HIPAA BUSINESS ASSOCIATE AGREEMENT

between

Jal Technology LLC d/b/a QRCodeKey

647 Rose Lane, Bartlett, Illinois 60103, USA

and

[CUSTOMER LEGAL NAME]

[Customer address line 1]

[Customer address line 2]

Effective Date: _____

Template Version 1.0 — May 2026

Recitals

This HIPAA Business Associate Agreement (this "Agreement" or "BAA") is entered into as of the Effective Date set forth on the cover page by and between Jal Technology LLC, an Illinois limited liability company doing business as QRCodeKey, with its principal place of business at 647 Rose Lane, Bartlett, Illinois 60103 ("Business Associate" or "QRCodeKey"), and the customer identified on the cover page ("Covered Entity"). Business Associate and Covered Entity are referred to individually as a "Party" and collectively as the "Parties".

WHEREAS, Covered Entity is a "Covered Entity" or a "Business Associate" as defined under the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the implementing regulations at 45 C.F.R. Parts 160 and 164 (collectively, "HIPAA");

WHEREAS, Covered Entity has subscribed to one or more services of QRCodeKey (the "Services") in connection with which Business Associate may, on behalf of Covered Entity, create, receive, maintain, or transmit Protected Health Information ("PHI");

WHEREAS, the Parties intend to comply with the requirements of HIPAA, including 45 C.F.R. § 164.504(e), 45 C.F.R. § 164.314(a), and any analogous state or foreign healthcare-privacy law that applies to the Parties' relationship;

NOW, THEREFORE, in consideration of the mutual promises set forth in this Agreement and the underlying QRCodeKey Terms of Service (the "Underlying Agreement"), and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows.

1. Definitions

Capitalized terms used but not otherwise defined in this Agreement shall have the meanings ascribed to them in HIPAA. The following terms shall have the meanings set forth below:

"Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of the PHI, as defined in 45 C.F.R. § 164.402.

"Designated Record Set" means a group of records as defined in 45 C.F.R. § 164.501.

"Electronic PHI ("ePHI")" means PHI that is transmitted or maintained in electronic media, as defined in 45 C.F.R. § 160.103.

"HIPAA Rules" means the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164.

"Individual" means the person who is the subject of the PHI, including a personal representative under 45 C.F.R. § 164.502(g).

“Protected Health Information (“PHI”)” means individually identifiable health information, as defined in 45 C.F.R. § 160.103, that is created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity through the Services. PHI does not include de-identified information that meets the requirements of 45 C.F.R. § 164.514(b).

“Required by Law” means as defined in 45 C.F.R. § 164.103.

“Secretary” means the Secretary of the U.S. Department of Health and Human Services or any officer or employee of that Department to whom relevant authority has been delegated.

“Subcontractor” means a person who creates, receives, maintains, or transmits PHI on behalf of Business Associate, as defined in 45 C.F.R. § 160.103.

“Underlying Agreement” means the QRCodeKey Terms of Service available at qrcodekey.com/terms, as amended from time to time, together with any subscription order, statement of work, or invoice between the Parties referencing those Terms.

2. Permitted Uses and Disclosures of PHI

2.1 Use and Disclosure for Covered Entity

Business Associate may use and disclose PHI only as necessary to perform the Services for, or on behalf of, Covered Entity under the Underlying Agreement, and only as permitted or required by this Agreement and the HIPAA Rules. Business Associate shall not use or further disclose PHI in any manner that would violate the requirements of the HIPAA Rules if done by Covered Entity, except as expressly set forth in Section 2.3.

2.2 Minimum Necessary

Business Associate shall use, disclose, and request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request, in accordance with 45 C.F.R. § 164.502(b) and 45 C.F.R. § 164.514(d).

2.3 Permitted Uses for Business Associate’s Operations

Business Associate may use PHI for the proper management and administration of Business Associate, or to carry out its legal responsibilities, or for data aggregation services as defined in 45 C.F.R. § 164.501. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities only if: (a) the disclosure is Required by Law; or (b) Business Associate obtains reasonable assurances from the recipient that the PHI will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed, and the recipient notifies Business Associate of any instance of which it is aware in which the confidentiality of the PHI has been breached.

2.4 Prohibited Uses and Disclosures

Business Associate shall not (a) use or disclose PHI for marketing purposes (as defined in 45 C.F.R. § 164.501) without the prior written authorization of the Individual; (b) sell PHI without the

prior written authorization of the Individual, except as permitted by 45 C.F.R. § 164.502(a)(5)(ii); (c) use PHI to train any third-party machine-learning model or share PHI with any third-party AI provider that has not been bound by a written subcontractor agreement under Section 3.5; or (d) use or disclose PHI in any manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity.

3. Obligations of Business Associate

3.1 Safeguards

Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI, including ePHI, as required by 45 C.F.R. § 164.308, § 164.310, § 164.312, and § 164.316. Without limiting the generality of the foregoing, Business Associate shall:

- Encrypt ePHI at rest using AES-256 (or stronger) and in transit using TLS 1.2 (or stronger);
- Apply role-based access controls, multi-factor authentication for administrative accounts, and audit logging of all PHI access;
- Conduct an annual risk analysis under 45 C.F.R. § 164.308(a)(1)(ii)(A) and document mitigation steps;
- Maintain a written information security policy, an incident response plan, and a business continuity / disaster recovery plan;
- Train workforce members who have access to PHI on the requirements of HIPAA and this Agreement at least annually.

3.2 Reporting of Unauthorized Use, Disclosure, or Breach

Business Associate shall report to Covered Entity, without unreasonable delay and in any event no later than ten (10) business days after Business Associate's discovery: (a) any use or disclosure of PHI not permitted by this Agreement; (b) any Security Incident as defined in 45 C.F.R. § 164.304 that results in unauthorized access to ePHI; and (c) any Breach of unsecured PHI within the meaning of 45 C.F.R. § 164.402. The report shall include the information required by 45 C.F.R. § 164.410, including: (i) identification of each Individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed; (ii) a description of what happened; (iii) a description of the types of unsecured PHI involved; (iv) the steps Individuals should take to protect themselves; (v) a brief description of what Business Associate is doing to investigate, mitigate, and prevent recurrence; and (vi) contact information for follow-up. The Parties agree that this Section satisfies the notice requirement of 45 C.F.R. § 164.410.

3.3 Mitigation

Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement.

3.4 Access, Amendment, and Accounting

Within fifteen (15) business days of receipt of a written request from Covered Entity (or within such shorter period as required by HIPAA in the specific circumstance), Business Associate shall:

- Provide access to PHI in a Designated Record Set to Covered Entity, or directly to the Individual, as directed by Covered Entity, in a manner consistent with 45 C.F.R. § 164.524;
- Make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by Covered Entity in a manner consistent with 45 C.F.R. § 164.526;
- Document and provide to Covered Entity the disclosures of PHI necessary to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures, as required by 45 C.F.R. § 164.528.

3.5 Subcontractors

Business Associate may use Subcontractors to perform any portion of the Services that involves the creation, receipt, maintenance, or transmission of PHI only if Business Associate enters into a written agreement with the Subcontractor that requires the Subcontractor to comply with restrictions and conditions on the use and disclosure of PHI that are at least as stringent as those imposed on Business Associate by this Agreement, as required by 45 C.F.R. § 164.502(e)(1)(ii) and § 164.308(b)(2). Business Associate shall maintain a current list of Subcontractors that handle PHI and shall make the list available to Covered Entity upon request.

3.6 Compliance with Privacy Rule

To the extent that Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity in the performance of those obligations.

3.7 Books and Records

Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Rules, subject to applicable attorney-client and attorney work-product privileges.

4. Obligations of Covered Entity

4.1 Notice of Privacy Practices

Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices under 45 C.F.R. § 164.520, to the extent that any such limitation may affect Business Associate's use or disclosure of PHI.

4.2 Changes in Permission

Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that any such changes may affect Business Associate's use or disclosure of PHI.

4.3 Restrictions Agreed to by Covered Entity

Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI to which Covered Entity has agreed in accordance with 45 C.F.R. § 164.522, to the extent that any such restriction may affect Business Associate's use or disclosure of PHI.

4.4 Permissible Requests

Covered Entity shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity, except as permitted by Section 2.3 of this Agreement.

4.5 Customer Configuration

Covered Entity is solely responsible for configuring its QRCodeKey account, including any field-mapping, retention setting, or sharing setting that may affect the handling of PHI within the Services. Covered Entity shall not enter PHI into any field, free-text input, or upload that has not been designated by Business Associate as approved for PHI processing.

5. Term and Termination

5.1 Term

This Agreement shall commence on the Effective Date and shall continue in effect until terminated as set forth in this Section 5 or until the Underlying Agreement terminates, whichever occurs first. The obligations of Business Associate under Section 6 (Effect of Termination) and any other provision that by its nature should survive shall survive termination of this Agreement.

5.2 Termination for Cause by Covered Entity

Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall provide written notice to Business Associate identifying the breach and providing thirty (30) days to cure. If Business Associate fails to cure the breach within the thirty-day period, Covered Entity may terminate this Agreement and the Underlying Agreement immediately upon written notice.

5.3 Termination for Cause by Business Associate

Upon Business Associate's knowledge of a material breach of this Agreement by Covered Entity, Business Associate shall provide written notice to Covered Entity identifying the breach and providing thirty (30) days to cure. If Covered Entity fails to cure the breach within the thirty-day period, Business Associate may terminate this Agreement and the Underlying Agreement immediately upon written notice.

6. Effect of Termination — Return or Destruction of PHI

Upon termination of this Agreement for any reason, Business Associate shall, at the option of Covered Entity exercised by written notice within thirty (30) days of termination, return to Covered Entity or destroy all PHI that Business Associate or its Subcontractors maintain in any form. If return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to the PHI that cannot be returned or destroyed and shall limit further uses and disclosures of that PHI to those purposes that make return or destruction infeasible, for so long as Business Associate maintains the PHI. Business Associate shall provide Covered Entity with a written certification of return or destruction within sixty (60) days of receipt of Covered Entity's instruction.

7. Miscellaneous

7.1 Regulatory References

A reference in this Agreement to a section of the Code of Federal Regulations means the section as in effect or as amended.

7.2 Amendment

The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the Parties to comply with the requirements of the HIPAA Rules and any other applicable healthcare-privacy law.

7.3 Survival

The respective rights and obligations of Business Associate under Sections 3, 6, and 7 of this Agreement shall survive the termination of this Agreement.

7.4 Interpretation

Any ambiguity in this Agreement shall be resolved to permit the Parties to comply with the HIPAA Rules. In the event of any conflict between this Agreement and the Underlying Agreement, the terms of this Agreement shall control with respect to the handling of PHI.

7.5 No Third-Party Beneficiaries

Nothing in this Agreement shall confer any rights, remedies, obligations, or liabilities upon any person other than the Parties, their respective successors, and permitted assigns.

7.6 Indemnification

Each Party shall indemnify, defend, and hold harmless the other Party and its officers, directors, employees, agents, and successors from and against any and all third-party claims, demands, actions, suits, judgments, fines, penalties, losses, damages, settlements, costs, and expenses (including reasonable attorneys' fees) to the extent arising out of or resulting from the indemnifying Party's breach of this Agreement, negligence, willful misconduct, or violation of the HIPAA Rules.

7.7 Limitation of Liability

Except for the indemnification obligations in Section 7.6 and either Party's breach of confidentiality obligations under Sections 2 and 3, neither Party's aggregate liability under or in connection with this Agreement shall exceed the limitation of liability set forth in the Underlying Agreement.

7.8 Governing Law and Venue

This Agreement is governed by, and shall be construed in accordance with, the laws of the State of Illinois, without regard to its conflict-of-laws principles, and applicable U.S. federal law. The exclusive venue for any dispute arising out of or relating to this Agreement shall be the state or federal courts located in DuPage County, Illinois, and each Party irrevocably submits to the personal jurisdiction of those courts.

7.9 Notices

All notices under this Agreement shall be in writing and shall be delivered by email and by either certified mail (return receipt requested) or recognized overnight courier to the addresses set forth on the cover page (or to such other address as a Party may designate by written notice). Notices to Business Associate shall be sent to info.qrcodekey@gmail.com with a copy to the address on the cover page.

7.10 Counterparts; Electronic Signature

This Agreement may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same agreement. Electronic signatures (including DocuSign and similar) shall have the same legal effect as original signatures.

7.11 Entire Agreement

This Agreement, together with the Underlying Agreement, constitutes the entire agreement between the Parties with respect to PHI and supersedes all prior or contemporaneous agreements, representations, and understandings.

Signatures

IN WITNESS WHEREOF, the Parties have caused this HIPAA Business Associate Agreement to be executed by their duly authorized representatives as of the Effective Date.

BUSINESS ASSOCIATE — Jal Technology LLC d/b/a QRCodeKey

By: _____

Name: Ashvinkumar Chaudhari

Title: Founder & Authorized Signatory

Date: _____

Email: info.qrcodekey@gmail.com

COVERED ENTITY — [CUSTOMER LEGAL NAME]

By: _____

Name: _____

Title: _____

Date: _____

Email: _____

Appendix A — Permitted Workflows for PHI Processing

Business Associate has approved the following QRCodeKey product workflows for PHI processing under this Agreement. Workflows not listed below shall not be used to process PHI without prior written authorization from Business Associate:

- Visitor management — visitor sign-in / sign-out where the visitor is identifiable as a patient or where the purpose-of-visit field discloses treatment information.
- Group attendance — staff attendance tracking where the Group includes clinical workforce members and the dataset is linked to patient encounters or scheduling.
- Custom workflows pre-approved by Business Associate in writing.

All other QRCodeKey use cases (general visitor sign-in for delivery / vendor / family-member visitors not identified as patients, staff attendance not linked to patient encounters, asset and key tracking, lost-and-found) do not involve PHI and may be used without invoking this Agreement.

Appendix B — Sub-Processor List (as of Effective Date)

Business Associate uses the following Subcontractors, each of which is bound by a written agreement that satisfies 45 C.F.R. § 164.502(e)(1)(ii):

- MongoDB Atlas (database hosting; AES-256 at rest; SOC 2 Type II) — operated by MongoDB, Inc., New York, NY, USA.
- Render, Inc. (application hosting; SOC 2 Type II) — operated by Render Services, Inc., San Francisco, CA, USA.
- Vercel Inc. (frontend hosting; SOC 2 Type II) — operated by Vercel Inc., San Francisco, CA, USA.
- Stripe, Inc. (payment processing; PCI-DSS Level 1; HIPAA-eligible only with separate BAA — Business Associate does not transmit PHI to Stripe).
- Twilio Inc. / Telnyx LLC (SMS notification — only patient-non-identifiable messages may be sent).

Business Associate shall update this list when it adds, replaces, or removes a Subcontractor that handles PHI. The current list is also published at qrcodekey.com/sub-processors.