QueueRX

Pharmacy operations and compliance platform by PhaBO Labs LLC

Security & HIPAA Overview

For pharmacy owners and vendor compliance files

Last reviewed October 2026

45 CFR §164.502(b) MINIMUM NECESSARY

We check the claim, not the patient

A claim check needs drug-level fields only. Patient identifiers are removed before analysis and never written to storage.

What QueueRX reads	What QueueRX never stores
✓ Drug name and strength	✗ ~~Patient name~~
✓ NDC	✗ ~~Date of birth~~
✓ Quantity billed	✗ ~~Home address~~
✓ Pack size	✗ ~~Phone and email~~
✓ Days supply	✗ ~~Social Security number~~

45 CFR §164.504(e)

A Business Associate Agreement on every plan

Any vendor that receives or transmits protected health information for a pharmacy is a business associate, even if it stores nothing. QueueRX signs a BAA with every customer before onboarding, covering permitted uses, safeguards, incident reporting, and return or destruction of data when service ends.

45 CFR §164.410

Breach notification

HIPAA requires a business associate to report a breach without unreasonable delay and no later than 60 calendar days after discovery. That is the legal limit, not our target: our incident response plan notifies you as soon as a breach is confirmed, with the details you need for your own notifications.

Infrastructure

Hosting	Amazon Web Services, HIPAA-eligible services under the AWS Business Associate Addendum
In transit	TLS 1.2 or higher on every connection
At rest	AES-256 on every database, file store and backup
Sign-in	Unique accounts, multi-factor authentication, automatic logoff
Subprocessors	Amazon Web Services (hosting, compute, storage)

Safeguards, mapped to the HIPAA Security Rule

Each safeguard below is listed with the section of 45 CFR Part 164 it answers to.

§164.308

Administrative

- ✓ **Risk analysis.** Documented security risk analysis, reviewed every year. (a)(1)(ii)(A)
- ✓ **Workforce training.** Security training for everyone with system access. (a)(5)
- ✓ **Contingency plan.** Encrypted backups and a written recovery plan. (a)(7)
- ✓ **Vendor oversight.** A BAA with every subprocessor that handles protected data. (b)

§164.310

Physical

- ✓ **Facility access.** Hosted in AWS data centers with controlled physical access. (a)(1)
- ✓ **Workstation security.** Company devices are encrypted and lock automatically. (b), (c)
- ✓ **Device and media controls.** Storage media is wiped or destroyed before reuse or disposal. (d)(1)

§164.312

Technical

- ✓ **Access control.** Unique logins, role-based access, automatic logoff. (a)(1)
- ✓ **Audit controls.** Every view, export and change is logged. (b)
- ✓ **Integrity.** Records protected from improper alteration. (c)(1)
- ✓ **Authentication.** Multi-factor sign-in for every account. (d)
- ✓ **Transmission security.** TLS 1.2 or higher on every connection. (e)(1)

NPRM, 90 FR 898 (JAN 6, 2025)

Ready for the proposed Security Rule update

HHS has proposed making encryption and multi-factor authentication mandatory for all electronic protected health information. QueueRX already does both.

About “HIPAA certification.” There is no government-issued HIPAA certification, and HHS does not recognize private ones (HHS Security Rule FAQ 2003). Compliance is demonstrated through a signed BAA, documented safeguards and a current risk analysis. QueueRX maintains all three.

Questions or BAA requests: support@queuerx.com | (201) 241-9626 | queuerx.com/security.html Describes QueueRX practices. Not legal advice.