for e-prescribing. Healthcare organizations can also use YubiKeys for strong access controls and authentication for systems storing patient data and ePHI, to stay compliant with HIPAA.

2. **Protect Electronic Health Record (EHR) applications**
   Healthcare organizations using an EHR or other electronic technology for collection and use of ePHI, must comply with HIPAA Security Rule and Meaningful Use requirements. Additionally, protecting patients' privacy and securing their health information stored in an EHR is a core requirement of the Medicare and Medicaid EHR Incentive Programs. These protections are essential regardless of whether the EHR is installed on a server in the office or hosted by a cloud service provider (CSP).

   Using YubiKeys for strong MFA for EHR systems as an additional layer of verification to user identities ensures that only authorized individuals can gain access to systems containing ePHI, as stated in HIPAA 164.308(a)(4)(ii)(B). By validating user presence with the tap/touch of the YubiKey, physicians and other clinicians can securely access EHR applications from their own devices or even shared devices/workstations. This user presence verification ensures that it's not a remote attacker or malware trying to login.

3. **Secure remote access to patient data**
   Many healthcare employees have been working remotely since early 2020 due to COVID-19, but still need access to systems and data including clinician and research databases, test results, financial data, organizational data, image archives, pathology slides, and more.

Enabling MFA should be one of the top requirements in a distributed or remote workforce environment. The YubiKey offers an easy-to-use, durable, and multi-function solution for all employees regardless of device type, operating system, or location. YubiKeys can be used to enable MFA for identity access management (IAM) systems and identity providers (IdPs) such as Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, PingID, and RSA SecurID® Suite. The YubiKey in conjunction with IAM vendors and IdPs can also be used for Single Single On (SSO) to other business critical messaging or video conferencing apps such as Microsoft Teams, Google Hangouts, and Zoom.

Many healthcare organizations use Virtual Desktop Infrastructure (VDI) for remote employees such as Citrix and VMware. Access to these can be secured using the YubiKey.

YubiKeys can also be used to ensure secure VPN access to the healthcare provider network. Pulse Secure and Cisco AnyConnect can be configured to work with a YubiKey as a smartcard (PIV) for remote access. Other VPN applications that offer native support for YubiKeys use the one-time password (OTP) capabilities.

Other best practices to secure remote access include leveraging the smart card functionality of the YubiKey and using the YubiKey in addition to a PIN to lock down access to a computer, as well as to step up authentication for password managers.

4. **Secure access for call center agents**
   Given the sensitive Electronic Health Information (EHI), account information, health and payment data accessible to call center agents, securing access to that data is critical. The use of mobile phone based authenticators within call centers poses particular challenges due to security, productivity, and compliance risks. Using mobile devices for 2FA can provide call center employees with a means to easily capture sensitive data on camera without being noticed—putting healthcare organizations at great risk.

   Hardware security keys such as the YubiKey are ideal for call centers. By eliminating the dependence on mobile phones, call centers can ensure that agents cannot capture images of customer and financial data such as account numbers, SSN numbers, credit card information, and numerous details that might violate customer privacy. Restricting the use of mobile phones also helps improve call center productivity.

5. Protect connected medical (IoMT) devices

Connected medical devices or Internet of Medical Things (IoMT) devices such as infusion pumps, imaging systems, patient monitors, point of care analyzers, medical device gateways and ECG systems among others, are highly susceptible to hacking if proper security and access controls aren't implemented. Medical devices typically connect to a large array of sensors and monitors, and can act as a potential entry point for a cyber criminal into a healthcare providers' IT network. The 2018 Annual Zingbox Threat Report on Medical Devices notes that US hospitals typically have 10-15 connected devices per bed. Due to their long life cycles, connected medical devices can pose a serious security risk if their operating systems aren't routinely patched or upgraded, or if they are still using default manufacturer supplied passwords.[5] The 2020 Unit 42 IoT Threat Report found that 83% of medical imaging devices run on unsupported operating systems, a 56% jump from 2018.[6]

YubiKeys ensure strong 2FA and MFA security for connected medical devices by adding a hardware-backed security authentication layer in addition to username and password. This prohibits unauthorized access to connected medical devices, and helps prevent account takeovers even if weak or manufacturer-set passwords are in use.

[5] Zingbox 2018 Annual Threat Report Medical Devices

[6] 2020 Unit 42 IoT Threat Report

6. **Secure patient access to healthcare and insurance systems**

   Timely access to providers is crucial in the healthcare industry. Inadequate medical care can have serious consequences, yet patient access to care can be difficult due to various circumstances. This underlies the importance for telehealth. Patients want to be able to access their healthcare on an on-demand basis - when they need it. Healthcare organizations have been tapping telemedicine to close care gaps caused by geographic barriers. Many smaller facilities in rural areas also use telemedicine to connect with experts in more urban areas, keeping patients from having to travel great distances to receive intensive or specialized care.[7]

   The YubiKey can be deployed for MFA to telehealth applications, healthcare websites and insurance and payment systems empowering patients and ensuring secure access and use of their data. Having timely and secure electronic access to health information makes it easier for people to make more informed decisions about their healthcare needs.

7. **Protect clinical research and pharmaceutical supply chains**

   The pharmaceutical and clinical research sectors rely heavily on virtual collaboration across geographies and organizations. This has never been more apparent with the current COVID-19 crisis. Additionally, the pharmaceutical industry relies on foreign sourcing for critical components, materials, and finished products, as identified in the U.S. Department of Commerce's Office of Technology Evaluation's 2011 report, 'Reliance on Foreign Sourcing in the Healthcare and Public Health (HPH) Sector: Pharmaceuticals, Medical Devices and Surgical Equipment.'[8] Unless every supplier within the clinical research and pharmaceutical supply chain is strongly secured against account takeovers and other cyber attacks, foreign actors and nation states can get easy access to proprietary and confidential information.

   The YubiKey is simple to implement making it easy for all agencies across supply chains to deploy strong authentication. YubiKeys feature modern protocols like FIDO2 and WebAuthn, as well as OTP, SmartCard (PIV), OpenPGP, earlier FIDO versions, and more. A single YubiKey supports multiple applications, allowing the keys to work with current applications and authentication methods in addition to advanced and emerging protocols. Users also have the ability to store their SAFE-BioPharma certified identity credentials on the YubiKey to ensure high-assurance identity trust for cyber transactions.

2020 redefined the healthcare industry—making strong authentication a cybersecurity necessity

COVID-19 accelerated digital transformation across the healthcare industry, increasing adoption of telehealth, online insurance and payments, and vital global collaborative drug and vaccine research. It also exposed security gaps that cyber criminals and nation-states are taking advantage of. 2020 has shown that strong authentication that is purpose-built for security, phishing resistant, and stops account takeovers, is a key requirement for ensuring compliance and protecting sensitive healthcare data.

In planning for the post-pandemic future, healthcare organizations should look to implement YubiKeys for strong authentication without compromising on security, usability or scale.

[7] https://patientengagementhit.com/news/top-challenges-impacting-patient-access-to-healthcare

[8] https://www.fda.gov/news-events/congressional-testimony/safeguarding-pharmaceutical-supply-chains-global-economy-10302019#ftn3

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.