Business Associate Agreement

HIPAA Compliance · Version 2.0 · Last updated July 22, 2026

This Business Associate Agreement (BAA) is entered into as of the date of electronic acceptance between the healthcare provider, practice, or other organization identified in the acceptance record (Covered Entity) and QRRX LLC, a New York limited liability company operating the QR Rx digital aftercare platform (Business Associate). Each is a Party and together they are the Parties.

The Parties have entered into the QR Rx Terms of Service, an order form, or another services agreement (the Services Agreement). Business Associate may create, receive, maintain, or transmit Protected Health Information on behalf of Covered Entity while providing the Service. This BAA is intended to satisfy 45 CFR 164.502(e), 164.504(e), and applicable provisions of the HIPAA Rules.

1. Definitions

Terms including Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic PHI or ePHI, Health Care Operations, HIPAA Rules, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information or PHI, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured PHI, and Use have the meanings assigned by HIPAA. Covered Entity and Business Associate have the meanings in 45 CFR 160.103. PHI under this BAA is limited to PHI created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity.

2. Permitted and required uses and disclosures

Business Associate may use or disclose PHI only as necessary to provide, secure, support, and improve the Service for Covered Entity; as expressly authorized by this BAA; or as Required By Law. This includes creating and delivering care plans, operating patient access, mapping connected-system events, sending transactional aftercare communications, supporting treatment workflows, providing reports, responding to Covered Entity, and maintaining security and audit records.

Business Associate may use PHI for its proper management and administration or to carry out its legal responsibilities. It may disclose PHI for those purposes only if Required By Law or after obtaining reasonable assurances that the recipient will keep the PHI confidential, use it only for the disclosed purpose or as Required By Law, and notify Business Associate of any breach of confidentiality.

Business Associate may provide Data Aggregation services relating to the Health Care Operations of Covered Entity and other covered entities only as permitted by HIPAA and the Services Agreement.

3. De-identification and non-PHI information

Covered Entity authorizes Business Associate to de-identify PHI in accordance with 45 CFR 164.514(a)-(c). Information is treated as de-identified only after Business Associate documents that the applicable Safe Harbor or Expert Determination standard has been satisfied. Business Associate will not attempt to re-identify de-identified information and will not disclose a re-identification key.

After lawful de-identification, Business Associate may use de-identified information to operate, secure, measure, and improve the Service and to maintain a procedure-level, clinician-reviewed aftercare knowledge base. De-identified information will not be sold or used for targeted advertising.

4. Restrictions and minimum necessary

Business Associate will not use or disclose PHI in a manner that would violate the HIPAA Rules if done by Covered Entity, except for uses expressly permitted for a business associate's management and administration or Data Aggregation. Business Associate will make reasonable efforts to limit PHI to the Minimum Necessary and will comply with Covered Entity's communicated restrictions to the extent required by law and technically feasible.

Business Associate will not sell PHI, use PHI for advertising, or use PHI to train a general-purpose artificial intelligence model.

5. Safeguards and Security Rule

Business Associate will implement and maintain appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI and will comply with the applicable requirements of 45 CFR Part 164, Subpart C for ePHI. Safeguards include risk analysis and risk management, workforce access controls, authentication, encryption in transit and at rest where reasonable and appropriate, audit controls, incident response, contingency planning, vendor management, and periodic review.

Security measures may evolve as risks, technology, and legal requirements change. Business Associate will not materially reduce the overall protection of PHI during the term.

6. Impermissible uses and Security Incidents

Business Associate will report to Covered Entity any use or disclosure of PHI not permitted by this BAA and any successful Security Incident affecting Covered Entity's ePHI without unreasonable delay and no later than five business days after discovery. Reports may be updated as facts become available.

The Parties acknowledge that unsuccessful pings, scans, failed login attempts, blocked malware, and similar unsuccessful incidents occur routinely. To the extent they do not result in unauthorized access, use, disclosure, modification, destruction, or material interference, they are deemed reported through this provision and do not require individual notice.

7. Breach notification

Following discovery of a Breach of Unsecured PHI, Business Associate will notify Covered Entity without unreasonable delay and no later than ten calendar days after discovery. To the extent available, the notice will identify affected Individuals; describe the nature and date of the Breach and discovery; identify the types of PHI involved; describe investigation, mitigation, and corrective actions; and provide information reasonably needed for notices required under 45 CFR Part 164, Subpart D.

Business Associate will provide supplemental information as it becomes available and reasonably cooperate with Covered Entity's risk assessment, notification, and regulatory response. The Parties will coordinate public statements and individual notices unless law requires otherwise. Responsibility for notification costs and liabilities will be determined under applicable law and the Services Agreement.

8. Mitigation

Business Associate will mitigate, to the extent practicable, harmful effects known to it from a use or disclosure of PHI in violation of this BAA and will take reasonable corrective action to prevent recurrence.

9. Subcontractors

Business Associate will ensure that each Subcontractor that creates, receives, maintains, or transmits PHI on its behalf agrees in writing to the same restrictions, conditions, and Security Rule obligations that apply to Business Associate with respect to that PHI.

The current Subprocessor Register at qrrx.io/subprocessors is incorporated by reference. Business Associate will provide at least 30 days' advance notice before enabling a new Subcontractor to access PHI, except when an emergency replacement is reasonably necessary to protect security or continuity. Covered Entity may raise a reasonable data-protection objection during that period, and the Parties will work in good faith on a commercially reasonable solution.

10. Access to PHI

To the extent Business Associate maintains PHI in a Designated Record Set, it will make the PHI available to Covered Entity in the time and manner reasonably requested so Covered Entity can meet 45 CFR 164.524. If an Individual submits a request directly to Business Associate, Business Associate will forward it to Covered Entity within five business days unless Covered Entity has instructed Business Associate to respond directly.

11. Amendment

Business Associate will make PHI in a Designated Record Set available for amendment and incorporate amendments as directed by Covered Entity within 15 business days or another mutually agreed period so Covered Entity can comply with 45 CFR 164.526.

12. Accounting of disclosures

Business Associate will document and make available information about disclosures of PHI as needed for Covered Entity to respond under 45 CFR 164.528. Business Associate will provide available accounting information within ten business days of a written request.

13. Covered Entity obligations performed by Business Associate

To the extent Business Associate is expressly delegated an obligation of Covered Entity under 45 CFR Part 164, Subpart E, Business Associate will comply with the requirements of Subpart E that apply to Covered Entity in performing that obligation.

14. HHS access

Business Associate will make its internal practices, books, and records relating to the use and disclosure of PHI received from or created for Covered Entity available to the Secretary for purposes of determining compliance with the HIPAA Rules.

15. Covered Entity responsibilities

- Notify Business Associate of limitations in its Notice of Privacy Practices that affect the Service.
- Notify Business Associate of changes in an Individual's permissions and of restrictions that affect Business Associate's use or disclosure of PHI.
- Not request a use or disclosure that would violate HIPAA if performed by Covered Entity, except as permitted for a business associate.
- Maintain all permissions, legal bases, contact preferences, and records required for information and communications sent through the Service.

- Configure users, templates, integrations, mappings, and autonomous delivery consistent with the Minimum Necessary standard and applicable law.

16. Ownership and stewardship

As between the Parties, Covered Entity retains its rights in PHI and clinic content. Business Associate acquires no ownership interest in PHI. Individual rights in PHI are governed by applicable law. Business Associate may retain security, legal, billing, and acceptance records that do not contain PHI or that it is Required By Law to retain.

17. Term and termination

This BAA begins on electronic acceptance and remains in effect while Business Associate maintains PHI for Covered Entity. Covered Entity may terminate the Services Agreement and this BAA for a material violation by Business Associate. If the violation can be cured, Covered Entity will provide a reasonable cure period not exceeding 30 days; no cure period is required when cure is not possible or delay would create a material risk to PHI.

At termination, Business Associate will, if feasible, return or destroy all PHI, including PHI held by Subcontractors, and retain no active copy. Covered Entity may request an available export during the 30-day transition period. Residual PHI in isolated backups will not be used or disclosed except for disaster recovery and will be overwritten through standard backup cycles. If return or destruction is infeasible or retention is Required By Law, Business Associate will continue this BAA's protections and limit further use and disclosure to the reason retention is required.

18. Cura, translation, and artificial intelligence

Business Associate may use automated tools to organize, translate, or retrieve information from Covered Entity-approved content. PHI may be provided to an AI or translation Subcontractor only when that Subcontractor is bound by an appropriate BAA and listed in the Subprocessor Register. A vendor without a BAA may receive information only after Business Associate has documented de-identification under 45 CFR 164.514.

Cura first uses Covered Entity-authored FAQs and the procedure-level Cura Knowledge Base. Any external model fallback involving patient-specific context will remain disabled unless the preceding BAA or documented de-identification condition is satisfied. AI vendors may not use PHI to train general-purpose models.

Only content de-identified in accordance with Section 3 may be promoted to the cross-clinic Cura Knowledge Base. Covered Entity may opt out of future contributions or request removal of material attributable only to Covered Entity by contacting privacy@qrrx.io. Independently verified, de-identified entries may remain without attribution.

19. Effect and order of precedence

This BAA is part of the Services Agreement. If they conflict regarding PHI, this BAA controls. All other commercial limitations and remedies in the Services Agreement apply unless they would prevent compliance with HIPAA.

20. Regulatory change

References to law mean the law as amended. The Parties will amend this BAA as reasonably necessary to comply with a material change in the HIPAA Rules. Until an amendment is effective, the Parties will interpret this BAA to permit compliance with applicable law.

21. Notices

Legal and breach notices to Business Associate must be sent to legal@qrrx.io and security@qrrx.io. Notices to Covered Entity will be sent to the owner or legal notice email recorded for the account. Either Party must keep its notice information current.

22. Governing law and general provisions

The HIPAA Rules govern this BAA and New York law applies where not preempted. This BAA binds permitted successors and assigns. If a provision is unenforceable, it will be narrowed to the minimum extent necessary and the remainder remains effective. No third party is a beneficiary. Sections concerning restrictions, Individual rights, HHS access, return or destruction, and any provision that by its nature should survive will survive termination.

23. Electronic acceptance

By selecting I Accept, the signer represents that they are authorized to bind Covered Entity and agrees to this BAA. QR Rx records the accepting user, organization, document version and cryptographic hash, date and time, IP address, user agent, and acceptance statement. Electronic acceptance and counterparts have the same effect as a signed original.

Electronic acceptance record

An authorized Covered Entity representative accepts this BAA in QR Rx. QR Rx records the signer identity, organization, document version and fingerprint, date and time, and available device and network evidence.

Business Associate: QRRX LLC

Covered Entity: Electronically accepted in QR Rx

Canonical document SHA-256: 09aec0eaf03e1b38573d14c371284ff84b3c05f6dd99aa5a07ec1ede9377f4e9