Medical Multi-Factor Authentication Design & Policies

Security Analyst: Uzair Khan, B.S. Cybersecurity, minor: Computer Science

Date: 02/15/2026

Scenario:

Revolant Medical, a small medical office (5 doctors, 3 staff members) needs better security. They currently use only passwords. Design a practical MFA system for them.

Scope of Work:

The Design Will Include:

- Password security hygiene policies.
- Two authentication factors.
- Implementation plan.
- User experience and time-frame considerations.

Factors Considered:

- Something you know (password, PIN).
- Something you have (phone, token, card).
- Something you are (fingerprint, face).

Real-World Constraints and Considerations:

- Doctors are often in a hurry.
- Not everyone is tech-savvy.
- Budget is limited.
- Must meet **HIPAA** requirements.

Revolant Medical Cybersecurity MFA Design:

Default Standard: Secure Password Policies

- Passwords must contain a minimum of 16 characters.
- Passwords must contain uppercase and lowercase letters.
- Passwords must contain numbers and special characters.
- Password resets must not use a previously created password.
- Passwords will be changed immediately if notified of compromised credentials.

Multi-Factor Authentication Policies:

Factor 1: Microsoft Authenticator App

All Revolant Medical employees will download and use Microsoft Authenticator, a free authenticator app which can work offline, is easy to deploy, and is HIPAA compliant when used with secure systems.

At Revolant, Microsoft Authenticator will act as the “something you have” factor. When logging into email through Microsoft 365, the system will prompt MFA through the authenticator app through either a code or approve/deny push notification.

Factor 2: Biometric Windows Hello Login on Office Computers

All applicable office computers will utilize Windows Hello biometric login using fingerprint or face unlock. Windows Hello biometric login allows a user to log into the computer with their face or fingerprint for applicable systems. Many hospitals use this technology to access their computers and sensitive personally identifiable information such as patient records. This technology provides convenience and speed for busy medical professionals, and it reduces their reliance on manual logins.

Factor 3: Physical Security

Revolant Medical shall lock all premises before/after public hours. Office access shall be controlled via a smart key, badge, or code. Laptops, desktops, and electronic devices shall be logged out and powered off after use for protected health information (PHI).

Factor 4 (optional): Bitwarden Password Manager

To further aid security and long-term ease for Revolant Medical employees, staff members can install **Bitwarden** for free and secure password management along with paid team password management options. By only using and memorizing one secure master password, employees can create secure passwords throughout all medical work domains.

Implementation Plan & Timeframe:

Step 1: Preparation (Week 1)

First, Revolant Medical staff members or an outsourced IT/cybersecurity professional should create an inventory of which devices support Windows Hello and confirm that employee devices are capable of running the Microsoft Authenticator app. Staff shall be notified of new password policies. An optional step will be recommended to install Bitwarden and create staff accounts to ensure all hardware is ready for MFA implementation.

Step 2: Staff Setup (Week 2)

Default Standard – Password Policies

Staff shall be notified of new password policies and instructed to ensure standards are met in a timely manner. Staff members shall receive a follow up after MFA factors have been enacted and given follow-ups on a yearly basis.

Factor 1 – Microsoft Authenticator App

Staff shall install the authenticator app on their phones and complete an initial test login procedure. In the case of lost devices or failure, they shall create printed recovery codes to log in and re-enroll authenticator on a new device under office supervision.

Factor 2 – Biometric Windows Hello Login

Staff using supported devices log in with their passwords, enroll fingerprint or facial recognition, and test Windows Hello logins. In the case of lost devices or failure, staff members may use Microsoft Authenticator to log in instead and wait for administrator to reset Windows Hello if necessary.

Factor 3 – Physical Security

Staff shall log out and power off all laptops, desktops, and electronic devices after use, ensure office doors and access points are locked during after hours, and ensure access controls are in place.

Factor 4 (optional) – Bitwarden Password Manager
Staff administrator will install Bitwarden password manager on laptops, devices, and optionally phones, create or direct employees to create a strong master password, and import/generate passwords for all systems/accounts used. In the case of lost master password, admin shall assist with secure password reset procedure.

Step 3: Testing and Documentation (Week 3)

Schedule a 1-hour full-office meeting session in which staff, logs in using Windows Hello and Authenticator, tests recovery codes, and practices Bitwarden autofill if available. Document setup completion and recovery procedures for HIPPA compliance.

User Experience:

The specialized MFA policies for Revolant Medical ensure a robust security posture and when combined with security awareness training will create a foundational long-term security plan. All considerations can be implemented at no cost or can use paid options for easier use and scalability.

All security policies do not take any considerable time to enact during workdays and can even make device login easier for medical professionals. The Windows Hello login using a fingerprint or face unlock takes no more than 10 seconds, making it quick and convenient for doctors. For any unsupported devices, Microsoft Authenticator provides a quick <20 second login with MFA codes. The emergency/lost device lockout options can be done quickly with easy recovery codes within a minute to ensure staff is never locked out. Finally, Bitwarden auto-fills passwords and reduces errors to speed up logins and aid secure password creation and management.

While the password policies and the optional password management options are strict and may be tedious, given the sensitive nature of patient data and the susceptibility of healthcare organizations, maintaining a strong security posture is vital for long-term security and the financial wellbeing of Revolant Medical.