

UT-HIP DATA HOSTING AGREEMENT

This Data Hosting Agreement ("Agreement") is entered into as of [EFFECTIVE DATE] ("Effective Date") by and between The University of Texas Health Science Center at Houston, a component institution of The University of Texas System, on behalf of The University of Texas Health Intelligence Platform, with its principal place of business at 7000 Fannin Street, Houston, TX 77030 ("Host"); and **[INSTITUTION NAME]**, a component institution of the University of Texas System, with its principal place of business at [Address] for the benefit of [Researcher] an individual employed by the Institution (collectively "Researcher"). Host and Researcher are each a "Party" and collectively the "Parties."

WHEREAS, UT-HIP serves as a System-wide health intelligence platform that leverages data, technology, and collaboration across the UT Health Enterprise to support clinical operations, research, and improved health outcomes; and

WHEREAS, Researcher desires to deposit certain data sets with Host for secure storage and management; and

WHEREAS, Host is willing to provide data hosting services subject to the terms and conditions set forth herein;

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein, and for other good and valuable considerations, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. DEFINITIONS

As used in this Agreement, the following terms have the meanings set forth below:

"Applicable Law" means all federal, state, and local laws, regulations, rules, and guidance applicable to the handling, storage, transmission, or use of the Data, including without limitation HIPAA, the HITECH Act, the Common Rule (45 C.F.R. Part 46), and any implementing regulations as amended from time to time.

"Authorized Purpose" means the research, academic, or programmatic activities described in Exhibit A, which Researcher has certified are authorized under all Applicable Law.

"Breach" has the meaning ascribed to it under the HITECH Act (42 U.S.C. § 17921) and its implementing regulations (45 C.F.R. § 164.402), and more broadly means any actual or reasonably suspected unauthorized acquisition, access, use, or disclosure of Data that compromises the security or privacy of the Data.

"Data" means all data sets, files, records, and associated metadata that Researcher submits to Host under this Agreement, as further described in Exhibit A.

"Data Subject" means any natural person whose information is contained in or derivable from the Data.

"De-Identified Data" has the meaning set forth at 45 C.F.R. § 164.514(a)-(b) or, where non-HIPAA data is involved, data processed to reasonably eliminate the ability to identify a natural person using generally accepted standards.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191), and its implementing regulations at 45 C.F.R. Parts 160, 162, and 164, as amended.

"HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, enacted as Division A, Title XIII and Division B, Title IV of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), and any implementing regulations, as amended.

"Hosting Platform" means the secure computing infrastructure, systems, software, and facilities operated by Host on which the Data will be stored and made accessible in accordance with this Agreement.

"Protected Health Information" or "PHI" has the meaning ascribed to it under HIPAA (45 C.F.R. § 160.103).

"Required Authorizations" means, collectively, all institutional review board ("IRB") approvals or waivers, data governance approvals, informed consents or waivers thereof, data use agreements, material transfer agreements, federal or sponsor authorizations, and any other permissions, licenses, or regulatory clearances required by Applicable Law or any institutional policy for Researcher to collect, hold, transfer, and otherwise process the Data for the Authorized Purpose.

"Security Incident" has the meaning set forth at 45 C.F.R. § 164.304, and more broadly means any attempted or actual unauthorized access, use, disclosure, modification, or destruction of Data, or any interference with system operations.

"Services" means the data hosting services provided by Host under this Agreement, as set forth in Exhibit B.

2. HOSTING SERVICES

2.1. Provision of Services. Host shall provide to Researcher the Services described in Exhibit B, including secure storage of the Data on the Hosting Platform in accordance with the Researcher Certification Form set forth in Exhibit C and all Applicable Law.

2.2. Access Controls. Host shall implement and maintain commercially reasonable administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of the Data. Access to the Data shall be limited to personnel with a documented need to know and who are bound by written obligations of confidentiality no less protective than those set forth in this Agreement.

2.3. No Ownership; Custodial Role. Host acknowledges that, subject to UT System Regents Rule 90101, as between the Parties, Researcher retains all right, title, and interest in and to the Data. Host's role is that of a data custodian and, where Applicable Law requires, a business associate (as defined under HIPAA), which will only occur in situations where a separate Business Associate Agreement ("BAA") is signed and agreed to. Host shall not use the Data for any purpose other than performing the Services.

2.4. Subprocessors and Subcontractors. Host shall use reasonable efforts to ensure subprocessors or subcontractors are not engaged to process or store the Data without

Researcher's prior written approval. Any approved subprocessor shall be bound by data protection obligations at least as stringent as those in this Agreement.

2.5. HIPAA Business Associate Provisions. To the extent the Data contains PHI and Host is acting as a business associate of Researcher, the Parties shall execute a Business Associate Agreement.

3. RESEARCHER RESPONSIBILITIES AND CERTIFICATIONS

3.1. Authority and Required Authorizations — Certification. Prior to submitting any Data to Host, and as a continuing obligation throughout the Term, Researcher represents, warrants, and certifies that:

- (a) Researcher has obtained all Required Authorizations for the collection, transfer, storage, and use of each Data set submitted under this Agreement;
- (b) The submission of Data to Host and the hosting of Data on the Hosting Platform are within the scope of and consistent with all Required Authorizations;
- (c) To the extent any Required Authorization has a defined scope, term, or data category limitation, Researcher has not submitted Data or directed any use that exceeds such limitations;
- (d) Where applicable, Researcher has complied with the Common Rule (45 C.F.R. Part 46) and any applicable state human subjects research statutes, including obtaining IRB approval or a valid waiver of such approval, prior to submitting Data involving human subjects;
- (e) Researcher has the legal authority to bind the institution or entity identified as Researcher herein, and all internal institutional approvals (including data governance reviews, sponsored research office approvals, and technology transfer approvals) necessary for execution and performance of this Agreement have been obtained; and
- (f) **Researcher** is employed by a state of Texas institution who is participating in The University of Texas Health Intelligence Platform
- (g) Researcher will promptly notify Host in writing if any Required Authorization is revoked, lapses, or is amended in a manner that restricts or prohibits the continued hosting of any Data and will cooperate with Host in taking any corrective action required by Applicable Law.

3.2. Data Quality and Accuracy. Researcher is solely responsible for the accuracy, quality, integrity, and lawfulness of the Data submitted, and for ensuring that the Data has been de-identified, anonymized, or limited to categories consistent with any Required Authorizations

before submission, to the extent required by Applicable Law or by the applicable IRB or consent documents.

3.4. Compliance with Applicable Law. Researcher shall comply with all Applicable Law governing the Data, including, without limitation, HIPAA, the HITECH Act, the Common Rule, the Family Educational Rights and Privacy Act ("FERPA") where applicable, and any state privacy or data protection statutes applicable to the Data or the Data Subjects.

3.5. Permitted Uses. Researcher shall access and use the Data on the Hosting Platform solely for the Authorized Purpose and shall not direct Host to process, use, or disclose Data in any manner inconsistent with the Required Authorizations or Applicable Law.

4. DATA BREACH NOTIFICATION AND RESPONSE

4.1. Host Notification Obligation. Host shall notify Researcher without unreasonable delay, and in no event later than five days after Host's discovery of a Breach or Security Incident affecting the Data, by contacting Researcher's designated privacy/security contact identified in Exhibit A. Such notification shall include, to the extent then known: (a) the date and nature of the Breach; (b) the categories and approximate number of Data Subjects affected; (c) the categories and approximate volume of Data records involved; (d) a description of the likely consequences; (e) the measures Host has taken or proposes to take to address the Breach; and (f) the name and contact information of Host's responsible contact.

4.2. Researcher Retains Notification Responsibility. Notwithstanding any role Host plays in the initial detection and reporting of a Breach, Researcher acknowledges and agrees that:

(a) Researcher Obligation to Notify Data Subjects. Researcher is and remains solely responsible for providing all legally required notifications to Data Subjects whose information may have been involved in a Breach. This obligation arises from Researcher's status as the data controller, covered entity, or other responsible party under Applicable Law with respect to the Data Subjects, and Host's custodial role does not transfer, diminish, or discharge this obligation.

(b) Regulatory Notifications. Researcher is and remains solely responsible for making all required notifications to governmental authorities, regulators, and oversight bodies (including the U.S. Department of Health and Human Services Office for Civil Rights and, where applicable, state attorneys general) arising from a Breach involving the Data.

(c) Timeliness. Researcher shall provide all required Data Subject and regulatory notifications within the timeframes mandated by Applicable Law (including the sixty (60)-day notification period under the HITECH Act, 45 C.F.R. § 164.404, and any applicable state breach notification statutes, which may impose shorter timelines).

(d) Host's Assistance. Host shall provide reasonable cooperation and assistance to Researcher in connection with any Breach investigation and notification, including providing relevant logs, records, and forensic information in Host's possession to the extent permitted by Applicable Law, at Researcher's reasonable cost and expense unless the Breach was caused by Host's failure to meet its obligations under this Agreement, in which case Host shall bear the costs of its own cooperation.

(e) No Admission. Nothing in this Section 4.2 constitutes an admission by either Party as to fault or liability for any Breach.

4.3. Breach Response Protocol. Upon discovery or notification of a Breach, Host shall promptly: (a) take all commercially reasonable steps to contain and mitigate the Breach; (b) preserve all relevant evidence and logs; (c) cooperate with Researcher's designated privacy officer or outside counsel; and (d) not make any public statement or press release concerning the Breach without Researcher's prior written consent, except to the extent required by Applicable Law.

5. SECURITY STANDARDS AND COMPLIANCE

5.1. Federal Law Compliance. Host shall maintain the Hosting Platform and perform the Services in compliance with all Applicable Law.

5.2. Personnel. Host shall ensure that all personnel with access to the Data receive appropriate training on data privacy and security obligations consistent with Applicable Law and are bound by written confidentiality obligations at least as protective as those in this Agreement.

6. REPRESENTATIONS AND WARRANTIES

6.1. Mutual Representations. Each Party represents and warrants that: (a) it is duly organized, validly existing, and in good standing under applicable law; (b) it has full power and authority to execute, deliver, and perform this Agreement; (c) this Agreement has been duly authorized, executed, and delivered by such Party and constitutes a legal, valid, and binding obligation enforceable against it in accordance with its terms; and (d) the execution and performance of this Agreement will not violate any other agreement to which it is a party.

6.2. Researcher Representations and Warranties. Researcher additionally represents and warrants, as of the Effective Date and on a continuing basis throughout the Term, that:

- (a) All Required Authorizations have been obtained, are in full force and effect, and are sufficient in scope to authorize the submission, storage, and use of the Data as contemplated by this Agreement;
- (b) The Data does not contain information that Researcher is prohibited from disclosing under any contractual, regulatory, or legal obligation;
- (c) Researcher has not made and will not make any misrepresentation to any IRB, data governance committee, sponsor, or regulatory authority in connection with the Required Authorizations;
- (d) All Data Subjects, where legally required to have consented, have provided valid, informed consent to the collection, use, and disclosure of their information in a manner consistent with the Authorized Purpose; and
- (e) Researcher has the institutional authority to execute this Agreement on behalf of the institution identified as Researcher herein and has obtained all necessary internal approvals to do so.

6.3. Disclaimer. EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER PARTY MAKES ANY WARRANTY, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. HOST DOES NOT WARRANT THAT THE HOSTING PLATFORM WILL BE UNINTERRUPTED OR ERROR-FREE.

7. TERM AND TERMINATION

7.1. Term. This Agreement shall commence on the Effective Date and shall continue for a period of [7 year(s)] (the "Initial Term"), unless earlier terminated in accordance with this Section 7.

7.2. Termination for Convenience. Either Party may terminate this Agreement for any reason upon ninety (90) days' prior written notice to the other Party.

7.3. Termination for Cause. Either Party may terminate this Agreement immediately upon written notice if: (a) the other Party materially breaches this Agreement and fails to cure such breach within thirty (30) days after receipt of written notice specifying the breach in reasonable detail; or (b) the other Party becomes insolvent, makes a general assignment for the benefit of its creditors, or is the subject of any bankruptcy, insolvency, or reorganization proceeding.

7.4. Effect of Termination; Data Return and Destruction. Upon expiration or termination of this Agreement: (a) Researcher may, within sixty (60) days following the effective date of termination (the "Retrieval Period"), retrieve a complete copy of the Data from the Hosting Platform in a mutually agreed-upon format; (b) following the Retrieval Period, Host shall, at Researcher's election and upon written instruction, securely destroy or return all Data in Host's possession, including all copies and backup copies, and certify such destruction in writing; (c) all accrued payment obligations shall survive; and (d) all obligations relating to Data Subjects whose data was hosted shall survive to the extent required by Applicable Law.

7.5. Suspension. Host may suspend access to the Hosting Platform immediately, with prior notice to the extent practicable, if: (a) Host reasonably believes continued operation poses an imminent risk to the security of the Data; (b) Researcher is in material breach of this Agreement; or (c) continuation would violate Applicable Law. Host shall provide written notice of any suspension as soon as practicable and shall restore access promptly upon resolution of the underlying issue.

8. CONFIDENTIALITY

8.1. Confidential Information. Each Party (as a "Receiving Party") agrees to hold the other Party's Confidential Information in confidence, using at least the same degree of care it uses to protect its own confidential information, but in no event less than reasonable care, and shall not use or disclose such Confidential Information except as required to perform its obligations or exercise its rights under this Agreement. "Confidential Information" means any non-public information disclosed by one Party to the other that is designated as confidential or that reasonably should be understood to be confidential, including the Data, the terms of this Agreement, security architecture of the Hosting Platform, and Required Authorizations.

8.2. Exceptions. Confidentiality obligations do not apply to information that: (a) is or becomes publicly available through no fault of the Receiving Party; (b) was known to the Receiving Party prior to disclosure without restriction; (c) is rightfully received from a third party without restriction; or (d) is independently developed by the Receiving Party without reference to the Confidential Information.

8.3. Required Disclosure. If a Receiving Party is required by Applicable Law, court order, or regulatory requirement to disclose Confidential Information, it shall, to the extent permitted by law: (a) promptly notify the Disclosing Party prior to disclosure; (b) cooperate with the Disclosing Party in seeking a protective order or other appropriate relief; and (c) disclose only that portion of the Confidential Information that is legally required to be disclosed.

9. GENERAL PROVISIONS

9.1. Governing Law; Dispute Resolution. This Agreement shall be governed by and construed in accordance with the laws of the State of Texas.

9.2. Entire Agreement; Amendments. This Agreement, together with all Exhibits, constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior negotiations, representations, or agreements, whether oral or written. This Agreement may only be amended by a written instrument signed by authorized representatives of both Parties.

9.3. No Waiver. The failure of either Party to exercise any right or remedy provided under this Agreement shall not constitute a waiver of that right or remedy.

9.4. Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect, and the Parties shall negotiate in good faith to replace the invalid or unenforceable provision with one that, to the greatest extent possible, achieves the same commercial and legal effect.

9.5. Assignment. Neither Party may assign this Agreement or any rights or obligations hereunder without the other Party's prior written consent, which shall not be unreasonably withheld, except that either Party may assign this Agreement without consent in connection with a merger, or acquisition of all or substantially all of its assets to another similarly situated state agency, provided the assignee assumes all obligations under this Agreement. Any purported assignment in violation of this Section is void.

9.6. Notices. All notices under this Agreement shall be in writing and delivered by: (a) overnight courier with tracking; (b) certified mail, return receipt requested; or (c) email with confirmation of receipt, to the addresses set forth in Exhibit A, or such other address as a Party may designate in writing. Notices are effective upon receipt.

9.7. Force Majeure. Neither Party shall be liable for delays or failures in performance resulting from causes beyond its reasonable control (each, a "Force Majeure Event"), provided that: (a) the affected Party provides prompt written notice to the other Party; and (b) the affected Party uses commercially reasonable efforts to mitigate the impact and resume performance. If a Force Majeure Event affecting Host continues for more than thirty (30) days, Researcher may terminate this Agreement for convenience without penalty, and Host shall cooperate with Data retrieval on an expedited basis.

9.8. Survival. Sections 1 (Definitions), 4 (Data Breach — notification obligations only), 6 (Representations and Warranties), 7.4 (Effect of Termination; Data Return and Destruction), 8 (Confidentiality), 9.4 (Severability), and this Section 9 shall survive the expiration or termination of this Agreement.

9.9. Counterparts; Electronic Signatures. This Agreement may be executed in counterparts, each of which shall be deemed an original, and all of which together shall constitute one instrument. Electronic signatures shall be deemed valid and binding.

9.10 Researcher acknowledges that Host is an Agency of the State of Texas and as such performance by Host under this Agreement may be dependent upon the appropriation and allotment of funds by the Texas State Legislature (the "Legislature") and/or allocation of funds by the Board of Regents of The University of Texas System (the "Board"). If the Legislature fails to appropriate or allot the necessary funds, or the Board fails to allocate the necessary funds, then Host will issue written notice to Researcher and Host may terminate this Agreement without further duty or obligation hereunder. Researcher acknowledges that appropriation, allotment, and allocation of funds are beyond the control of Host.

SIGNATURE PAGE

IN WITNESS WHEREOF, the authorized representatives of the Parties have executed this Data Hosting Agreement as of the Effective Date.

HOST:

The University of Texas Health Science
Center at Houston

RESEARCHER:

[RESEARCHER / INSTITUTION]

By: _____

Name: _____

Title: _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT A — DATA DESCRIPTION AND CONTACT INFORMATION

A.1 Description of Data

[Describe the data sets to be hosted, including data type (e.g., clinical records, survey data, genomic data), approximate volume, format, and whether Data contains PHI, PII, or other regulated categories.]

A.2 Authorized Purpose

[Describe the research or programmatic activities for which the Data will be used. Reference applicable grant number, IRB protocol number, or other governing approval.]

A.3 Contact Information

HOST Privacy/Security Contact:

Name: John Flores

Title: Chief Information Security Officer

Email: uthip@utsystem.edu

RESEARCHER Privacy/Security Contact (for Breach notification):

Name: _____

Title: _____

Email: _____

Phone: _____

EXHIBIT B — DESCRIPTION OF HOSTING SERVICES

[Describe the specific services to be provided, including: (1) storage capacity and infrastructure; (2) access methods (web portal, API, secure FTP, etc.); (3) uptime/availability commitments and SLA terms; (4) backup frequency and retention; (5) any data processing or computation services; and (6) support and maintenance terms.]

1. Infrastructure and Storage

Cloud-based, secure, and scalable infrastructure on Azure/Fabric based UT-HIP platform.

Support for structured and unstructured data across segregated environments

Each project has its own separate data hosting container within the UT-HIP platform.

2. Access Methods

Secure access to hosting using platform provided mechanism (e.g., Fabric UX, SFTP).

Role-based access control is integrated with enterprise identity systems (e.g., Entra ID).

3. Availability and SLA

Target availability of based on Azure uptime, excluding scheduled maintenance.

Response times based on incident severity, with immediate action for critical issues.

4. Backup and Retention

Regular automated backups, leveraging Azure infrastructure and capabilities

Retention and restore capabilities aligned with platform policy standards.

5. Data Processing

Support for data ingestion, transformation, and analytics workloads.

Monitoring and logging platform activity for governance and audit.

6. Security, Support, and Maintenance

Enforcement of least-privilege access and continuous monitoring.

Routine patching, maintenance, and security updates.

Technical support for incidents, access issues, and platform operations.

EXHIBIT C — RESEARCHER CERTIFICATION FORM

The undersigned authorized representative of [RESEARCHER / INSTITUTION NAME] ("Researcher") hereby certifies, represents, and warrants the following in connection with the Data Hosting Agreement dated [EFFECTIVE DATE] (the "Agreement"):

1. **Required Authorizations.** Researcher has obtained all Required Authorizations (as defined in the Agreement) necessary to collect, hold, transfer to Host, and use the Data described in Exhibit A for the Authorized Purpose. A list of all applicable IRB protocol numbers, waivers, consent forms or waivers thereof, data governance approvals, and sponsor authorizations is attached hereto.
2. **Scope Compliance.** The submission of the Data to Host and the continued hosting of the Data on the Hosting Platform are within the scope of, and consistent with, all Required Authorizations. No submission exceeds the scope, data category limitations, or term of any Required Authorization.
3. **Human Subjects Compliance.** To the extent the Data was derived from human subjects research, Researcher has complied with the Common Rule (45 C.F.R. Part 46), all applicable state human subjects protection statutes, and all applicable sponsor requirements. Researcher has obtained IRB approval or a valid waiver of IRB approval for each applicable protocol, and such approval or waiver remains in full force and effect.
4. **Data Subject Notification Responsibility.** Researcher acknowledges and accepts sole responsibility for providing all legally required notifications to Data Subjects and regulatory authorities in the event of a Breach involving the Data, in accordance with Section 4.2 of the Agreement and Applicable Law.
5. **Institutional Authority.** The undersigned has full authority to execute the Agreement and this Certification on behalf of Researcher, and all necessary internal institutional approvals have been obtained.
6. **No Misrepresentation.** Researcher has not made, and will not make, any material misrepresentation to any IRB, data governance body, sponsor, or regulatory authority in connection with the Required Authorizations.
7. **Prompt Notification.** Researcher will promptly notify Host in writing if any Required Authorization is revoked, lapses, is amended in a manner that restricts continued hosting of any Data, or if Researcher becomes aware of any violation of Applicable Law in connection with the Data.

I certify that the foregoing is true and correct to the best of my knowledge and belief, and that I am authorized to make this certification on behalf of Researcher.

Signature: _____

Printed Name: _____

Title: _____

Institution: _____

Date: _____

IRB Protocol No(s): _____