MASTER VENDOR SERVICES AGREEMENT

Effective Date: November 14, 2025
Document Type: Data Processing Agreement
Version: 1.0
Status: Sample Document for Compliance Testing

DISCLAIMER: *This is a sample contract generated for compliance testing purposes only. It should not be used as an actual legal agreement without proper legal review and customization for your specific requirements.*

MASTER VENDOR SERVICES AGREEMENT

This Master Vendor Services Agreement ("Agreement") is made effective as of February 10, 2025, between HealthTech Systems Inc., a Delaware corporation ("Company") and MediData Solutions LLC, a California limited liability company ("Vendor").

1. SERVICES AND DELIVERABLES

1.1 Scope of Services

Vendor agrees to provide healthcare data analytics and reporting services ("Services") as detailed in each Statement of Work (SOW) executed under this Agreement.

1.2 Performance Standards

Vendor shall perform Services in a professional and workmanlike manner, consistent with industry standards, and in compliance with all applicable laws including HIPAA, HITECH Act, and state healthcare privacy laws.

1.3 Service Levels

Response time for system issues: Critical (30 minutes), High (2 hours), Medium (8 hours), Low (24 hours). System availability: 99.95% measured monthly excluding scheduled maintenance.

2. PROTECTED HEALTH INFORMATION (PHI)

2.1 Business Associate Status

Vendor acknowledges it will receive, create, maintain, or transmit Protected Health Information (PHI) as defined under HIPAA and agrees to function as a Business Associate of Company.

2.2 HIPAA Compliance

Vendor shall comply with all applicable provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and implementing regulations at 45 CFR Parts 160 and 164.

2.3 Permitted Uses and Disclosures

Vendor shall use or disclose PHI only as permitted by this Agreement, as required by law, or as authorized by Company in writing. Specifically, Vendor may use PHI solely to:

(a) Perform Services for Company;

(b) Comply with legal requirements;

(c) For Vendor's proper management and administration if disclosure is required by law;

(d) For data aggregation services if authorized;

(e) Report violations of law to appropriate authorities.

2.4 Prohibited Uses

Vendor shall NOT use PHI for marketing purposes, fundraising, or sale of PHI without Company's express written authorization and compliance with HIPAA requirements.

2.5 Minimum Necessary Standard

Vendor shall limit PHI use, disclosure, and requests to the minimum necessary to accomplish the intended purpose, except for disclosures to or requests by healthcare providers for treatment purposes.

3. SECURITY SAFEGUARDS

3.1 Administrative Safeguards

Vendor shall implement administrative safeguards including:

(a) Security management process with risk analysis, risk management, sanction policy, and information system activity review;

(b) Assigned security responsibility with designated security official;

(c) Workforce security with authorization procedures, workforce clearance, and termination procedures;

(d) Information access management with access authorization and access establishment;

(e) Security awareness training covering security reminders, protection from malicious software, log-in monitoring, and password management;

(f) Security incident procedures for response and reporting;

(g) Contingency planning including data backup, disaster recovery, emergency operations, and testing;

(h) Business associate contracts and other arrangements;

(i) Evaluation of security controls.

3.2 Physical Safeguards

Vendor shall implement physical safeguards including:

(a) Facility access controls with contingency operations, facility security plans, access control and validation, and maintenance records;

(b) Workstation use policies restricting physical access;

(c) Workstation security to prevent unauthorized viewing;

(d) Device and media controls for disposal, media re-use, accountability, and data backup/storage.

3.3 Technical Safeguards

Vendor shall implement technical safeguards including:

(a) Access controls with unique user identification, emergency access procedures, automatic logoff, and encryption/decryption;

(b) Audit controls for hardware, software, and procedural mechanisms to record and examine system activity;

(c) Integrity controls to protect against improper alteration or destruction;

(d) Person or entity authentication to verify identities;

(e) Transmission security with integrity controls and encryption for PHI transmitted over electronic networks.

3.4 Encryption Requirements

All PHI must be encrypted at rest using FIPS 140-2 validated AES-256 encryption. PHI in transit must be encrypted using TLS 1.2 or higher. Mobile devices and removable media containing PHI must use full-disk encryption.

3.5 Password and Authentication

Multi-factor authentication is required for all remote access to systems containing PHI. Passwords must be minimum 12 characters with complexity requirements and changed every 90 days.

4. BREACH NOTIFICATION AND INCIDENT RESPONSE

4.1 Discovery and Notification

Vendor shall notify Company within 6 hours of discovery of any breach of unsecured PHI or security incident affecting PHI. "Discovery" means when Vendor or any employee, officer, or agent knew or reasonably should have known of the breach.

4.2 Required Information

Breach notification must include:

(a) Identification of each individual whose PHI was or is reasonably believed to have been accessed, acquired, used, or disclosed;

(b) Brief description of what happened, date of breach, and date of discovery;

(c) Description of PHI involved (names, SSNs, medical record numbers, etc.);

(d) Steps individuals should take to protect themselves;

(e) Vendor's investigation, mitigation actions, and corrective measures;

(f) Contact information for questions.

4.3 Investigation and Mitigation

Vendor shall immediately:

(a) Investigate the breach to determine scope and cause;

(b) Take steps to mitigate harmful effects;

(c) Document incident and response;

(d) Preserve evidence for forensic analysis;

(e) Cooperate fully with Company's investigation;

(f) Implement corrective measures to prevent recurrence.

4.4 Company Responsibilities

Company is responsible for notifying affected individuals, the Secretary of HHS, and media (if required) in accordance with HIPAA Breach Notification Rule (45 CFR § 164.400-414). Vendor shall provide all reasonable assistance.

4.5 Vendor Liability

Vendor shall be liable for costs associated with breach notification, credit monitoring, legal fees, regulatory fines, and damages resulting from breaches caused by Vendor's failure to implement required safeguards or comply with this Agreement.

5. DATA SUBJECT RIGHTS

5.1 Right of Access

Within 5 business days of Company's request, Vendor shall provide PHI to enable Company to respond to individual requests for access to their PHI under 45 CFR § 164.524.

5.2 Right to Amendment

Vendor shall make amendments to PHI as directed by Company to fulfill individual rights under 45 CFR § 164.526 within 10 business days of request.

5.3 Accounting of Disclosures

Vendor shall document all disclosures of PHI and provide an accounting to Company within 15 business days to fulfill individual requests under 45 CFR § 164.528. Accounting must include date, recipient, description of PHI, and purpose.

5.4 Right to Restrict

Vendor shall comply with Company's requests to restrict uses or disclosures of PHI to the extent required under 45 CFR § 164.522.

6. SUBCONTRACTORS AND AGENTS

6.1 Authorization

Vendor may use subcontractors to assist in performing Services only with prior written approval from Company. Current approved subcontractors are listed in Schedule A.

6.2 Subcontractor Agreements

Vendor shall enter into written agreements with all subcontractors requiring compliance with HIPAA requirements equivalent to those in this Agreement. Vendor remains liable for subcontractor acts or omissions.

6.3 Notification of Changes

Vendor shall provide 30 days' advance notice of any new subcontractors with access to PHI, allowing Company opportunity to object.

7. AUDIT AND INSPECTION RIGHTS

7.1 Company Audits

Company may audit Vendor's HIPAA compliance annually or upon reasonable suspicion of breach. Audits may be conducted by Company personnel or third-party auditors. Vendor shall provide full access to facilities, systems, records, and personnel.

7.2 Audit Notice

Company shall provide 15 business days' notice for routine audits. No notice is required for audits following suspected breaches.

7.3 Costs

Company bears costs of routine audits. Vendor bears costs if audit reveals material non-compliance.

7.4 Government Audits

Vendor shall make internal practices, books, and records available to the Secretary of HHS for purposes of determining compliance with HIPAA.

7.5 Remediation

Vendor shall remediate any deficiencies identified in audits within timelines specified by Company, generally 30 days for non-critical items and immediately for critical vulnerabilities.

8. DATA RETENTION AND DESTRUCTION

8.1 Retention Period

Vendor shall retain PHI for 6 years from creation or last use, whichever is later, unless longer retention is required by law.

8.2 Return or Destruction

Upon termination, Vendor shall, at Company's direction:

(a) Return all PHI in Vendor's possession to Company in usable electronic format within 30 days; OR

(b) Destroy all PHI and certify destruction in writing; OR

(c) Extend protections of this Agreement if return/destruction is infeasible and limit further uses/disclosures.

8.3 Secure Destruction Methods

Destruction must render PHI unreadable, indecipherable, and unable to be reconstructed using:

(a) Physical destruction (shredding, burning, pulverizing);

(b) Electronic media sanitization per NIST SP 800-88 guidelines (degaussing, overwriting, cryptographic erasure).

8.4 Certificate of Destruction

Vendor shall provide written certification specifying: (a) date of destruction; (b) method used; (c) description of PHI destroyed; (d) confirmation that all copies are destroyed; (e) signature of responsible official.

9. TRAINING AND WORKFORCE

9.1 Workforce Training

All Vendor workforce members with access to PHI must complete HIPAA training within 30 days of hire and annually thereafter. Training must cover Security Rule, Privacy Rule, Breach Notification Rule, and this Agreement.

9.2 Background Checks

Vendor shall conduct criminal background checks on all personnel with PHI access prior to granting access.

9.3 Confidentiality Agreements

All Vendor workforce members must sign confidentiality agreements before accessing PHI.

9.4 Sanctions

Vendor shall apply appropriate sanctions against workforce members who violate HIPAA requirements or this Agreement, including termination for serious violations.

10. FEES AND PAYMENT

10.1 Service Fees

Company shall pay Vendor fees as specified in each SOW. Fees are exclusive of taxes, which Company shall pay.

10.2 Payment Terms

Invoices are due 45 days after invoice date. Late payments accrue interest at 1% per month.

10.3 Expenses

Pre-approved expenses are reimbursed at cost with documentation.

11. TERM AND TERMINATION

11.1 Term

This Agreement commences on the Effective Date and continues for 3 years unless terminated earlier.

11.2 Termination for Cause

Either party may terminate immediately if the other party materially breaches and fails to cure within 10 days of written notice.

11.3 Termination for HIPAA Violation

Company may terminate immediately if:

(a) Vendor breaches HIPAA provisions;

(b) Cure is not possible; OR

(c) Vendor fails to cure breach within 30 days.

11.4 Termination for Convenience

Company may terminate with 60 days' written notice. Vendor pays Company prorated refund of prepaid unused services.

11.5 Obligations Upon Termination

Upon termination: (a) Vendor returns/destroys PHI per Section 8; (b) Vendor delivers all work product; (c) Company pays for services rendered through termination date; (d) Sections 2-9, 12-15 survive.

12. REPRESENTATIONS AND WARRANTIES

12.1 Authority

Each party represents it has full authority to enter this Agreement.

12.2 Compliance

Vendor warrants: (a) Services comply with all laws including HIPAA; (b) no conflicts with other agreements; (c) personnel are qualified and trained; (d) security measures are implemented and maintained.

12.3 No Conflicts

Vendor represents no conflicts of interest exist that would impair performance.

13. INDEMNIFICATION

13.1 Vendor Indemnification

Vendor shall defend, indemnify, and hold harmless Company from all claims, damages, fines, penalties, and costs (including attorneys' fees) arising from:

(a) Vendor's breach of HIPAA requirements;

(b) Unauthorized use or disclosure of PHI by Vendor;

(c) Security incidents caused by Vendor's negligence;

(d) Vendor's breach of this Agreement;

(e) Vendor's violation of laws or regulations.

13.2 Notice and Defense

Company shall promptly notify Vendor of claims, allow Vendor to control defense (with Company's reasonable participation), and cooperate in defense.

13.3 Regulatory Penalties

Vendor is liable for HIPAA civil monetary penalties assessed against Company due to Vendor's violations. This includes penalties up to $1.5 million per violation category per year.

14. LIMITATION OF LIABILITY

14.1 Cap on Liability

EXCEPT FOR EXCLUDED CLAIMS, VENDOR'S LIABILITY SHALL NOT EXCEED FEES PAID IN THE 12 MONTHS PRECEDING THE CLAIM.

14.2 Excluded Claims

Cap does not apply to: (a) HIPAA violations; (b) data breaches; (c) indemnification obligations; (d) willful misconduct or gross negligence; (e) violations of confidentiality; (f) payment obligations.

14.3 No Consequential Damages Limitation for PHI Breaches

For claims involving PHI breaches or HIPAA violations, there is NO limitation on consequential, indirect, or punitive damages.

15. INSURANCE

15.1 Required Coverage

Vendor shall maintain:

(a) Cyber liability and privacy breach insurance: $10 million per occurrence;

(b) Professional liability insurance: $5 million per occurrence;

(c) General liability insurance: $3 million per occurrence;

(d) Workers' compensation as required by law.

15.2 Proof of Insurance

Vendor shall provide certificates naming Company as additional insured within 10 days of request.

16. CONFIDENTIALITY

16.1 Non-PHI Confidential Information

Vendor shall protect Company's Confidential Information (non-PHI) with same care as its own confidential information, but no less than reasonable care.

16.2 Proprietary Information

All work product, inventions, and intellectual property developed under this Agreement belong exclusively to Company.

17. GENERAL PROVISIONS

17.1 Governing Law

This Agreement is governed by federal HIPAA regulations and California state law.

17.2 Dispute Resolution

Disputes shall be resolved through good-faith negotiation, then mediation, then binding arbitration in San Francisco, California under AAA Healthcare Payor Provider Arbitration Rules.

17.3 Notices

All notices shall be sent to:

Company: HealthTech Systems Inc., Legal Department, 555 Healthcare Way, Boston, MA 02101, legal@healthtechsys.com

Vendor: MediData Solutions LLC, Compliance Office, 888 Data Center Blvd, San Diego, CA 92101, compliance@medidatasol.com

17.4 Entire Agreement

This Agreement, including all SOWs and schedules, constitutes the entire agreement between the parties.

17.5 Amendments

Amendments must be in writing signed by both parties, except Company may amend to comply with HIPAA changes upon 30 days' notice.

17.6 Severability

Invalid provisions are severed; remaining provisions remain in effect.

17.7 Assignment

No assignment without prior written consent, except to successor in merger/acquisition.

IN WITNESS WHEREOF, the parties have executed this Agreement effective as of the date first written above.

COMPANY: HealthTech Systems Inc. By: _____ Name: Dr. Robert Williams Title: Chief Medical Information Officer Date: February 10, 2025

VENDOR: MediData Solutions LLC By: _____ Name: Patricia Anderson Title: Chief Executive Officer Date: February 10, 2025

SCHEDULE A - APPROVED SUBCONTRACTORS

1. AWS (Amazon Web Services) - Cloud hosting infrastructure

2. DataSecure Inc. - Encryption and key management services 3. AnalyticsPro - Healthcare data analytics processing 4. ComplianceTrack - HIPAA compliance monitoring tools

SCHEDULE B - SERVICE LEVEL METRICS

| Metric | Target | Measurement | Remedy | |--------|--------|-------------|---------| | System Availability | 99.95% | Monthly | 5% credit per 0.1% below target | | Critical Issue Response | 30 min | Per incident | $500 penalty per violation | | Data Processing Accuracy | 99.9% | Quarterly audit | Reprocessing at no charge | | Scheduled Maintenance | <4 hours/month | Monthly | Must not exceed without approval |

SIGNATURE PAGE

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

CONTROLLER	PROCESSOR
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____