HEALTHCARE | HIPAA SECURITY RULE

Token & HIPAA Security Rule

The strengthened HIPAA Security Rule modernizes the technical safeguards governing electronic protected health information. It defines and requires multi-factor authentication (MFA), makes encryption of ePHI a required (no longer "addressable") safeguard, and tightens controls across access, audit, workforce, and incident response. TokenCore Wearable and TokenCore Portable deliver FIDO2-certified, hardware-bound, biometrically-verified authentication that maps directly to the technical safeguards below.

Requirements Mapping

§ Section	Requirement	How Token addresses it
164.312(f)	Standard: Authentication. Verify identity using Multi-Factor Authentication — two of three factor categories: knowledge, possession, or inherence.	TokenCore Wearable and TpkenCore Portable deliver possession (hardware-bound device) plus inherence (on-device fingerprint match) in a single tap. FIDO2-certified, phishing-resistant, origin-bound credentials defeat reverse-proxy and AiTM kits that defeat OTP and push-MFA — the vector behind Change Healthcare and most ransomware initial access.
164.312(a)	Standard: Access Control. Implement technical policies and procedures permitting only authorized persons or software programs access to ePHI.	Hardware-bound credentials tie every access decision to a specific device and a specific person — no shared secrets, no phishable factors. Match-on-chip biometrics: the fingerprint template is created and verified inside the secure element and never leaves the device.
164.312(b)	Standard: Encryption and Decryption. Encrypt ePHI at rest and in transit. Encryption is required (no longer "addressable"), with limited exceptions.	Private keys are generated and held inside an EAL5+ certified secure element; they cannot be exported, copied, or replayed. NFC and BLE channels carry only signed FIDO2 assertions, never credentials. Hardens the authentication leg of the encryption requirement.
164.312(d)	Standard: Audit Trail and System Log Controls. Record and examine activity in information systems containing ePHI.	Every authentication produces a signed, attestable event tied to a specific authenticator and workforce member. Feeds Epic, Cerner, Okta, Microsoft Entra, and SIEM logs with tamper-evident identity signals — exactly the evidence OCR cites as deficient in recent enforcement actions.
164.308(a)(9)	Standard: Workforce Security. Authorize, supervise, and terminate workforce access to ePHI; respond to credential changes.	Lost, stolen, or departing-credential revocation is a single action in your IAM console — the credential dies with the device. No password resets, no help-desk social-engineering window (the Scattered Spider vector behind MGM, Aflac, and Coinbase).
164.308(a)(12)	Standard: Security Incident Procedures. Identify and respond to suspected or known security incidents; mitigate harm; document.	Phishing-resistant authentication removes the most common initial-access vector behind ransomware and account takeover in healthcare. Reduces both the frequency and blast radius of reportable breaches under § 164.408 and the strengthened incident procedures.
164.308(a)(2) & 164.314	Risk Analysis & Business Associate Contracts. Document risks to ePHI; require business associates to apply equivalent technical safeguards.	Token deploys in hours alongside Okta, Microsoft Entra, Ping, Duo, and CyberArk — extends the same phishing-resistant MFA standard to clinicians, contractors, and BAs. Gives the Security Official a defensible, documented control upgrade for the annual risk analysis and BA verification.
164.312(a)	Standard: Access Control. Implement technical policies and procedures permitting only authorized persons or software programs access to ePHI.	Hardware-bound credentials tie every access decision to a specific device and a specific person — no shared secrets, no phishable factors. Match-on-chip biometrics: the fingerprint template is created and verified inside the secure element and never leaves the device.
164.312(b)	Standard: Encryption and Decryption. Encrypt ePHI at rest and in transit. Encryption is required (no longer "addressable"), with limited exceptions.	Private keys are generated and held inside an EAL5+ certified secure element; they cannot be exported, copied, or replayed. NFC and BLE channels carry only signed FIDO2 assertions, never credentials. Hardens the authentication leg of the encryption requirement.

Token Products Referenced

TokenCore Wearable

FIDO2 authenticator. EAL5+ certified secure element, 508 DPI on-device fingerprint sensor, BLE + NFC. Match-on-chip biometrics; private keys never leave the ring. Designed for shared workstation retail, call center, and back office settings.

TokenCore Portable

Wireless FIDO2 hardware security key with on-device fingerprint sensor and secure element. Field-upgradable firmware. Drop-in replacement for OTP and tap-only keys for admin, developer, and business associate workforce.