

AGREEMENT FOR USE OF CENTER FOR HEALTH INFORMATION AND ANALYSIS DATA

This Data Use Agreement (“Agreement”) is effective on the date of its last signature (“Effective Date”), by and between the Center for Health Information and Analysis (“CHIA”) and Organization Name (“Data Recipient”) (each a “Party” and together the “Parties”).

This Agreement relates to CHIA’s approval of Data Recipient’s use of CHIA Data for the purposes described in its application titled “Project Title” and attached hereto as **Exhibit A**.

This Agreement sets forth the terms and conditions pursuant to which CHIA will release, and the Data Recipient will access, use, and disclose any data provided by CHIA.

For purposes of this Agreement, the following terms shall have the following meanings:

“Authorized User” means any individual associated with the Data Recipient or a Third Party approved by CHIA to access CHIA Data under this Agreement.

“CHIA Data” means any and all data, including identifiable and de-identified data, information, records, files, databases, reports, analyses, or other materials provided by CHIA to the Data Recipient under this Agreement.

“Data Application” means the application to access CHIA Data submitted by the Data Recipient and attached to this Agreement as **Exhibit A**.

“Data Breach” means any access, use, or disclosure of CHIA Data not authorized under this Agreement or applicable law.

“De-Identified Data” means health care information concerning an individual patient, insurance member, or recipient of health care services that does not identify such individual and with respect to which there is no reasonable basis to believe the information can be used to identify such individual. CHIA Data may be de-identified using methods such as those that satisfy the requirements of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-1320d-8, and its implementing regulations at 45 C.F.R. § 164.514(a)-(c), including the Safe Harbor method or the Expert Determination method.

“Project” means the specific research, analysis, study, or other activity described in and approved under the Data Application.

“Third Party” means any person, organization, governmental body, or other legal entity, other than the Data Recipient, that works on behalf of, under the direction of, or in connection with the Data Recipient, including but not limited to contractors, subcontractors, agents, and any successors or assigns of any of the foregoing. This definition includes any such person or entity regardless of the nature, form, or legal basis of the relationship with the Data Recipient, whether contractual, employment-based, agency, fiduciary, or otherwise, and regardless of whether such relationship is formal or informal, direct or indirect, temporary or permanent, paid or unpaid, or whether such person or entity is located within or outside the United States. The definition of Third Party shall be construed broadly to encompass any person or entity that

could potentially receive or access CHIA Data as a result of the Data Recipient's possession, use, or control of such CHIA Data. An individual associated with a Third Party must become an Authorized User before it may receive, access, use, store, process, transmit, or otherwise come into contact with CHIA Data.

1. Representations and Warranties

1.1. Mutual Representations and Warranties

Each Party represents and warrants to the other Party that:

- (a) It has full power and authority to enter into this Agreement and to perform its obligations hereunder;
- (b) The execution, delivery, and performance of this Agreement have been duly authorized by all necessary action; and
- (c) No consent, approval or authorization is required for its execution or performance of this Agreement that has not been obtained.

1.2. Data Recipient Representations and Warranties

Data Recipient represents and warrants to the CHIA that:

- (a) The representations made in the Data Application, and any other statements or documentation submitted to CHIA in support of such Data Application, were true, complete, and accurate as of the date submitted and continue to be true, complete, and accurate;
- (b) Data Recipient is in compliance with all applicable federal, state, and local laws and regulations relating to data protection, privacy, and information security;
- (c) Data Recipient has implemented and maintains administrative, physical, and technical safeguards sufficient to protect CHIA Data in accordance with the Standards and other requirements established in this Agreement;
- (d) All Authorized Users have received training on data handling, confidentiality, and security requirements applicable to CHIA Data;
- (e) Data Recipient's use of CHIA Data will not exceed the scope or purposes approved in this Agreement;
- (f) Data Recipient is aware of and will comply with all applicable breach notification requirements;
- (g) Data Recipient has not had its access to data revoked, suspended, or terminated by any federal, state, or local governmental authority, or any other data custodian, for any violation of a data use agreement, data security incident, breach of confidentiality, or any other reason relating to the misuse or mishandling of data; and
- (h) There is no pending or, to Data Recipient's knowledge, threatened litigation, investigation, or proceeding that would materially affect Data Recipient's ability to perform its obligations under this Agreement.

2. Data Use

2.1. General Terms

The Data Recipient shall comply with this Agreement to ensure that the privacy, security, and related obligations of the Data Recipient are met. The Data Recipient shall not access, use, or disclose CHIA Data except as permitted under this Agreement. The Data Recipient shall ensure that all Authorized Users comply with the relevant terms and conditions of this Agreement and any amendments to this Agreement.

2.2. Restrictions on Use

The Data Recipient's use of CHIA Data is strictly limited to the Project. Any other use of CHIA Data is prohibited. The Data Recipient shall not use De-Identified Data received from CHIA to identify any person for any purpose. Any attempt to re-identify individuals from De-Identified Data, whether successful or not, shall constitute a material breach of this Agreement and a violation of M.G.L. c. 12C, § 12(e) and 957 CMR 5.07(3). The Data Recipient shall not link, match, or combine CHIA Data with any other data or information, whether from internal or external sources, except as expressly described and approved in the Data Application or as subsequently authorized in writing by CHIA.

2.3. Legally Protected Healthcare Activity

The Data Recipient agrees to comply with all applicable Massachusetts laws regarding a Legally Protected Healthcare Activity, as defined in M.G.L. c. 12 § 1111/2, including but not limited to M.G.L. c. 12C § 12 and any related regulations or guidance.

The Data Recipient shall withhold access to any CHIA Data or any other data or information derived by CHIA Data that would allow the identification of a patient or provider, in response to any inquiry or investigation into services constituting a Legally Protected Health Care Activity, except as required by federal law.

The Data Recipient shall immediately notify CHIA of any conflict between this section and the Data Recipient's other legal obligations and shall not use CHIA Data to fulfill those or otherwise respond to those other legal obligations without CHIA's prior written consent.

2.4. Artificial Intelligence

The Data Recipient shall not use, store, or upload CHIA Data into an environment that utilizes artificial intelligence, including but not limited to generative artificial intelligence, or use CHIA Data to train an artificial intelligence model, unless previously authorized in writing by CHIA. For purposes of this Agreement, artificial intelligence has the meaning set forth in 15 U.S.C. 9401(3) and is defined as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments."

2.5. Prohibition on Contact with Individuals

Unless authorized by CHIA in writing, the Data Recipient, Authorized Users, and Third Parties shall not attempt to contact, communicate with, or otherwise reach out to any individual whose information is contained in CHIA Data, whether directly or indirectly, and regardless of the method of contact, including but not limited to telephone, email, text messaging, postal mail, social media, or in-person contact. This prohibition applies to any contact attempt for any purpose whatsoever, including but not limited to verification of information, recruitment for studies or surveys, marketing, or any other communication.

Any contact authorized by CHIA must be conducted in strict compliance with all applicable federal and state laws and regulations, including but not limited to privacy, confidentiality, and data protection requirements, as well as any additional conditions, restrictions, or requirements imposed by CHIA.

2.6. Prohibition on Patient Investigations and Liability

The Data Recipient acknowledges that pursuant to M.G.L. c. 12C, § 12(f), a recipient of CHIA Data shall not use such information to: (i) conduct a criminal, civil or administrative investigation into any individual patient; or (ii) impose criminal, civil or administrative liability on any individual patient. Accordingly, the Data Recipient, Authorized Users, and Third Parties shall not use CHIA Data, either directly or indirectly, to: (i) conduct, facilitate, contribute to, or support any criminal, civil, or administrative investigation into any individual patient; or (ii) impose, seek to impose, facilitate the imposition of, or support the imposition of any criminal, civil, or administrative liability on any individual patient.

This prohibition includes, without limitation: (a) using CHIA Data as evidence, testimony, or support in any legal, administrative, or regulatory proceeding against an individual patient; (b) using CHIA Data to identify individuals for the purpose of subjecting them to investigation or liability; (c) providing CHIA Data to any Third Party for the purpose of conducting investigations or imposing liability on individual patients; (d) creating analyses, reports, or other materials based on CHIA Data that are intended to be used in proceedings against individual patients; (e) any other use of CHIA Data that directly or indirectly contributes to, supports, or facilitates investigation or liability of individual patients; and (f) permitting, authorizing, or enabling any person or entity to use CHIA Data for any of the foregoing prohibited purposes.

The Data Recipient acknowledges that pursuant to M.G.L. c. 12C, § 12(i), a violation of M.G.L. c. 12C, § 12(f) or any rule or regulation issued thereunder shall constitute a violation of M.G.L. c. 93A.

3. Authorized Users and Contractors

3.1. CHIA Approval Required

CHIA approval is required for any individual to become an Authorized User. Individuals listed on the Data Application are considered Authorized Users as of the Effective Date of this Agreement.

3.2. Minimum Necessary

Access to CHIA Data shall be limited to the minimum amount of data and minimum number of Authorized Users necessary to complete the Project for which CHIA Data was released.

3.3. Adding or Removing Authorized Users

The Data Recipient must provide CHIA with written notice at least five (5) business days prior to the addition or removal of any Authorized Users. For each proposed new Authorized User, the Data Recipient must submit to CHIA the individual's name, title, organizational affiliation, role in the Project, and a brief description of such individual's need for access to CHIA Data.

For individuals associated with a Third Party, the Data Recipient must also provide: (i) the name of the Third Party entity; (ii) a description of the Third Party's role in the Project and the bases for its relationship with the Data Recipient; and (iii) confirmation that a written agreement as required by **Section 3.4** is in place or will be executed prior to data access.

CHIA reserves the right, in its sole discretion, to reject any proposed Authorized User for any reason or no reason, and such rejection shall not be subject to appeal or review. Upon receipt of CHIA's written approval, the Data Recipient may grant the approved individual access to CHIA Data as an Authorized User, subject to all terms and conditions of this Agreement.

The Data Recipient must immediately revoke access to CHIA Data for any Authorized User who: (i) no longer requires access to perform duties related to the approved Project; (ii) ceases to be employed by or affiliated with the Data Recipient or any Third Party; (iii) violates any provision of this Agreement; or (iv) is requested to be removed by CHIA.

3.4. Approval of Third Party Individual as Authorized User

An individual associated with a Third Party must become an Authorized User in the manner described in **Section 3.3**. For the avoidance of doubt, Third Party individuals included in the Data Recipient's approved Data Application are Authorized Users as of the Effective Date of this Agreement, subject to the written agreement requirement set forth below.

Before any Third Party individual is granted access to CHIA Data, the Data Recipient must enter into a written agreement with that individual's Third Party that binds the Third Party to the same privacy, security, and use restrictions applicable to the Data Recipient under this Agreement, including all requirements set forth in 957 CMR 5.00. The Data Recipient shall provide copies of all such agreements to CHIA upon request.

The Data Recipient bears sole and exclusive responsibility for ensuring each Third Party's compliance with this Agreement and applicable law and shall be jointly and severally liable with any Third Party for such party's violations of this Agreement. Approval by CHIA of any Third Party individual as an Authorized User does not relieve the Data Recipient of any liability or obligation under this Agreement.

3.5. Access Log

The Data Recipient shall maintain an access log that must contain, at a minimum:

- A list of the names of all Authorized Users, including individuals affiliated with a Third Party, with access to CHIA Data;
- The Project for which each individual was granted access;
- The date access was granted; and
- The date access was terminated, if applicable.

4. Medicaid ("MassHealth") Data

The Data Recipient shall comply with the terms and conditions set forth in the Acknowledgment of Conditions Upon Receipt of MassHealth Data ("MassHealth Acknowledgment"), hereto attached as Exhibit C, if, as part of the Data Application the Data Recipient requested and received MassHealth data. The Data Recipient acknowledges that the terms and conditions applicable to MassHealth data may be changed, modified, or supplemented by the Executive Office of Health and Human Services ("EOHHS") or MassHealth at any time and without prior notice to the Data Recipient. Any new or modified terms imposed by EOHHS or MassHealth shall be automatically incorporated into this Agreement upon notice to the Data Recipient, without the need for a formal amendment. CHIA shall have no liability whatsoever for any such changes or for any consequences arising from the Data Recipient's inability or unwillingness to comply with such changes. If the Data Recipient does not agree to any new or modified terms, or is unable or unwilling to comply with such terms, the Data Recipient must immediately cease all use of MassHealth data and destroy all MassHealth data in its possession in accordance with **Section 12.2** of this Agreement.

5. Confidentiality

The Data Recipient shall:

- maintain, and ensure that all Authorized Users maintain, the confidentiality of CHIA Data and access, use, or disclose CHIA Data solely for the purposes approved in this Agreement;

- not disclose or otherwise make CHIA Data available, either directly or indirectly, to any person or entity other than another Authorized User; and
- comply with any applicable laws and regulations relating to the confidentiality of CHIA Data.

6. Security

6.1. Security Standards

The Data Recipient shall ensure administrative, physical, and technical safeguards exist to protect CHIA Data from unauthorized access, acquisition, disclosure, destruction, alteration, accidental loss, misuse, or damage. Such safeguards shall be no less rigorous than accepted industry practices identified by the National Institute of Standards and Technology (NIST) Special Publication 800-53 rev. 5 or 800-66 rev. 2, or the most recent standards issued by NIST (all such NIST standards and practices collectively, the “**Standards**”), and must comply with this Agreement and all other applicable data protection and privacy laws. The Data Recipient shall ensure that any Third Party that receives, accesses, stores, processes, or otherwise comes into contact with CHIA Data maintains administrative, physical, and technical safeguards no less rigorous than the Standards. The Data Recipient shall, as a condition precedent to any disclosure of CHIA Data to a Third Party, contractually obligate such Third Party to implement, maintain, and demonstrate compliance with such safeguards. Any failure by a Third Party to comply with the Standards or to maintain the required safeguards shall be deemed a breach of this Agreement by the Data Recipient, and the Data Recipient shall be fully liable for all consequences of such failure as if the Data Recipient itself had failed to comply.

6.2. Data Transmission

The Data Recipient acknowledges that the use of unencrypted telecommunications, including but not limited to unencrypted file transfers over the Internet, to transmit CHIA Data is prohibited. CHIA Data may not be moved, transferred, or disclosed from the site identified for storage on the Data Application without prior written authorization from CHIA.

6.3. Notice of Changes

Within forty-eight (48) hours of becoming aware of any changes to its administrative, technical, or operational environments or safeguards that compromise the security of CHIA Data or reduce the Data Recipient’s compliance with the Standards, the Data Recipient shall provide CHIA with written notice of such changes.

6.4. Written Information Security Policy

The Data Recipient shall maintain and implement a written information security program (“WISP”) that complies with the requirements set forth in M.G.L. c. 93H and 201 CMR 17.

6.5. Audits

CHIA, directly or through an independent auditor, may conduct compliance audits and request information regarding Data Recipient's use, storage, and protection of CHIA Data. Data Recipient shall cooperate with any such audit and provide complete and accurate responses within a reasonable time of CHIA's request. If CHIA determines that Data Recipient is not in compliance with this Agreement, CHIA may, in its sole discretion, (a) direct Data Recipient to remediate the non-compliance within a timeframe specified by CHIA, or (b) require Data Recipient to destroy all CHIA Data in accordance with the requirements set forth in **Section 12.2**.

7. Obligations in the Event of a Data Breach

7.1. Duty to Report Data Breaches

No later than forty-eight (48) hours after the Data Recipient knows of or has reason to know of any Data Breach, the Data Recipient shall provide written notice to CHIA advising CHIA of the Breach ("First Breach Notice"). The First Breach Notice shall include:

- date and time of the Data Breach;
- date and time of the discovery of the Data Breach;
- nature and scope of the Data Breach;
- the steps the Data Recipient has taken, and plans to take, to contain and remediate the Data Breach.

7.2. Supplemental Data Breach Notice

If requested by CHIA, the Data Recipient shall, as soon as practicable and without undue delay, provide a supplemental notice ("Supplemental Breach Notice") containing additional details about the Data Breach, including, but not limited to:

- the nature of the Data Breach, including a root cause analysis, containing as much specific detail as possible (e.g., cause, contributing factors, chronology of events);
- The specific data involved in the Data Breach (e.g., the types of identifiers and other information involved), together with samples of any forms or documents that were involved in the Data Breach to illustrate the type of data involved (with personal identifiers removed or redacted);
- the exact number of individuals whose data was involved in the Data Breach if known or, if unknown, a reasonable estimate based on known facts (categorized according to the type of data involved, if different types of data were involved for different individuals), together with an explanation of how the number of individuals was determined;
- a detailed description of the Data Recipient's investigation into the Data Breach;

- the harmful effects of the Data Breach that are known, or should be known, to the Data Recipient;
- a detailed breakdown of all actions the Data Recipient has taken or plans to take to mitigate such harmful effects, and the results of all mitigation actions already taken; and
- a summary of steps taken to prevent such a Data Breach in the future, including copies of revised policies and procedures, changes in business processes and staff training.

7.3. Duty to Investigate and Mitigate

In the event of a Data Breach, the Data Recipient shall, as soon as practicable and without undue delay, take all reasonable and appropriate action necessary to:

- retrieve, to the extent practicable, any CHIA Data involved in the Data Breach;
- mitigate, to the extent practicable, any harmful effect of the Data Breach; and
- take any such other action(s) as may be required in connection with the Data Breach to comply with any applicable laws.

The Data Recipient shall also, as soon as practicable and without undue delay, conduct a thorough investigation into the cause(s) of the Data Breach and, if applicable, its impact on the integrity of the Data Recipient's data systems.

7.4. Coordination with CHIA

The Data Recipient shall also, if requested by CHIA, immediately return CHIA Data to CHIA or destroy CHIA Data and any copies thereof. Upon destroying CHIA Data, the Data Recipient shall timely send written certification of the destruction of CHIA Data to CHIA, attached hereto as **Exhibit B**.

In the event of a Data Breach, the Data Recipient shall fully cooperate with CHIA, including, without limitation:

- assisting with any investigation;
- providing CHIA with physical access to the facilities and operations affected, as reasonable;
- facilitating interviews with the Data Recipient's employees and agents, Authorized Users, and others involved in the Data Breach;
- making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable laws, regulations, industry standards, or as otherwise required by CHIA; and
- if the Data Breach is the result of a security incident or violation of Standards, such as hacking, ransomware, malicious third-party attack, or other related event the Data Recipient shall prepare and provide a written forensics report to CHIA that shall, at a minimum, describe the attack, security vulnerabilities, and any other information CHIA deems necessary. Such information, documents, and deliverables shall not be redacted or withheld by the Data Recipient.

7.5. Corrective Action Plan

The Data Recipient shall, upon request by CHIA, submit a corrective action plan with steps designed to prevent any future Data Breaches. The corrective action plan must be provided within thirty (30) business days of the date of CHIA's request.

7.6. Notice to External Parties

The Data Recipient agrees that it shall not inform any external party of any Data Breach without first obtaining CHIA's written consent, other than to inform the Data Recipient's legal counsel. If CHIA determines, in its sole discretion, that the Data Recipient is required to provide notification to affected individuals or to state or federal agencies, the Data Recipient shall, at Data Recipient's sole cost, assist CHIA in drafting such notices for CHIA's review and approval, and shall take such other action(s) as CHIA may reasonably request. In no event shall the Data Recipient have the authority to provide any such notification on CHIA's behalf, unless CHIA authorizes and directs the Data Recipient to do so in writing.

7.7. Reimbursement and Indemnification

The Data Recipient shall reimburse CHIA for all costs incurred or sustained by CHIA in responding to, investigating, and mitigating any Data Breach, including but not limited to costs of notification, credit monitoring, forensic investigation, legal fees, and regulatory response. Indemnification for Data Breaches and all other claims arising under this Agreement is subject to and governed by the Comprehensive Indemnification Section, Section 14.6 Comprehensive Indemnification of this Agreement.

8. Response to Legal Process

8.1. Notice of Legal Demands for CHIA Data

The Data Recipient shall notify CHIA in writing within forty-eight (48) hours of receiving any subpoena, court order, administrative order, or other legal process seeking CHIA Data, or any public records or freedom of information request under applicable state or federal law. Data Recipient shall provide CHIA with a copy of the demand or request promptly upon receipt.

8.2. Response to Legal Demands

The Data Recipient shall not disclose CHIA Data in response to any legal demand or public records request without prior written authorization from CHIA. Upon receiving any such demand or request, Data Recipient shall follow CHIA's instructions, which may include objecting to or seeking to quash the demand. If CHIA elects to respond directly, Data Recipient shall cooperate and provide reasonable assistance. All responses shall comply with M.G.L. c. 12C, M.G.L. c 66A § 2(k), 801 CMR 3.00, 42 CFR Part 2, and any other applicable law.

9. Ownership of CHIA Data

CHIA owns or otherwise holds all rights in CHIA Data provided to the Data Recipient under this Agreement. Data Recipient's right to access and use CHIA Data is limited to the purposes and scope expressly authorized in this Agreement. The Data Recipient acquires no ownership interest in CHIA Data or in any data derived from CHIA Data, and all such derived data shall be subject to the same terms and restrictions as CHIA Data.

10. Disclaimer of Warranties

CHIA Data is provided "as is". CHIA HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. CHIA SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR PRACTICE. CHIA makes no warranty of any kind that CHIA Data will be secure, accurate, complete, free of harmful code, or error free.

11. Disclosures and Publications

11.1. Restrictions on Publication

The Data Recipient shall not disclose to any person other than an Authorized User any findings, listings, or information derived from CHIA Data, with or without direct identifiers, if such information could, by itself or in combination with other data, be used to identify an individual.

11.2. Deidentification and Cell Suppression

Any document created using CHIA Data that is shared with any person other than an Authorized User shall:

- (a) be deidentified pursuant to the deidentification standards set forth in Section 164.514(a) of the HIPAA Privacy Rule, and
- (b) adhere to the most recent version of the CMS Cell Size Suppression Policy ("CMS Policy"). CMS Policy stipulates that no cell (e.g. admissions, discharges, patients, services, etc.) containing a value of 1 to 10 can be reported directly. A value of zero does not violate the minimum cell size policy. In addition, no cell can be reported that allows a value of 1 to 10 to be derived from other reported cells or information. For example, the use of percentages or other mathematical formulas that, in combination with other reported information, result in the display of a cell containing a value of 1 to 10 are prohibited. CMS Policy applies to the reporting of excluded cases. In the event the CMS Policy is updated, the Data Recipient should refer to the version referenced in this Agreement. See <https://www.hhs.gov/guidance/document/cms-cell-suppression-policy>.

11.3. Notice to CHIA Regarding Publications and Research Findings

At least ten (10) business days before releasing or disclosing any analysis, research, or other material based on CHIA Data to any person other than an Authorized User, Data Recipient shall submit a copy to CHIA for review.

If CHIA objects on the grounds that the material violates applicable law or this Agreement, Data Recipient shall not release or disclose the material until CHIA confirms in writing that its concerns have been addressed. If CHIA does not respond within the ten (10) business day review period, the Data Recipient may proceed with release or disclosure.

CHIA's review, approval, or failure to object does not constitute endorsement of, or assumption of responsibility for, the accuracy, completeness, or conclusions of any materials, and does not relieve the Data Recipient of any obligations under this Agreement or applicable law.

12. Data Destruction

12.1. Data Destruction Upon Project Completion or Termination

Except as set forth herein, CHIA Data may be retained by the Data Recipient only for the duration of the Project. Within thirty (30) days of Project completion, Data Recipient shall notify CHIA of the Project completion, destroy all CHIA Data in its possession, and provide written certification of destruction.

If this Agreement is terminated prior to Project completion, Data Recipient must destroy all CHIA Data in its possession and provide written certification of destruction within fifteen (15) days of the termination.

12.2. Data Destruction Standards

The Data Recipient shall destroy CHIA Data in accordance with standards set forth in NIST Special Publication 800-88, Guidelines for Media Sanitization, M.G.L. c. 93I, applicable laws relating to the destruction of confidential information, applicable state and federal record retention laws and regulations, and state data security policies including policies issued by CHIA. Written certification of destruction must be provided using the form attached hereto as **Exhibit B**.

13. Term and Termination of Agreement

13.1. Termination for Convenience

This Agreement is effective on the Effective Date and continues until Project completion or termination in accordance with this Section 13, whichever occurs first. The Agreement may be terminated by either Party at any time for any reason upon thirty (30) days written notice to the other Party. Upon notice of termination by the Data Recipient, CHIA shall not release any further CHIA Data to the Data Recipient, and the Data Recipient shall destroy all CHIA Data within fifteen (15) days pursuant to **Sections 12.1 and 12.2.**

13.2. Termination for Cause

CHIA may terminate this Agreement immediately upon written notice to the Data Recipient, without any opportunity to cure, upon (a) any Data Breach or security incident involving CHIA Data, or (b) CHIA's determination, in its sole discretion, that continued provision of CHIA Data poses any risk to individual privacy, CHIA Data Security, or CHIA's statutory mission. For any other breach of this Agreement by the Data Recipient, any Third Party, or any Authorized User, that does not pose a risk to individual privacy, CHIA Data security, or CHIA's statutory mission, CHIA may, in its sole discretion, provide the Data Recipient ten (10) business days to cure the breach. The Data Recipient has no right to terminate this Agreement for cause. Upon any termination for cause, the Data Recipient must immediately cease all use of CHIA Data and destroy all CHIA Data in its possession within five (5) business days in a manner consistent with **Section 12.2.** Termination for cause does not limit any other rights or remedies available to CHIA and does not relieve the Data Recipient of any liability arising from the conduct that gave rise to the termination.

14. Other Terms and Conditions

14.1. Amendments and Submissions of Certificates of Continued Need

The terms of this Agreement can only be amended in writing. A Data Recipient that was approved to receive prospective years of CHIA Data shall submit a completed Certificate of Continued Need and Compliance, a form of which will be provided by CHIA, prior to the receipt of such years or release versions of CHIA Data.

14.2. Violations and Penalties

A violation of this Agreement may result in penalties, remedies, and damages available under law or this Agreement, including those provided under M.G.L. c 12C, 957 CMR 5.00 et seq., M.G.L. c. 214 § 1B and M.G.L. c. 93A. All remedies are cumulative and not exclusive. CHIA may notify state and federal law enforcement officials of any Data Breach or violation of this Agreement as CHIA determines appropriate. It is the sole responsibility of the Data Recipient to ensure compliance with applicable local, state, and federal laws and regulations.

14.3. Survival

Any provision of this Agreement that by its nature or context is intended to survive termination or expiration, including without limitation any provision relating to confidentiality, security, data protection, data destruction, indemnification, liability, or the protection of CHIA Data, shall survive termination or expiration of this Agreement and shall remain in full force and effect indefinitely or until fully performed.

14.4. Data Recipient Responsibility and Compliance

The Data Recipient is solely and exclusively responsible for compliance with applicable law and all terms, conditions, and obligations under this Agreement. The Data Recipient is solely responsible for all acts and omissions of its Authorized Users and Third Parties with access to CHIA Data through the Data Recipient, whether such persons or entities are acting within or outside the scope of their authority. Pursuant to 957 CMR 5.03(3), upon receipt of CHIA Data, the Data Recipient shall be responsible for any breach of privacy or security, unauthorized access, acquisition, disclosure, misuse, or other violation arising from the Data Recipient's possession, use, or control of CHIA Data.

The Data Recipient acknowledges that CHIA is providing access to sensitive health care data in reliance on the Data Recipient's representations and warranties, and that any breach of such representations or warranties could cause irreparable harm to CHIA and to the individuals whose information is contained in CHIA Data. The Data Recipient's obligations under this Agreement are non-delegable and cannot be transferred, assigned, or subcontracted without CHIA's prior written consent. Any delegation to other parties shall not relieve the Data Recipient of any obligation or liability under this Agreement.

14.5. Materiality of All Terms

All terms, conditions, obligations, restrictions, and requirements in this Agreement are material and essential to CHIA's willingness to provide CHIA Data to the Data Recipient. Any breach of any provision of this Agreement, regardless of the nature or scope of such breach, shall constitute a material breach of this Agreement. CHIA shall not be required to demonstrate materiality of any breach to exercise its rights or remedies under this Agreement. No provision of this Agreement shall be deemed less material by reason of the absence of specific language designating it as material, and no breach shall be deemed non-material by reason of its characterization as technical, inadvertent, or minor in nature.

14.6. Comprehensive Indemnification

The Data Recipient shall indemnify, defend, and hold harmless CHIA, the Commonwealth of Massachusetts, and their respective officers, employees, agents, representatives, successors, and assigns from and against any and all claims, demands, actions, suits, proceedings, investigations, losses, damages, liabilities, judgments, awards, settlements, fines, penalties, sanctions, costs, and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, and remediation) arising from or related to:

- (a) any breach or alleged breach of this Agreement by Data Recipient, a Third Party, or an Authorized User;
- (b) any violation or alleged violation of applicable law by Data Recipient, a Third Party, or an Authorized User in connection with CHIA Data;
- (c) any unauthorized access to, or disclosure of, CHIA Data in the possession or control of Data Recipient, a Third Party, or an Authorized User;
- (d) any claim by any individual whose information is contained in CHIA Data, data subjects, patients, providers, payers, or regulatory authorities arising from Data Recipient's activities under this Agreement;
- (e) any negligent or wrongful act or omission of Data Recipient, a Third Party, or an Authorized User related to CHIA Data.

This indemnification obligation applies regardless of whether CHIA reviewed or approved the activity giving rise to the claim. Data Recipient shall not settle any claim without CHIA's prior written consent. This obligation survives termination or expiration of this Agreement.

14.7. Disclaimer of CHIA Liability

Nothing in this Agreement creates any partnership, joint venture, agency, or fiduciary relationship between CHIA and Data Recipient. CHIA has no obligation to ensure the success of Data Recipient's project or to provide technical assistance beyond what is expressly stated in this Agreement.

CHIA shall not be liable to the Data Recipient or any other party for any claims, damages, losses, costs, or expenses arising from Data Recipient's access to, use of, or reliance on CHIA Data, or any analyses, publications, or other products derived therefrom. CHIA's approval of the Data Application, execution of this Agreement, approval of any Authorized Users or Third Parties, or review of any analyses or publications does not constitute assumption of any liability or responsibility for Data Recipient's activities. In no event shall CHIA be liable for any indirect, incidental, consequential, special, punitive, or exemplary damages, regardless of the theory of liability. CHIA's total liability under this Agreement shall not exceed the fees actually paid by the Data Recipient to CHIA under this Agreement.

14.8. Cumulative Remedies and Enforcement, Attorney's Fees

All rights and remedies available to CHIA under this Agreement are cumulative and in addition to any other rights and remedies available to CHIA at law or in equity. Any waiver by CHIA of any provision of this Agreement must be in writing and signed by an authorized representative of CHIA. No waiver of any provision or breach constitutes a waiver of any other provision or any subsequent breach of the same or any other provision. Data Recipient acknowledges that any breach of this Agreement may cause irreparable harm to CHIA and to the individuals whose information is contained in CHIA Data, for which monetary damages would be an inadequate remedy, and therefore CHIA shall be entitled to seek injunctive relief, specific performance, and other equitable remedies without the necessity of posting bond or proving actual damages. If CHIA prevails in any action to enforce the terms of this Agreement or to collect any amounts due hereunder, the Data Recipient shall pay all of CHIA's reasonable costs and expenses incurred in connection with such action, including but not limited to reasonable attorneys' fees, court costs, expert witness fees, and other litigation expenses, whether incurred at the trial or appellate level, in bankruptcy proceedings, or in any other proceedings

14.9. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Massachusetts, without regard to its conflict of laws principles. Any action arising out of or relating to this Agreement shall be brought exclusively in the state or federal courts located in Suffolk County, Massachusetts, and each party consents to the jurisdiction of such courts.

14.10. Severability

If any provision of this Agreement is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such provision shall be deemed modified to the minimum extent necessary to make it enforceable while preserving the original intent and scope of protection for CHIA and for individuals whose information is contained in CHIA Data. In no event shall any such provision be simply struck or rendered void if it can be reformed to be enforceable. The remaining provisions of this Agreement shall remain in full force and effect and shall be construed to give maximum effect to the intent of the parties to protect the confidentiality, security, and proper use of CHIA Data. Notwithstanding any finding of invalidity or unenforceability of any provision, the Data Recipient's obligations relating to confidentiality, security safeguards, data destruction, indemnification, and protection of individual privacy shall survive and remain fully enforceable. Any court interpreting this Agreement shall construe its provisions broadly to achieve the protective purposes for which it was intended, particularly with respect to safeguarding sensitive health information and ensuring compliance with applicable privacy and security laws.

14.11. Entire Agreement

This Agreement, together with all exhibits attached hereto including the approved Data Application referenced herein, constitutes the complete and exclusive agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous negotiations, proposals, representations, agreements, and understandings, whether oral or written, relating to such subject matter. Notwithstanding the foregoing, nothing in this Agreement shall limit, supersede, or modify CHIA's statutory authority, rights, powers, duties, or obligations under M.G.L. c. 12C, 957 CMR 5.00, or any other applicable law, all of which are hereby preserved in their entirety. This Agreement may not be amended, modified, or supplemented except by a written instrument signed by an authorized representative of CHIA. No course of dealing, course of performance, usage of trade, or other conduct by the parties shall be deemed to modify, amend, or supplement any provision of this Agreement. CHIA's failure to enforce any provision of this Agreement shall not constitute a waiver, modification, or amendment of such provision, and CHIA expressly reserves the right to enforce any and all provisions at its sole discretion. Data Recipient acknowledges that it has not relied upon any representation, statement, promise, inducement, or agreement not expressly set forth in this Agreement, and Data Recipient waives any claim based on any such extraneous representation or statement

14.12. Notices

All notices, requests, demands, and other communications required or permitted under this Agreement shall be in writing and shall be deemed given: (i) when delivered by hand with receipt acknowledged; (ii) on the date sent by email if sent during normal business hours (9:00 AM to 5:00 PM, Eastern Time on a business day), or on the next business day if sent after normal business hours; or (iii) on the third business day after deposit in the United States mail, first class postage prepaid, certified mail, return receipt requested. Notices sent by mail or hand delivery must also be sent by email to the designated CHIA email address listed below.

All notices shall be addressed as follows:

If to CHIA:
Donald Kirkwood
Senior Privacy Officer
Center for Health Information and Analysis
501 Boylston Street, Suite 5100
Boston, MA 02116
Donald.Kirkwood@chiamass.gov

If to Data Recipient:
First and Last Name. _____
Title _____
Address _____
Email Address _____

Each Party shall notify the other in writing of any change to its designated contact person, address, or email for notices under this Agreement as soon as practical, but not less than ten (10) business days prior to any change taking effect. Until such notice is received, notices sent to the previously designated address shall be deemed effective.

Signatures

IN WITNESS WHEREOF, the parties by their duly authorized representatives have executed this Agreement as of the Effective Date.

CENTER FOR HEALTH INFORMATION AND ANALYSIS

Name of CHIA Representative:	Title:
Street Address: 501 Boylston Street, Suite 5100, Boston, MA 02116	
Office Telephone (<i>Include Area Code</i>):	E-Mail Address:
Signature:	Date:

AUTHORIZED SIGNATORY FOR DATA RECIPIENT

Name of Authorized Signatory:	Title:
Street Address:	
Office Telephone (<i>Include Area Code</i>):	E-Mail Address:
Signature:	Date:

Exhibit A
Approved Data Application

EXHIBIT B
CERTIFICATION OF PROJECT COMPLETION & DATA DESTRUCTION

CHIA Data must be destroyed pursuant to NIST Special Publication 800-88, Guidelines for Media Sanitization, M.G.L. c. 93I, and all other Applicable Law. All data destruction must comply with the requirements of M.G.L. c. 93I.

The undersigned hereby certifies that **all CHIA Data provided for the Project entitled:** _____ **has been destroyed** as of _____ in accordance with the terms of the Data Use Agreement.

Name of Custodian:	Data Recipient:	
Street Address:		
Office Telephone (<i>Include Area Code</i>):	E-Mail Address:	
Signature:	Title:	Date:

EXHIBIT C
ACKNOWLEDGMENT OF CONDITIONS UPON RECEIPT OF MASSHEALTH DATA

This Acknowledgment supplements the Data Use Agreement (“DUA”) dated _____, between the Center for Health Information and Analysis (“CHIA”) and _____, hereinafter referred to as “Recipient”.

This Acknowledgment pertains to the project entitled: _____ as described in the Recipient’s Data Application for data from the Massachusetts All Payer Claims Database (“APCD”).

This Acknowledgment is effective as of the date of execution below. To the extent that this Acknowledgment is inconsistent with any terms in the DUA, this Acknowledgment modifies and overrides the DUA, which shall otherwise remain in full force and effect.

The undersigned Recipient hereby acknowledges that:

- Pursuant to an interagency service agreement between CHIA and MassHealth, CHIA submitted the Recipient’s request for Medicaid data from the APCD to MassHealth for review to determine whether the request is “directly connected” to the administration of the MassHealth program;
- Federal regulation at 42 CFR 431.302 provides purposes directly related to plan administration which include (1) Establishing eligibility; (2) Determining the amount of medical assistance; (3) Providing services for beneficiaries; and (4) Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan.
- For all Recipients, EHS approves the request contingent upon the following requirements:
 - that the Recipient shall provide an advance draft of any publication to the MassHealth Chief of Staff (Celia.S.Segel@mass.gov), and if the Recipient accessed identifiable data an additional draft must be provided to the EHS Privacy Office (privacy.officer@mass.gov), five (5) business days prior to publication; and
 - that the Recipient shall provide EHS with the results of its analysis of the MassHealth data.
 - The undersigned Recipient hereby agrees to comply with the above requirement(s), as a condition of receiving MassHealth data from CHIA.

The Recipient acknowledges that the above condition(s) are hereby incorporated into the Recipient’s DUA with CHIA as obligations of the Recipient and that, as such, failure to comply with any of the listed conditions could result in denial of future access to any CHIA Data, termination of current access to CHIA Data, and/or a demand for immediate return or destruction of all CHIA data.

On behalf of the Recipient the undersigned individual hereby attests that he or she is authorized to legally bind the Recipient to the terms of this Acknowledgment and agrees to all the terms specified herein.

Authorized Signatory:		
Street Address:		
Office Telephone (<i>Include Area Code</i>):		E-Mail Address:
Signature:	Title:	Date: