Participant Agreement

This Participant Agreement ("Agreement"), effective as of the date of last signature, is entered into by and between The University of Texas at Austin ("University") and Williamson County, acting herein for Williamson County Emergency Medical Services ("Participant") (each a "Party" and collectively the "Parties").

I. Background:

A. Williamson County has agreed to participate in the implementation of the Texas Connecting Overdose Prevention Efforts platform (TxCOPE), an initiative conducted under the University (hereafter referenced as "Program").

B. The Program provides a platform designed to detect and predict overdose incidents from data collected from organizations involved with substance abuse, including Emergency Services, Health Care Providers, Substance Abuse Treatment Providers, Public Health Surveillance Organizations, Non-governmental Organizations, and State Agencies.

C. The Program will aggregate data sources from a number of Participant Organizations (Participants) to inform Program data dashboards and visualizations to support data-driven community response efforts to the opioid crisis.

D. Data derived from the Program will be used, in part, to help advocate for increased resource allocation to Participants to mitigate overdose incidents and continue monitoring overdose activity in the Participant's locale.

E. The Program is a research effort organized and operated under the University's Dell Medical School and Steve Hicks School of Social Work.

F. The University is a public research university organized under the laws and Constitution of the State of Texas.

G. The University will receive certain confidential data from Participant that may be classified as Protected Health Information (PHI) that is protected under the Health Insurance Portability and Accountability Act (HIPAA) and the HIPAA Regulations, Health Information Technology for Economic and Clinical Health Act (HITECH Act) and/or state law(s), including the Medical Records Privacy Act (MRPA), and will manage such information only in accordance with HIPAA and the HIPAA Regulations, HITECH Act, and MRPA. The Parties agree that this data is being transmitted in support of the Program only as described herein, and the data use is limited for these purposes only.

H. The Parties will mutually agree upon what data will be provided for the Program.

I. A Business Associate Agreement ("BAA") or Data Use Agreement, as appropriate, may be executed between the parties in support of the data transfer for the Project.

II. Scope of Program

A. The purpose of the Program is to deploy the TxCOPE platform among relevant organizations serving people at risk of, or experiencing, an opioid overdose across the State of Texas.

B. The Program is also meant to support Public Health and Public Health Surveillance efforts and activities across the State of Texas.

C. The TxCOPE platform will be scaled throughout the State of Texas in an effort to improve overdose surveillance and real-time, data-driven prevention efforts across the State of Texas.

D. The TxCOPE platform is designed to import and export data.

E. Participants may enter data: 1) directly into the TxCOPE dashboard; 2) use an Application Programming Interface (API) for data exportation into TxCOPE, or 3) submit batch data to the TxCOPE platform.

F. Data ingested into the TxCOPE platform is used to populate heat maps and data dashboards that are accessible only to Participants and state and federal agencies supporting public health response.

G. Participants will have access to organizational-level and county-level data.

H. De-identified state-level data will be disseminated via quarterly reports to non-participating organizations, governmental organizations, the media, and others.

III. Participant Organization On-boarding and Responsibilities

A. In order to accommodate for the diversity of data collection environments and operations that characterize Participants, Program will develop with each Participant a mutually acceptable onboarding process relative to: 1) the reporting of overdose incidents in the TxCOPE platform at consistent intervals; 2) the reporting of overdose interventions

(known commonly as reversals) in the TxCOPE platform; and 3) the reporting of Narcan distribution in the TxCOPE platform.

B. Participant agrees to provide public health information related to overdose incidents regularly in accordance with the purposes and scope of the Program to support the updating and maintenance of public health data dashboards. The Program will maintain one data dashboard that will be dedicated for the use of the Participant and one dashboard will be dedicated to show county-level aggregated trends.

C. Participant will establish and maintain an active Participant Agreement with the Program for the duration of their use of the Platform.

D. Best practices identified during the collective on-boarding process of Participants will be compiled in a "TxCOPE Users Implementation Guide" ("Guide") which will be developed by University and made available to current and prospective Participants to help facilitate additional on-boardings and on-going operation of the Platform. No organizationally-identifiable information will be included in this Guide. Participants are encouraged to provide recommended best practices to University for possible inclusion in this Guide.

E. Once mutually acceptable terms are determined for Section III (A), Participant agrees to upload data to the TxCOPE platform in a method and data format mutually agreed upon by the Parties.

IV. Ownership and Work Product

A. Participant owns all data and other identifiable information ("Participant Data") it submits to University. Participant hereby grants to University a worldwide, fully paid-up, royalty-free license to copy, format, distribute and publicly present the Participant Data in whatever form or medium University may require to support the Program.

B. University owns all aggregate and non-identifiable information it has developed associated with the Program.

V. Term and Termination

A. Term. The term of this Agreement shall commence as of the date of last signature and shall continue for the duration of the Program, unless terminated earlier in accordance with the provisions of this section.

B. Termination by University. University may terminate this Agreement at any time upon thirty (30) days notice by notifying Participant in writing.

C. Termination by Participant. Participant may terminate this Agreement at any time upon thirty (30) days notice by notifying University in writing.

VI. Miscellaneous.

A. Change in Law. The Parties agree to negotiate in good faith to amend this Agreement to comport with changes in federal law that materially alter either or both parties' obligations under this Agreement. Provided however, that if the Parties are unable to agree to mutually acceptable amendment(s) by the compliance date of the change in applicable law or regulations, either Party may terminate this Agreement as provided in section V.

B. Construction of Terms. The terms of this Agreement shall be construed to give effect to applicable federal interpretative guidance regarding HIPAA and HIPAA Regulations.

C. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

D. Headings. The headings and other captions in this Agreement are for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this Agreement.

E. Other Provisions. No amendment to the Agreement will be effective unless in writing and signed by the Parties. Neither the Agreement nor the rights and obligations of the Parties hereunder may be sold, assigned or otherwise transferred. If any provision of the Agreement is held to be unenforceable, all other provisions will continue in full force and effect. The Agreement supersedes any and all prior understandings or previous agreements between the Parties, oral or written, relating to the subject matter herein and constitutes the sole and complete agreement between the Parties related to the subject matter herein. Any delay by a Party to enforce any right under the Agreement shall not act as a waiver of that right, nor as a waiver of the Party's ability to later assert that right relative to any particular factual situation. The Agreement will be construed and enforced in accordance with laws of the U.S. and the State of Texas, without regard to choice of law and conflicts of law principles. The parties hereby agree that any dispute that cannot be resolved under this Agreement will be venued in a court of competent jurisdiction located in Travis County, Texas. The Parties acknowledge that nothing in the Agreement shall constitute a waiver of sovereign immunity by Parties that are state or local government agencies.

F. Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below and via email to the address(es) listed below. Each Party named below may change its address and that of its representative for notice by the giving of notice thereof in the manner herein provided. If

notice is provided in writing to an addressee below, a courtesy copy of such notice shall also be provided via email.

If to Participant:
Williamson County
Attn: County Judge
710 South Main Street, Suite 101
Georgetown, Texas 78626

Courtesy Copy Sent to:
Williamson County Emergency Medical Services
Attn: EMS Director
3189 South-East Inner Loop
Georgetown, Texas 78627

If to The University of Texas at Austin:
The University of Texas at Austin
Office of Research
Dell Medical School
1601 Trinity Street, Building B
Austin, TX 78703
kasey.claborn@austin.utexas.edu &
dellmedresearchcontracts@austin.utexas.edu

Williamson County	**The University of Texas at Austin**
By: _____	**By:** DocuSigned by: Mohini Patel CA21577FB04F443...
(Authorized Signature)	**(Authorized Signature)**
Name: _____	**Name:** Mohini Patel
(Type or Print)	**(Type or Print)**
Title: _____	**Title:** Sr. Manager
Date: _____	**Date:** 2023-05-05 | 11:30:14 CDT

Business Associate Agreement

This Business Associate Agreement ("Agreement"), effective date of last signature("Effective Date"), is entered into by and between The University of Texas at Austin ("Business Associate") and Williamson County, a body corporate and politic under the laws of the State of Texas("Covered Entity", as more fully defined in section 1(c)) (each a "Party" and collectively the "Parties").

RECITALS

WHEREAS, Covered Entity has entered or is entering into that certain Participant Agreement with Business Associate ("the Underlying Agreement") by which it has engaged Business Associate to perform services;

WHEREAS, Covered Entity possesses Protected Health Information that is protected under HIPAA and the HIPAA Regulations, HITECH Act and state law, including the Medical Records Privacy Act (MRPA), and is permitted to manage such information only in accordance with HIPAA and the HIPAA Regulations, HITECH Act, and MRPA;

WHEREAS, Business Associate may receive such information from Covered Entity, or create, receive, maintain or transmit such information on behalf of Covered Entity, in order to perform certain of the services under the Underlying Agreement;

WHEREAS, the Parties desire to comply with health information privacy and security protections subsequent to the enactment of the HITECH Act, Subtitle D of the American Recovery and Reinvestment Act of 2009 which has established requirements for compliance with HIPAA. In particular, the requirements provide that: (1) Covered Entity give affected individuals notice of security breaches affecting their PHI, and Business Associate give notice to Covered Entity pursuant to the provisions below; (2) Business Associate comply with the HIPAA security regulations; and (3) additional and/or revised provisions be included in Business Associate Agreement;

WHEREAS, Under HIPAA and HITECH, Covered Entity is required to enter into protective agreements, generally known as "business associate agreements," with certain downstream entities that will be entrusted with HIPAA-protected health information;

WHEREAS, Health information is further protected by state law, including the MRPA; and

WHEREAS, Covered Entity wishes to ensure that Business Associate will appropriately safeguard Protected Health Information.

NOW THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions. The Parties agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in HIPAA and the HIPAA Regulations and the MRPA. All

capitalized terms used in this Agreement but not defined below shall have the meaning assigned to them under the HIPAA Regulations.

a. "Breach" shall have the meaning given such term under 45 C.F.R. § 164.402 as such regulation is revised from time to time.

b. "Breach of System Security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Sensitive Personal Information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

c. "Business Associate" means, with respect to a Covered Entity, a person who:

1) on behalf of such Covered Entity or of an Organized Health Care Arrangement (as defined under the HIPAA Regulations) in which the Covered Entity participates, but other than in the capacity of a member of the workplace of such Covered Entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, HIPAA Regulations, or MRPA including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. 3.20, billing, benefit management, practice management, and re-pricing; or

2) provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an Organized Health Care Arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of PHI from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

d. "Data Aggregation" means, with respect to PHI created or received by Business Associate in its capacity as the Business Associate of Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

e. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

f. "HIPAA Regulations" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164 subparts A and E ("The Privacy Rule") and the Security Standards as they may be amended from time to time, 45 C.F.R. Parts 160, 162 and 164, Subpart C ("The Security Rule").

g. "HITECH Act" means the provisions of Division A, Title XIII of the American Recovery and Reinvestment Act of 2009, known as The Health Information Technology for Economic and Clinical Health, Act 42 U.S.C. §3000 et. seq., and implementing regulations and guidance, including the regulations implemented in 78 Fed. Reg. 5566 (January 25, 2013).

h. "Individually Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and:

1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2) relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

a) that identifies the individual; or

b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

i. "MRPA" means Texas Medical Records Privacy Act, as codified in Section 181 et seq. of the Texas Health and Safety Code and as implemented through regulations including the Standards Relating to the Electronic Exchange of Health Information, codified at Title 1, Section 390.1 et seq. of the Texas Administrative Code.

j. "Protected Health Information" or "PHI" means Individually Identifiable Health Information that is transmitted by electronic media; maintained in any medium described in the definition of the term electronic media in the HIPAA Regulations; or transmitted or maintained in any other form or medium. The term excludes Individually Identifiable Health Information in educational records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g; records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and employment records held by a Covered Entity in its role as employer and regarding a person who has been deceased more than 50 years.

k. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system, but does not include minor incidents that occur on a routine basis, such as scans, "pings", or unsuccessful random attempts to penetrate computer networks or servers maintained by Business Associate.

l. "Sensitive Personal Information" means: (1) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (a) social security number; (b) driver's

license number or government-issued identification number; (c) account number or credit or debit card number in combination with any required security code, access, code, or password that would permit access to an individual's financial account; or (2) PHI information that identifies an individual and relates to: (a) the physical or mental health or condition of the individual; (b) the provision of health care to the individual; or (c) payment for the provision of health care to the individual.

m. "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified in the guidance issued under Section 13402(h)(2) of the HITECH Act on the HHS web site.

2. Permitted Uses and Disclosures.

a. Compliance with Law. Covered Entity and Business Associate agree to comply with HIPAA, HIPAA Regulations, the HITECH Act, and the MRPA.

b. Performance of Services. Except as otherwise permitted by this Agreement, Business Associate may create, receive, maintain or transmit PHI on behalf of Covered Entity only in connection with the performance of the services contracted for in the Underlying Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103).

c. Proper Management and Administration. Business Associate may use PHI it receives in its capacity as Covered Entity's Business Associate for the proper management and administration of Business Associate in connection with the performance of services in the Underlying Agreement, as permitted by this Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103), and to carry out the legal responsibilities of Business Associate. Business Associate may also disclose Covered Entity's PHI for such proper management and administration of Business Associate and to carry out the legal responsibilities of Business Associate. Any such disclosure of PHI shall only be made in accordance with the terms of this Agreement, including Section 5(c) if to an agent or subcontractor of Business Associate, and only if Business Associate obtains reasonable written assurances from the person to whom the PHI is disclosed that: (1) the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and (2) Business Associate will be notified by such person of any instances of which it becomes aware in which the confidentiality of the PHI has been breached.

d. Data Aggregation. Business Associate may use and disclose PHI received by Business Associate in its capacity as Covered Entity's business associate in order to provide Data Aggregation services relating to Covered Entity's health care operations only with Covered Entity's permission.

e. Business Associate may use and disclose de-identified health information if written approval from the Covered Entity is obtained, and the PHI is de-identified in compliance with the HIPAA Rules.

3. Nondisclosure.

a. As Provided in Agreement. Business Associate shall not use or further disclose Covered Entity's PHI other than as permitted or required by this Agreement or as Required by Law (as that term is defined by 45 C.F.R. § 164.103).

b. Disclosures Required By Law. Business Associate shall not, without prior written consent of Covered Entity, disclose any PHI on the possibility that such disclosure is required by law without notifying, to the extent legally permitted, Covered Entity so that the Covered Entity shall have an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such a disclosure, Business Associate, shall, to the extent permissible by law, refrain from disclosing the PHI until Covered Entity has exhausted all alternatives for relief. Business Associate shall require reasonable assurances from persons receiving PHI in accordance with Section 2(c) that such persons will provide Covered Entity with similar notice and opportunity to object before disclosing PHI when a disclosure is required by law.

c. Additional Restrictions. If Covered Entity notifies Business Associate that Covered Entity has agreed to be bound by additional restrictions on the uses or disclosures of Covered Entity's PHI pursuant to HIPAA or the HIPAA Regulations, Business Associate shall be bound by such additional restrictions and shall not disclose Covered Entity's PHI in violation of such additional restrictions to the extent possible consistent with Business Associate's obligations set forth in the Underlying Agreement.

d. Restrictions Pursuant to Subject's Request. If Business Associate has knowledge that an individual who is the subject of PHI in the custody and control of Business Associate has requested restrictions on the disclosure of PHI, Business Associate must comply with the requested restriction if (a) the Covered Entity agrees to abide by the restriction; or (b) the disclosure is to a health plan for purposes of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which Covered Entity has been paid out of pocket in full. <u>If the use or disclosure of PHI in this Agreement is based upon an Individual's specific authorization for the use or disclosure of his or her PHI, and the Individual revokes such authorization, the effective date of such authorization has expired, or such authorization is found to be defective in any manner that renders it invalid, Business Associate shall, if it has notice of such revocation, expiration, or invalidity, cease the use and disclosure of the Individual's PHI except to the extent it has relied on such use or disclosure, or if an exception under the Privacy Rule expressly applies.</u>

e. Remuneration. Business Associate shall not directly or indirectly receive remuneration in exchange for disclosing PHI received from or on behalf of Covered Entity except as permitted by HITECH Act § 13405, the MRPA, and any implementing regulations that may be promulgated or revised from time to time.

f. Disclosure. Business Associate shall not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. part 164, or MRPA, if done by the Covered Entity itself except as authorized under Section 2 of this Agreement.

4. Minimum Necessary. Business Associate shall limit its uses and disclosures of, and requests for, PHI, to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

5. Additional Business Associate Obligations.

a. Safeguards. Business Associate shall use appropriate safeguards and comply with Subpart C of 45 C.F.R. 164 with respect to electronic PHI to prevent use or disclosure of the PHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any paper or electronic PHI it creates, receives, maintains, or transmits on behalf of Covered Entity.

b. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of the obligations.

c. Business Associate's Agents and Subcontractors.

1) Business Associate shall ensure that any agents and subcontractors to whom it provides PHI agree to only create, receive, maintain or transmit PHI on behalf of the Business Associate under the same restrictions that apply to Business Associate. Such agreement between Business Associate and subcontractor or agent must be in writing and must comply with the terms of this Agreement and the requirements outlined at 45 C.F.R. §164.504(e)(2); 45 C.F.R. §164.502(e)(1)(ii); 45 C.F.R. §164.314; and 45 C.F.R. §164.308(b)(2). Additionally, Business Associate shall ensure agent or subcontractor agree to and implement reasonable and appropriate safeguards to protect PHI.

2) If Business Associate knows of a pattern of activity or practice of its subcontractor or agent that constitutes a material breach or violation of the agent or subcontractor's obligation under the contract or other arrangement, the Business Associate must take steps to cure the breach and end the violation and if such steps are not successful, must terminate the contract or arrangement if feasible. If it is not feasible to terminate the contract, Business Associate must promptly notify the Covered Entity.

d. Reporting. Business Associate shall, as soon as practicable but not more than five (5) business days after becoming aware of any successful security incident or use or disclosure of Covered Entity's PHI or Sensitive Personal Information in violation of this Agreement, report any such use or disclosure to Covered Entity. With the exception of law enforcement delays that satisfy the requirements under 45 C.F.R. § 164.412 or as otherwise required by applicable state law, Business

Associate shall notify Covered Entity in writing without unreasonable delay and in no case later than ten (10) calendar days upon discovery of a Breach of Unsecured PHI or Breach of Security System. Such notice must include, to the extent possible, the name of each individual whose Unsecured PHI or Sensitive Personal Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such breach. Business Associate shall also provide, to the extent possible, Covered Entity with any other available information that Covered Entity is required to include in its notification to individuals under 45 C.F.R. § 164.404(c) and Section 521.053, Texas Business & Commerce Code at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. For purposes of this Agreement, a Breach of Unsecured PHI or Breach of Security System shall be treated as discovered by Business Associate as of the first day on which such breach is known to Business Associate (including any person, other than the individual committing the breach, who is an employee, officer, or other agent of Business Associate, as determined in accordance with the federal common law of agency) or should reasonably have been known to Business Associate following the exercise of reasonable diligence.

e. Mitigation. Business Associate shall have procedures in place to mitigate, to the maximum extent practicable, any deleterious effect from any Use or Disclosure (as defined by 45 C.F.R. §160.103).

f. Sanctions. Business Associate shall apply appropriate sanctions in accordance with Business Associate's policies against any employee, subcontractor or agent who uses or discloses Covered Entity's PHI in violation of this Agreement or applicable law.

g. Covered Entity's Rights of Access and Inspection. From time to time upon reasonable notice, or upon a reasonable determination by Covered Entity that Business Associate has breached this Agreement, Covered Entity may inspect the facilities, systems, books and records of Business Associate related to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity or the safeguarding of such PHI to monitor compliance with this Agreement. Business Associate shall document and keep current such security measures and safeguards and make them available to Covered Entity for inspection upon reasonable request including summaries of any internal or external assessments Business Associate performed related to such security controls and safeguards. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Agreement, nor does Covered Entity's (1) failure to detect or (2) detection but failure to require Business Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of Covered Entity's enforcement or termination rights under this Agreement. This Section shall survive termination of this Agreement.

h. United States Department of Health and Human Services. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on

behalf of, Covered Entity available to the Secretary of the United States Department of Health and Human Services for purposes of determining Covered Entity's compliance with HIPAA and the HIPAA regulations, provided that Business Associate shall promptly notify Covered Entity upon receipt by Business Associate of any such request for access by the Secretary of the United States Department of Health and Human Services, and shall provide Covered Entity with a copy thereof as well as a copy of all materials disclosed pursuant thereto, unless otherwise prohibited by law.

i. Training. Business Associate shall provide such training in the privacy and security of PHI to its Workforce (as that term is defined by 45 C.F.R. § 160.103) as is required for Business Associate's compliance with HIPAA, HIPAA Regulations, HITECH, and the MRPA.

6. Obligation to Provide Access, Amendment and Accounting of PHI.

a. Access to PHI. Business Associate shall make available to Covered Entity, in the time and manner designated by the Covered Entity, such information as necessary to allow Covered Entity to meet its obligations under the HIPAA Regulations, PHI contained in a Designated Record Set held by Business Associate as Covered Entity may require to fulfill Covered Entity's obligations to provide access to, and copies of, PHI in accordance with HIPAA and the HIPAA Regulations and MRPA. In the event that any individual requests access to PHI directly from Business Associate, Business Associate shall notify Covered Entity within five (5) business days that such request has been made.

b. Amendment of PHI. Business Associate shall make available to Covered Entity PHI contained in a Designated Record Set held by Business Associate as Covered Entity may require to fulfill Covered Entity's obligations to amend PHI in accordance with HIPAA and the HIPAA Regulations. In addition, Business Associate shall, as directed by Covered Entity, incorporate any amendments to Covered Entity's PHI into copies of such information maintained by Business Associate. In the event that any individual requests amendment of PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five (5) business days.

c. Accounting of Disclosures of PHI.

1) Record of Disclosures. Business Associate shall maintain a record of all disclosures of PHI received from, or created or received by Business Associate on behalf of, Covered Entity, except for those disclosures identified in Section 6(c)(2) below, including the date of the disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure which includes an explanation of the reason for such disclosure. Business Associate shall make this record available to Covered Entity upon Covered Entity's request. If Business Associate maintains records in electronic form, Business Associate shall account for all disclosures made during the period of three (3) years preceding the request. In the event that any individual requests an accounting of

disclosures of PHI directly from Business Associate, Business Associate shall notify Covered Entity within five (5) business days that such request has been made and provide Covered Entity with a record of disclosures within ten (10) days of an individual's request. If the request from an individual comes directly to Covered Entity and Covered Entity notifies Business Associate that it requires information from Business Associate in order to respond to the individual, Business Associate shall make available to Covered Entity such information as Covered Entity may require within ten (10) days from the time of request by Covered Entity.

2) Certain Disclosures Need Not Be Recorded. The following disclosures need not be recorded:

a) disclosures to carry out Covered Entity's treatment, payment and health care operations as defined under the HIPAA Regulations;

b) disclosures to individuals of PHI about them as provided by the HIPAA Regulations;

c) disclosures for Covered Entity's facility's directory, to persons involved in the individual's care, or for other notification purposes as provided by the HIPAA Regulations;

d) disclosures for national security or intelligence purposes as provided by the HIPAA Regulations;

e) disclosures to correctional institutions or law enforcement officials as provided by the HIPAA Regulations;

f) disclosures that occurred prior to the later of (i) the Effective Date or (ii) the date that Covered Entity is required to comply with HIPAA and the HIPAA Regulations;

g) disclosures pursuant to an individual's authorization in accordance with HIPAA and the HIPAA Regulations; and

h) any other disclosures excepted from the right to an accounting by the HIPAA Regulations.

7. Material Breach, Enforcement and Termination.

a. Term. This Agreement shall become effective on the Effective Date and shall continue unless or until this Agreement terminates, the Underlying Agreement terminates, or the Business Associate has completed performance of the services in the Underlying Agreement, whichever is earlier.

b. Termination. Either Party may terminate this Agreement:

1) immediately if the other Party is finally convicted in a criminal proceeding for a violation of HIPAA or the HIPAA Regulations;

2) immediately if a final finding or stipulation that the other Party has violated any standard or requirement of HIPAA or other security or privacy laws is made in any administrative or civil proceeding in which the other Party has been joined; or completed performance of the services in the Underlying Agreement, whichever is earlier.

3) pursuant to Sections 7(c) or 8(b) of this Agreement.

c. Remedies. Upon a Party's knowledge of a material breach by the other Party, the non-breaching Party shall either:

1) provide an opportunity for the breaching Party to cure the breach and end the violation or terminate this Agreement and the Underlying Agreement if the breaching Party does not cure the breach or end the violation within ten (10) business days or a reasonable time period as agreed upon by the non-breaching party; or

2) immediately terminate this Agreement and the Underlying Agreement if cure is not possible.

d. Injunctions. Covered Entity and Business Associate agree that any violation of the provisions of this Agreement may cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law or in equity, Covered Entity shall be entitled to seek an injunction or other decree of specific performance with respect to any violation of this Agreement or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages.

e. Indemnification. This indemnification provision is enforceable against the Parties only to the extent authorized under the Constitution and laws of the State of Texas. The Parties will indemnify, defend and hold harmless each other and each other's respective employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as "indemnified party," against all actual and direct losses suffered by the indemnified party and all liability to third parties arising from or in connection with any breach of this Agreement or of any warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under MRPA, HIPAA, the HIPAA Regulations, and the HITECH Act by the indemnifying party or its employees, directors, officers, subcontractors, agents or other members of its workforce.

f. Breach of PHI and Breach of System Security. To the extent permitted by the laws and the Constitution of the state of Texas, Business Associate will pay or reimburse Covered Entity for all costs and penalties incurred by Covered Entity in connection with any incident giving rise to a Breach of PHI and/or a Breach of System Security, including without limitation all costs related to any investigation,

any notices to be given, reasonable legal fees, or other actions taken to comply with HIPAA, the HITECH Act, or any other applicable law or regulation, where (i) the PHI was in the custody or control of Business Associate when the Breach of PHI and/or Breach of System Security occurred, or (ii) the Breach of PHI and/or Breach of System Security was caused by the negligence or wrongful acts or omissions of Business Associate and its employees, directors, officers, subcontractors, agents or other members of its workforce.

8. General Provisions.

a. State Law. Nothing in this Agreement shall be construed to require Business Associate to use or disclose PHI without written authorization from an individual who is a subject of the PHI, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure.

b. Amendment. Covered Entity and Business Associate agree to enter into good faith negotiations to amend this Agreement to come into compliance with changes in state and federal laws and regulations relating to the privacy, security and confidentiality of PHI. Covered Entity may terminate this Agreement upon thirty (30) days written notice in the event that Business Associate does not promptly enter into an amendment that Covered Entity, in its sole discretion, deems sufficient to ensure that Covered Entity will be able to comply with such laws and regulations.

c. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than Covered Entity, Business Associate, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

d. Ambiguities. The Parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable law protecting the privacy, security, and confidentiality of PHI, including, without limitation, MRPA, HIPAA, the HIPAA Regulations, and the HITECH Act.

e. Primacy. To the extent that any provision of this Agreement conflicts with the provision of any other agreement or understanding between the Parties, this Agreement shall control.

f. Destruction/Return of PHI. Business Associate agrees that, pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(I), upon termination of this Agreement or the Underlying Agreement, for whatever reason,

1) It will return or destroy all PHI, if feasible, received from or created or received by it on behalf of Covered Entity that Business Associate maintains in any form, and retain no copies of such information which for purposes of this Agreement shall mean all backup tapes. Prior to doing so, Business Associate further agrees to recover any PHI in the possession of its subcontractors or agents. An authorized representative of Business Associate shall certify in writing to Covered Entity, within thirty (30) days from the date of termination or other expiration of the Underlying Agreement, that all

PHI has been returned or disposed of as provided above and that Business Associate or its subcontractors or agents no longer retain any such PHI in any form.

2) If it is not feasible for Business Associate to return or destroy said PHI, Business Associate will notify the Covered Entity in writing. The notification shall include a statement that the Business Associate has determined that it is infeasible to return or destroy the PHI in its possession, and the specific reasons for such determination. Business Associate shall comply with the Security Rule and extend any and all protections, limitations and restrictions contained in this Agreement to Business Associate's use and/or disclosure of any PHI retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible.

3) If it is infeasible for Business Associate to obtain, from a subcontractor or agent any PHI in the possession of the subcontractor or agent, Business Associate must provide a written explanation to Covered Entity and require the subcontractors and agents to agree to comply with the Security Rule and extend any and all protections, limitations and restrictions contained in this Agreement to the subcontractors' and/or agents' use and/or disclosure of any PHI retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible.

g. Offshore Work. In performing the functions, activities or services for, or on behalf of Covered Entity, Business Associate shall not, and shall not permit any of its agents or subcontractors who receive Covered Entity's PHI to, transmit or make available any PHI to any entity or individual outside the United States without prior written consent of Covered Entity.

h. Integration. This Agreement embodies and constitutes the entire agreement and understanding between the Parties with respect to the subject matter hereof and supersedes all prior oral or written agreements, commitments and understandings pertaining to the subject matter hereof.

i. Governing Law. This Agreement is governed by, and shall be construed in accordance with, applicable federal law and the laws of the State of Texas without regard to choice of law principles.

j. Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below, and/or (other than for the delivery of fees) via facsimile to the facsimile telephone numbers listed below.

If to Business Associate: The University of Texas at Austin
Vice President of Legal Affairs

If to Covered Entity:

Williamson County
Attn: County Judge
710 South Main Street, Suite 101
Georgetown, Texas 78626

Each Party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner herein above provided.

k. Privilege. Notwithstanding any other provision in this Agreement, this Agreement shall not be deemed to be an agreement by Business Associate to disclose information that is privileged, protected, or confidential under applicable law to the extent that such privilege, protection or confidentiality (a) has not been waived or (b) is not superseded by applicable law.

l. Multiple Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which shall together constitute one and the same instrument. Facsimile and electronic (pdf) signatures shall be treated as if they are original signatures.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their respective duly authorized representatives in the manner legally binding upon them as of the date indicated below.

Williamson County	The University of Texas at Austin
By: _____ (Authorized Signature)	By: DocuSigned by: Mohini Patel CA21577FB04F443... (Authorized Signature)
Name: _____ (Type or Print)	Name: Mohini Patel (Type or Print)
Title: _____	Title: Sr. Manager
Date: _____	Date: 2023-05-05 | 11:30:14 CDT

DocuSign

Certificate Of Completion

Envelope Id: DD6ADE7A84A449D4BCE704D7FF7CD11F
Status: Completed
Subject: Complete with DocuSign: UTAUS-DUA00000752 WilCo EMS Clean.docx
Source Envelope:
Document Pages: 18
Signatures: 2
Certificate Pages: 1
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-06:00) Central Time (US & Canada)

Envelope Originator:
Mohini Patel
1 University Station
Austin, TX 78712
mp33283@eid.utexas.edu
IP Address: 70.115.145.210

Record Tracking

Status: Original
5/5/2023 11:28:21 AM
Holder: Mohini Patel
mp33283@eid.utexas.edu
Location: DocuSign

Signer Events	Signature	Timestamp
Mohini Patel mp33283@eid.utexas.edu Sr. Manager The University of Texas at Austin Security Level: Email, Account Authentication (None)	DocuSigned by: Mohini Patel CA21577FB04F443... Signature Adoption: Pre-selected Style Using IP Address: 70.115.145.210	Sent: 5/5/2023 11:29:35 AM Viewed: 5/5/2023 11:29:52 AM Signed: 5/5/2023 11:30:14 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	5/5/2023 11:29:36 AM
Certified Delivered	Security Checked	5/5/2023 11:29:52 AM
Signing Complete	Security Checked	5/5/2023 11:30:14 AM
Completed	Security Checked	5/5/2023 11:30:14 AM

Payment Events	Status	Timestamps