

BUSINESS ASSOCIATE AGREEMENT

HIPAA Compliance Agreement
Agreement No. BAA-2025-HCA-00312

ARTICLE 1 — PARTIES AND EFFECTIVE DATE

This Business Associate Agreement ("BAA") is entered into as of March 1, 2025 ("Effective Date") by and between:

Pacific Wellness Hospital Network, a nonprofit corporation organized under the laws of California, with principal offices at 500 Parnassus Ave, San Francisco, CA 94143 ("Covered Entity"); and

MedSecure Data Solutions Inc., a Delaware corporation with principal offices at 100 Technology Drive, Austin, TX 78701 ("Business Associate").

ARTICLE 2 — PURPOSE

The purpose of this BAA is to establish the responsibilities of Business Associate with respect to Protected Health Information ("PHI") as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), and their implementing regulations at 45 CFR Parts 160 and 164.

ARTICLE 3 — DEFINITIONS

"Protected Health Information" or "PHI" means individually identifiable health information transmitted or maintained in any form, including electronic PHI ("ePHI"), that relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

"Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of such PHI.

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

"Compliance Standards" referenced in this BAA include HIPAA, HITECH Act, 42 CFR Part 2, and applicable state privacy laws including the California Confidentiality of Medical Information Act (CMIA).

ARTICLE 4 — PHI CATEGORIES AND USE

4.1 Categories of PHI

Business Associate may receive, create, maintain, or transmit the following categories of PHI in connection with the services provided under the underlying service agreement:

- (a) Patient Demographics — names, dates of birth, Social Security numbers, addresses, phone numbers
- (b) Clinical Records — diagnoses, treatment plans, medications, lab results, imaging reports
- (c) Insurance Information — policy numbers, group identifiers, claims history
- (d) Payment Records — billing codes, payment history, financial responsibility
- (e) Genetic Information — genetic test results, family health history

4.2 Permitted Uses

Business Associate may use and disclose PHI solely for the purpose of performing its obligations under the underlying service agreement, including: (i) data analytics and population health management; (ii) quality improvement activities; (iii) care coordination; and (iv) administrative and billing functions.

4.3 Minimum Necessary Standard

Business Associate shall limit its use, disclosure, and request for PHI to the minimum amount necessary to accomplish the intended purpose, in accordance with 45 CFR 164.502(b) and 164.514(d).

ARTICLE 5 — SAFEGUARDS AND SECURITY

5.1 Administrative Safeguards

Business Associate shall implement administrative safeguards including: (i) a designated Security Officer; (ii) workforce training on HIPAA requirements; (iii) access authorization policies; (iv) regular risk assessments; and (v) sanctions for workforce members who violate this BAA.

5.2 Physical Safeguards

Business Associate shall implement physical safeguards including: (i) facility access controls; (ii) workstation security; (iii) device and media controls; and (iv) visitor management procedures at facilities where PHI is processed.

5.3 Technical Safeguards

Business Associate shall implement technical safeguards including: (i) unique user identification; (ii) emergency access procedures; (iii) automatic logoff; (iv) encryption of ePHI at rest (AES-256) and in transit (TLS 1.3); (v) audit logging of all access to ePHI; and (vi) integrity controls to prevent unauthorized alteration of ePHI.

5.4 Data Retention

Business Associate shall retain PHI for the minimum period required by applicable law, which shall not exceed seven (7) years from the date of last activity ("Retention Period"). Upon expiration of the Retention Period, PHI shall be securely destroyed using NIST 800-88 compliant methods.

ARTICLE 6 — BREACH NOTIFICATION

6.1 Notification Timeline

Business Associate shall report to Covered Entity any Breach of Unsecured PHI within seventy-two (72) hours of discovery ("Breach Notification Window"). Discovery occurs on the first day the Breach is known or should have been known by Business Associate.

6.2 Notification Content

The Breach notification shall include: (i) identification of each individual whose PHI was involved; (ii) description of the types of PHI involved; (iii) the date of the Breach and date of discovery; (iv) description of what Business Associate is doing to investigate and mitigate the Breach; and (v) contact information for the individual coordinating the response.

6.3 Mitigation

Business Associate shall take prompt corrective action to mitigate any harmful effects of the Breach, including: (i) conducting a thorough investigation; (ii) implementing additional security measures; (iii) cooperating with Covered Entity in providing required notifications; and (iv) providing credit monitoring services to affected individuals for a minimum of twenty-four (24) months.

6.4 Cost Allocation

Business Associate shall bear all costs associated with Breach notification and remediation, including: notification costs, credit monitoring, regulatory fines, and reasonable attorneys' fees.

ARTICLE 7 — SUBCONTRACTORS

Business Associate shall not subcontract any activities involving PHI without prior written approval from Covered Entity. Any approved subcontractor must execute a BAA containing substantially the same terms and conditions as this Agreement. Business Associate shall remain liable for the acts and omissions of its subcontractors.

ARTICLE 8 — INDIVIDUAL RIGHTS

8.1 Right of Access

Business Associate shall make PHI available to Covered Entity within fifteen (15) business days of a request, to enable Covered Entity to fulfill its obligations under 45 CFR 164.524.

8.2 Right of Amendment

Business Associate shall make PHI available for amendment within fifteen (15) business days of a request from Covered Entity, per 45 CFR 164.526.

8.3 Right to an Accounting of Disclosures

Business Associate shall maintain a log of all disclosures of PHI and make such log available to Covered Entity within thirty (30) days of a request, per 45 CFR 164.528.

ARTICLE 9 — LIABILITY AND INDEMNIFICATION

9.1 Liability Cap

The total aggregate liability of Business Associate under this BAA shall not exceed Ten Million Dollars (\$10,000,000.00), except that this limitation shall not apply to: (i) Breach notification costs; (ii) regulatory fines; or (iii) claims arising from Business Associate's gross negligence or willful misconduct.

9.2 Indemnification

Business Associate shall indemnify, defend, and hold harmless Covered Entity from all claims, damages, fines, and expenses (including reasonable attorneys' fees) arising from: (i) Business Associate's breach of this BAA; (ii) any unauthorized use or disclosure of PHI; (iii) any Breach caused by Business Associate or its subcontractors; and (iv) Business Associate's violation of HIPAA or applicable state privacy laws.

ARTICLE 10 — AUDIT AND MONITORING

Covered Entity shall have the right to audit Business Associate's compliance with this BAA upon thirty (30) days written notice, not more than once per calendar year. Business Associate shall provide access to relevant facilities, systems, records, and personnel. Business Associate shall remediate any findings within sixty (60) days of the audit report.

ARTICLE 11 — TERM AND TERMINATION

11.1 Term

This BAA shall be effective as of the Effective Date and shall continue for so long as the underlying service agreement remains in effect, plus the Retention Period.

11.2 Termination for Breach

Covered Entity may terminate this BAA immediately upon written notice if Covered Entity determines that Business Associate has materially breached any provision of this BAA and has failed to cure such breach within thirty (30) days of receiving written notice.

11.3 Return or Destruction of PHI

Upon termination, Business Associate shall return or destroy all PHI in its possession within sixty (60) days, using NIST 800-88 compliant methods. Business Associate shall certify destruction in writing.

ARTICLE 12 — REGULATORY COMPLIANCE

Business Associate shall comply with all applicable federal and state regulations including: HIPAA Privacy Rule (45 CFR Part 164 Subpart E), HIPAA Security Rule (45 CFR Part 164 Subpart C), HIPAA Breach Notification Rule (45 CFR Part 164 Subpart D), HITECH Act, 42 CFR Part 2 (Substance Abuse Records), and the California CMIA.

ARTICLE 13 — GENERAL PROVISIONS

13.1 Governing Law

This BAA shall be governed by federal law (HIPAA and HITECH) and, to the extent not preempted, the laws of the State of California.

13.2 Notices

All notices shall be in writing and sent to the addresses on the signature page via certified mail or overnight courier.

13.3 Entire Agreement

This BAA constitutes the entire agreement between the Parties regarding the handling of PHI and supersedes all prior agreements on this subject.

13.4 Amendment

The Parties agree to amend this BAA as necessary to comply with changes in HIPAA regulations or other applicable law. No amendment shall be effective unless in writing and signed by both Parties.

13.5 Survival

The obligations under Articles 5, 6, 7, 9, and 10 shall survive termination of this BAA.

EXHIBIT A — PHI DATA ELEMENTS

Category	Data Elements	Sensitivity
Demographics	Name, DOB, SSN, Address, Phone, Email	High
Clinical Records	Diagnoses (ICD-10), Medications, Lab Results	Very High
Insurance	Policy No, Group ID, Claims History	High
Payment	Billing Codes (CPT), Payment History	Medium
Genetic	Genetic Test Results, Family History	Very High

SIGNATURES

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

Pacific Wellness Hospital Network
Authorized Signatory

MedSecure Data Solutions Inc.
Authorized Signatory