Authentication for Healthcare: Identity Across Hospitals, Payers, Pharma, and Telehealth Without Slowing Care

Industry Guides / Last updated 2026-06-11 / https://www.scrambleid.com/learn/authentication-for-healthcare

In one sentence: Healthcare authentication has to satisfy clinical workflow at the bedside, regulatory constraints from HIPAA and DEA EPCS, the realities of shared workstations and roaming clinicians, and the same phishing-resistance bar that every other regulated industry now expects, all without making the next code-blue response slower.

TL;DR (canonical)

- HIPAA Security Rule (45 CFR 164.312) requires authentication safeguards. The proposed 2024 NPRM moves toward making MFA explicit; the operational standard is already there in HHS 405(d) Health Industry Cybersecurity Practices and OCR settlement language.
- DEA EPCS (21 CFR Part 1311) requires two-factor authentication at controlled-substance prescription signing, with at least one factor as hard token or biometric. Phishing-resistant FIDO2 authenticators with FIPS 140 certification are the cleanest path.
- Shared-workstation reality (WoWs, nursing stations, ED) means clinical workflow demands sub-second context switches. The architecture that works: proximity badge for tap-and-go reauth on top of a primary phishing-resistant credential held by the clinician's device.
- Telehealth, patient portals, contact centers, and medical devices each have their own authentication patterns. The most failure-prone path in healthcare is the contact center, where KBA based on SSN/DOB/member ID continues to be the front line.
- The architecture that closes all of this: a single device-bound cryptographic credential per clinician, per member, per device, applied across web, EHR, telehealth, voice, and machine channels, with risk-based step-up at high-assurance moments (controlled-substance prescribing, large data exports, claims authorizations).

The healthcare threat landscape

Healthcare has the highest per-record breach cost of any industry. The threat patterns:

Ransomware delivered via phishing. A clinician clicks a phishing link, attacker gets a credential, lateral movement begins, EHR access is encrypted. The hospital is on diversion within 48 hours. Phishing-resistant authentication on workforce SSO is the highest-leverage control against this pattern.

Business email compromise (BEC) of finance and ops. Healthcare CFOs and procurement teams are heavily targeted for BEC. The mitigations are the same as financial services: phishing-resistant MFA on email, step-up authentication on payment-relevant actions, and a verifiable internal-to-internal trust signal so vishing of finance teams stops working.

Member-data fraud at health-plan contact centers. Fraudsters call the plan with stolen KBA inputs and harvest claims data, demographics, or authorization information for downstream fraud. Cryptographic caller verification replaces KBA.

Insider misuse of EHR access. Clinicians and staff accessing records for non-clinical reasons (celebrity records, ex-partner records, insurance claims). Authentication does not prevent this directly, but signed authentication events with role and patient context produce the audit trail that makes detection and discipline possible.

Telehealth-channel fraud. Imposter providers (offering fake telehealth services to harvest plan information) and imposter patients (using stolen credentials to obtain controlled-substance prescriptions). Both ends need stronger identity than video-conference logins provide by default.

Medical-device compromise. Connected infusion pumps, imaging systems, and clinical IoT are increasingly authentication-relevant. FDA premarket cybersecurity guidance is explicit about authentication on connected devices.

Regulatory landscape

Regulation	What it requires	Practical implication
HIPAA Security Rule (45 CFR 164.312)	"Reasonable and appropriate" technical safeguards including authentication; integrity controls; audit	Effectively requires MFA today; the proposed 2024 NPRM moves toward explicit MFA requirement for ePHI access
HITECH Act	Breach notification (60-day rule); penalty tiers	Stronger authentication reduces breach probability and severity tier
DEA EPCS (21 CFR Part 1311)	Two-factor authentication at prescription signing; at least one factor hard token or biometric; FIPS 140 for hard tokens, 21 CFR 1311.116 for biometrics	Phishing-resistant FIDO2 with FIPS-certified authenticator is the cleanest fit
42 CFR Part 2 (SUD records)	Heightened consent and access controls for substance-use-disorder records	Authentication and access logging at higher assurance for any system holding Part 2 records
State data breach notification laws	Varying notification windows and definitions	Lower breach probability has compounding state-by-state benefit

Regulation	What it requires	Practical implication
HHS 405(d) HICP	Industry-recognized cybersecurity practices; SS-7 mitigation against ransomware	MFA, phishing-resistance, and identity hygiene are core HICP practices
FDA Premarket Cybersecurity Guidance	Authentication requirements on connected medical devices	Device identity is in scope; long-lived service accounts on devices are increasingly indefensible
State All-Payer Claims Database (APCD) regulations	Authentication for state-mandated data submissions	M2M authentication on claims-submission channels

For a deeper compliance view including NIST SP 800-66 Rev. 2 (HIPAA Security Rule implementation), NIST SP 800-53 Rev. 5, and CISA phishing-resistant MFA guidance, see Compliance Mapping: NIST and CISA.

The healthcare channel mix

Channel	Who authenticates	Typical legacy method	Phishing-resistant pattern
EHR (clinician)	Physicians, nurses, residents	Password + push, SSO + push	Phishing-resistant SSO + EHR-context badge tap
Shared workstation (WoW, nursing station)	Roaming clinicians	Proximity badge, password + tap	Proximity badge tap on top of a phishing-resistant primary; periodic strong reauth
Controlled-substance prescribing (EPCS)	Prescribers	Password + hard token	FIPS-certified phishing-resistant authenticator at signing
Telehealth (clinician side)	Clinicians	EHR SSO	Phishing-resistant SSO with telehealth-specific context
Telehealth (patient side)	Patients	Email/password + sometimes SMS	Patient portal with phishing-resistant MFA, pinned to telehealth session
Patient portal	Patients	Email/password + SMS	Passkey-based portal authentication
Health-plan member portal	Members	Email/password + SMS	Passkey-based portal; SMS removed from chain
Health-plan contact center (IVR + agent)	Members calling	KBA (SSN, DOB, member ID, recent claims)	Cryptographic caller verification; KBA only for low-assurance read-only inquiries
Pharma sales reps and trial portals	Reps, investigators	SSO + push	Phishing-resistant SSO

Channel	Who authenticates	Typical legacy method	Phishing-resistant pattern
Connected medical devices	Device-to-EHR, device-to-cloud	Long-lived service accounts in firmware	Sender-constrained tokens; broker-mediated identity for legacy
Claims-submission and clearinghouse APIs	Practice management, billing systems, clearinghouses	Static API keys	Sender-constrained access tokens (mTLS, DPoP)
Privileged IT and clinical informatics	DBAs, EHR admins, integration engineers	SSO + push	Phishing-resistant SSO + JIT elevation + dual control

The places healthcare consistently underinvests: shared-workstation patterns (workflow latency wins over assurance), contact centers (KBA persists), and medical-device identity (technical debt).

Authentication patterns by use case

Pattern 1, the clinician on a shared workstation

Goal: Clinician walks up to a workstation on wheels, taps in, charts, walks away. Sub-second context switches without sacrificing assurance.

Approach: The clinician carries a phishing-resistant authenticator (badge or device-bound credential) registered to a personal authenticator. At workstation interaction, a tap initiates a cryptographic ceremony scoped to the workstation context and the EHR session. After a configured idle timeout or a high-assurance action (medication administration, large data export), a strong reauth is prompted. Some hospitals layer in periodic biometric reverification.

Outcome: Workflow latency stays at the badge-tap level. Authentication assurance moves from "shared password posted under the keyboard" to a signed, auditable cryptographic event. Lateral movement from one compromised workstation does not give the attacker every clinician's credentials.

Pattern 2, controlled-substance prescribing (EPCS)

Goal: Meet DEA 21 CFR Part 1311 at the prescription-signing event with the strongest possible factor.

Approach: Use a FIPS 140 certified authenticator (or a biometric subsystem meeting 21 CFR 1311.116) with a phishing-resistant ceremony at the signing moment. The clinician's authentication produces a digitally signed prescription that is auditable end-to-end. For prescribers in a hospital setting, the same authenticator covers EHR SSO, EPCS signing, and high-assurance step-up moments.

Outcome: A single authenticator covers EPCS, EHR, and step-up paths. EPCS audit becomes part of the standard authentication audit rather than a separate workflow.

Pattern 3, telehealth

Goal: Both clinician and patient authenticated at appropriate assurance for the visit.

Approach: Clinician side: phishing-resistant SSO into the EHR/telehealth platform. Patient side: passkey-based portal authentication. The video-conference session is initiated only after both sides have completed phishing-resistant authentication, with the visit context (clinician, patient, visit reason) signed into the session. For controlled-substance telehealth (where state law permits), the signing factor at prescription must still meet EPCS.

Outcome: Telehealth identity assurance is an explicit property of the session, not an artifact of "the clinician was already logged in to the conferencing tool."

Pattern 4, patient and member portals

Goal: Eliminate password reuse and SMS-OTP-driven account takeover on patient and member portals.

Approach: Passkey-based authentication on the portal as the default, with phishing-resistant recovery flows. For health-plan portals where members frequently call after attempting login, integrate the portal authenticator with the contact-center caller verification so the same identity travels.

Outcome: ATO on patient portals collapses. Members who can authenticate to the portal can also be cryptographically verified when they call.

Pattern 5, health-plan contact center

Goal: Replace KBA as the primary identity check for members calling about benefits, claims, and authorizations.

Approach: When the member calls, the IVR initiates a cryptographic challenge to the member's authenticator. The agent receives a verified member identity before any sensitive action. KBA is downgraded to a fallback for unauthenticated members on read-only inquiries.

Outcome: Vishing of plan agents with harvested KBA stops working. Authentication time drops. Audit evidence is a signed authentication event tied to a specific member, claim, or authorization.

Pattern 6, internal workforce (BEC and ransomware defense)

Goal: Eliminate password and push-OTP-based access for clinicians, billing, finance, and IT.

Approach: Phishing-resistant SSO across the workforce. Step-up at high-risk actions (vendor payment changes, large data export, system administration). Dual control on the highest-risk operations. Recovery and break-glass paths must be at the same assurance level as the primary; help-desk-driven resets are the largest source of post-passkey ATO.

Outcome: Ransomware delivered via credential phishing collapses. BEC of finance and procurement teams becomes structurally harder.

Pattern 7, connected medical devices and clinical IoT

Goal: Eliminate long-lived service-account credentials on connected medical devices.

Approach: For new devices, sender-constrained tokens (RFC 8705 mTLS, RFC 9449 DPoP) at the device-to-EHR and device-to-cloud boundary. Short-lived credentials brokered at runtime. For legacy devices that cannot be rearchitected, a broker-mediated identity gateway in front of the device. Engage with the device manufacturer's FDA premarket cybersecurity guidance to push for authentication-relevant features.

Outcome: A stolen credential from one device cannot be replayed from another network or workload. Device identity becomes a controllable axis rather than a 5-year procurement decision.

For deeper M2M coverage, see M2M Authentication Without Secrets and Machine Identity (PoP, DPoP, mTLS).

Shared-workstation deep-dive: tap-and-go without compromising assurance

The shared workstation is the single hardest authentication problem in healthcare. The constraints:

- A clinician switches workstations dozens of times per shift.
- Workflow latency tolerance is roughly 1 second; anything more disrupts care.
- Workstations are often in semi-public areas; physical proximity is a weak signal.
- The legacy pattern is a proximity badge that resumes a session, often without a true cryptographic ceremony.

The architecture that resolves the workflow tension without giving up assurance:

1. **Primary credential is phishing-resistant and held off the workstation.** The clinician's identity lives in a hardware-bound credential on a wearable badge or personal device, not on the workstation.
2. **Tap-in is a cryptographic ceremony, not a session resume.** The badge or device signs a fresh challenge per workstation interaction. The signed event is auditable and cannot be replayed elsewhere.
3. **Session is scoped tightly.** The session is bound to the workstation, the clinician, and a configurable duration. Walk-away timeouts are short.
4. **High-assurance actions trigger explicit reauth.** Medication administration, large exports, and patient-record writes that meet certain criteria require a fresh strong reauth, not just a session check.

5. **Recovery from a lost badge is identity-proofing-based, not help-desk-based.** Lost badges are common; the recovery path must not be a credential-phishing surface itself.

This architecture preserves the bedside workflow while moving the assurance from "shared password posted under the keyboard" to a signed cryptographic ceremony at every workstation tap.

Anti-patterns to avoid

1. **MFA on EHR, KBA on the contact center.** The plan member or patient calls, the contact-center agent walks them through KBA-based "verification," and the assurance gap is wide open. The fraud follows the path of least resistance.
2. **Push-OTP MFA without number-matching for clinicians.** MFA-fatigue attacks against clinicians on overnight shifts have happened. Number-matching plus contextual approval is the floor; phishing-resistant is the bar.
3. **Email-link recovery for patient portals.** A patient's compromised email becomes the portal compromise. Use phishing-resistant recovery.
4. **Long-lived service-account credentials on medical devices.** Device firmware with embedded API keys is the next regulator-action target. Move toward sender-constrained tokens.
5. **Tap-and-go that is just session resume with no cryptographic ceremony.** This is widespread and increasingly indefensible. Tap-and-go must produce a signed event per tap.
6. **Telehealth where the clinician is "logged in to the conferencing tool" and that's the assurance.** Telehealth visits need explicit, signed identity assurance for both ends.
7. **Treating EPCS as a separate authentication track.** A FIPS-certified phishing-resistant authenticator can serve as the EPCS factor and the EHR SSO factor with the right architecture; running two parallel authentication stacks is operational debt.

Compliance mapping (worked example)

A typical regional health system has hospital and clinic operations (HIPAA), a small health-plan business (HIPAA + Medicare Part C ACA), prescribers writing controlled substances (DEA EPCS), telehealth (DEA + state laws), connected medical devices (FDA), and 42 CFR Part 2 records in a behavioral-health unit.

Control area	HIPAA Sec. Rule	DEA EPCS	42 CFR Part 2	FDA Premarket Cyber	NIST 800-66 R2
User authentication	164.312(d)	21 CFR 1311.115	Heightened access controls	Authentication on connected devices	IA-2 implementation
MFA / phishing resistance	Reasonable and	Two-factor at signing, hard token	Aligned with HIPAA	Authentication strength expectations	IA-2(8), IA-2(11)

Control area	HIPAA Sec. Rule	DEA EPCS	42 CFR Part 2	FDA Premarket Cyber	NIST 800-66 R2
	appropriate	/ biometric			
Audit	164.312(b)	1311.115(d) audit trail	Detailed access logging	Logging on connected devices	AU-2, AU-3
Recovery	Implicit in 164.308(a)(7)	Re-enrollment proofing	Heightened in Part 2	Device re-credentialing	IA-5(1)
M2M / device ID	164.312(c) integrity	Out of scope	Out of scope	Authentication on device communications	IA-9

This is a sketch, not a formal mapping. Build the actual mapping with HIPAA counsel, your DEA EPCS vendor, and your medical-device security team. The unifying point: a single phishing-resistant architecture can satisfy the majority of these controls when authentication is treated as a property of the system rather than a feature added in one place.

How to evaluate a vendor for healthcare authentication

Beyond the standard passwordless evaluation criteria (see Enterprise Passwordless Vendors Compared), healthcare buyers should weight:

1. **Shared-workstation tap-and-go fit.** Does the vendor support a sub-second clinical workflow with a true cryptographic ceremony per tap?
2. **EPCS support.** FIPS 140 certification on the authenticator path (and 21 CFR 1311.116 compliance for any biometric subsystem)? Integration with major EHR EPCS workflows (Epic, Oracle Health, MEDITECH, athenahealth)?
3. **Voice/contact-center authentication.** Same as financial services. KBA replacement is the highest-leverage move at health-plan contact centers.
4. **Telehealth integration.** Can the platform pin authentication assurance into a telehealth visit context for both clinician and patient?
5. **Recovery posture.** Phishing-resistant recovery for lost badges, lost devices, and forgotten credentials. Help-desk-driven password resets are the largest post-passkey ATO surface.
6. **Audit and SIEM integration.** Are authentication events signed and shippable in formats useful for HIPAA audit, OCR investigations, and DEA EPCS audit?
7. **Medical-device identity.** Is there a path for connected-device authentication, or is that scope explicitly out?

Key Takeaway

Healthcare authentication must reconcile clinical workflow (sub-second context switches at shared workstations) with regulatory bars from HIPAA, DEA EPCS, 42 CFR Part 2, and FDA medical-device cybersecurity guidance, plus the practical realities of telehealth, patient portals, contact centers, and connected devices. The architecture that closes the gap: a single phishing-resistant cryptographic credential per clinician, per member, per device, applied across web, EHR, telehealth, voice, and machine channels, with sub-second tap-and-go on shared workstations and FIPS-certified authenticators at controlled-substance prescribing. The biggest failure modes are KBA-based contact-center authentication, push-OTP MFA without phishing resistance, and long-lived service accounts on connected medical devices.

FAQ

Does HIPAA require MFA?

The HIPAA Security Rule itself does not name MFA as an explicit standard, but it requires "reasonable and appropriate" technical safeguards including authentication of users (45 CFR 164.312(d)). Effectively every recent HHS Office for Civil Rights settlement, OCR cybersecurity newsletter, and the 405(d) Health Industry Cybersecurity Practices recognize MFA as a baseline reasonable safeguard. The HHS HIPAA Security Rule NPRM published in late 2024 proposes making MFA explicitly required for most ePHI access; verify the current rule status with counsel.

What does DEA EPCS require for authenticating a prescriber?

21 CFR Part 1311 requires a two-factor authentication ceremony at the time the controlled-substance prescription is signed, with at least one factor being a hard token (FIPS 140-2/3 cryptographic) or biometric (meeting the biometric subsystem requirements of 21 CFR 1311.116). Knowledge factors (passwords, PINs) alone are not sufficient. The signing event must produce a digitally signed prescription that is auditable. Phishing-resistant FIDO2 authenticators meeting FIPS 140 certification are the cleanest path for this requirement.

Why is shared-workstation authentication so hard at hospitals?

On a hospital floor, dozens of clinicians share a small number of workstations on wheels (WoWs) or fixed nursing-station terminals. The clinical workflow demands sub-second context switches; a clinician walks up, taps in, charts, walks away. Password-based MFA breaks this workflow. The dominant pattern is proximity badges (tap and go) plus a primary cryptographic credential held by the clinician's device, with periodic strong reauth. The trade-off is between workflow latency and authentication assurance, and no naive solution gets it right.

What authentication does a telehealth visit need?

Both sides need stronger identity than a standard video-conferencing login. The clinician needs to be authenticated to the EHR with phishing-resistant MFA. The patient needs to be authenticated to the patient portal at a level commensurate with the data being discussed. For high-acuity visits or controlled-substance prescribing, both ends should be at NIST SP 800-63 AAL2 or AAL3 properties, with audit evidence of the authentication ceremony.

How does contact-center authentication work for a health plan?

Health-plan contact centers face the same KBA-vulnerability problem as banks: SSN, DOB, member ID, and recent claims are all available to fraudsters. The pattern is to bind a cryptographic credential to the member at first portal login or at IVR enrollment, then use that credential to verify the caller cryptographically. KBA falls back to a low-assurance fallback for unauthenticated members on read-only inquiries, not as the primary trust path.

What about medical-device identity?

Medical devices that connect to the EHR or to cloud platforms increasingly need machine identity. The FDA's cybersecurity guidance for premarket submissions calls for authentication on connected devices. For new devices, sender-constrained tokens (mTLS, DPoP) and short-lived credentials are the path. For legacy devices that cannot be rearchitected, broker-mediated identity (a trust gateway in front of the device) is the practical pattern. Long-lived service-account passwords stored in device firmware are the worst case.

Is push-to-phone MFA enough for a hospital?

It is better than passwords alone but it is not phishing-resistant. MFA-fatigue attacks have driven multiple healthcare breaches. Push with number-matching and contextual approval text raises the bar but does not match FIDO2/WebAuthn-grade resistance. For the most sensitive functions (admin, EHR write, controlled-substance prescribing, large data exports), phishing-resistant cryptographic factors should be the primary.

References (public)

- HHS, HIPAA Security Rule: https://www.hhs.gov/hipaa/for-professionals/security/index.html
- DEA Diversion Control, Electronic Prescriptions for Controlled Substances: https://www.deadiversion.usdoj.gov/ecomm/e_rx/
- 21 CFR Part 1311 (Electronic Prescriptions): https://www.ecfr.gov/current/title-21/chapter-II/part-1311
- HHS 405(d) Health Industry Cybersecurity Practices: https://405d.hhs.gov/

- NIST SP 800-66 Rev. 2 (HIPAA Security Rule Implementation): https://csrc.nist.gov/pubs/sp/800/66/r2/final
- FDA Cybersecurity in Medical Devices: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
- 42 CFR Part 2 (SUD records): https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-2
- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- NIST SP 800-53 Rev. 5: https://csrc.nist.gov/pubs/sp/800-53/r5/final

---

Related reading

- Phishing-Resistant Web Authentication
- Caller Authentication: Stop Vishing
- Omnichannel Authentication
- Recovery and Fallback Playbook
- Compliance Mapping: NIST and CISA
- M2M Authentication Without Secrets
- Lockstep: Dual Control