Logging In:
Real World Challenges in a Healthcare Setting

the sequoia project
carequality

Johnathan Coleman
The Sequoia Project
CISO, TEFCA RCE

Ryan Patrick
VP, Adoption
HITrust

Drew McCombs
CISO, Epic Nexus

Elliott Jones
VP, CISO
Kaiser Permanente

This panel will discuss how authentication mechanisms need to balance the need for security with the operational reality of providing care to patients.

Do tools such as Multi Factor Authentication (MFA) or One Time Passwords (OTPs) help or hurt?

Are they appropriate for everyone in a healthcare setting, or should they only be deployed in select circumstances?

Terminology Refresher

- **What is Authenticator Assurance Level 2 (AAL2)?**
  - AAL2 provides high confidence that the person making the claim actually controls the authenticator bound to their account.
  - Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.*

  There are two options:
  1) Use of either a multi-factor authenticator OR
  2) A combination of two single-factor authenticators.

- **Example 1: Multi-Factor Authenticator Example:**
  - *A multi-factor OTP device:* This could be a software-based OTP generator installed on a mobile phone which also requires a PIN or biometric to be used each time the OTP is generated.
    - The multi-factor OTP device is something you *have*, and is activated by something you *know* or something you *are*

- **Example 2: Two single-factor authenticators**
  - Combination of a Password (or PIN) and a possession-based authenticator (i.e., "something you have")
    - Something you have could be an out-of-band device (e.g. mobile phone receiving an SMS message)

*See NIST SP800-63B for AAL2 types: https://pages.nist.gov/800-63-3/sp800-63b.html#aal2types

Authentication: Making the case for AAL2

1) Health Care Industry Cybersecurity Task Force Report[1] on Improving Cybersecurity in the Health Care Industry (June 2017) includes Recommendation 2.4: "***Require strong authentication to improve identity and access management for health care workers, patients, and medical devices/EHRs***."

"Clinicians in a hospital setting are required to access multiple computers throughout the facility repeatedly (up to 70 times per shift) as they deliver care to patients.

In order to authenticate… …a clinician typically enters his or her username and a unique password.

This widely used, single factor approach to accessing information is particularly prone to cyber attack as such passwords can be weak, stolen, and are vulnerable to external phishing attacks, malware, and social engineering threats.

NIST SP 800-63 adopts alternatives to the use of passwords for user authentication, including items in the user's possession (e.g., a proximity card or token) or biometrics."

Action Item 2.4.2: In situations where the provider is accessing an EHR or Health Information Exchange external to the hospital or clinical environment, the health care industry should adopt the NIST SP 800-46[2] guidelines ***for remote access including the use of two-factor authentication*** to ensure a compromised password cannot alone be used to gain access.

Authentication: Making the case for AAL2

2) **OCR Breach Reporting Portal**[3]: Query on the archived cases (does not include open investigations) shows approximately 1.9M patients affected by incidents where the mitigation or corrective action plan shows that ***multi-factor authentication*** will be implemented as a result of the incident.
3) **Health Sector Cybersecurity Coordination Center (HC3) Threat Brief**[4], June 16, 2022: Strengthening Cyber Posture in the Health Sector includes the recommendation: "***Validate that all remote access to the organization's network, as well as privileged or administrative access, requires multi-factor authentication***."
4) **HC3 Ransomware Trends Report:** Includes as an example, CISA's Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks[5] which recommends ***multi-factor authentication be required for remote access***.
5) **HC3 Threat Brief**[6], January 12, 2023 for the Royal & BlackCat Ransomware[7] includes ***FBI's recommendation for multi-factor authentication*** as a means of mitigation and defense.
6) **OWASP Top 10 Brief**[8] **and threat brief**[9] includes Common Weakness Enumerations (CWEs) related to authentication. *"Most authentication attacks occur due to the continued use of passwords as a sole factor. Once considered the best practices, password rotation and complexity requirements encourage users to use and reuse weak passwords. Organizations are recommended to stop these practices per NIST 800-63 and use multi-factor*. Where possible, ***implement multi-factor authentication*** to prevent automated credential stuffing, brute force, and stolen credential reuse attacks".

Authentication: Stakeholder Comments

- Concerns that physician burden and further frustration with IT may prevent participation
- Concerns that AAL2 is not practical for clinical kiosks, shared workstations etc.
- Misconception that AAL2 would require 2FA to be used for *every* access to every record
- Many systems are already using 2FA for remote access and are utilizing tap-badges/proximity cards for local users
- Consider MFA for remote workers only; 2 Factor authentication is widely adopted for offsite/remote users and is a reasonable requirement


Annual Meeting
2023
SAN DIEGO
California
the sequoia project
carequality