

**INTERLOCAL COOPERATION AGREEMENT FOR PUBLIC HEALTH DATA SHARING  
BETWEEN AUSTIN PUBLIC HEALTH AND  
THE TRAVIS COUNTY HEALTHCARE DISTRICT**

This Interlocal Cooperation Agreement ("Agreement") for Public Health Data Sharing is made by and between the Travis County Healthcare District d/b/a Central Health ("Central Health" or the "Coordinating Entity"), a hospital district operating under Chapters 61 and 281 of the Texas Health & Safety Code, and Austin Public Health, a department of the City of Austin (the "City" or "Austin Public Health" or "APH"). Each is individually a "Party" and collectively, the "Parties."

**WHEREAS**, on March 6, 2020, a Declaration of Local Disaster was issued to allow the City of Austin to take measures to reduce the possibility of exposure to COVID-19 and promote the health and safety of Austin residents; and

**WHEREAS**, on March 13, 2020, a Declaration of State of Disaster was issued by Governor Abbott to take additional steps to prepare for, respond to, and mitigate the spread of COVID-19 to protect the health and welfare of Texans; and

**WHEREAS**, Austin Public Health, a department of the City of Austin, is a "health authority", as such term is defined by Section 81.003 of the Texas Health & Safety Code, and is a "public health authority" within the meaning of 45 C.F.R. § 164.50, and

**WHEREAS**, pursuant to 45 C.F.R. § 164.512(b), a covered entity may disclose data, including Protected Health Information ("PHI"), to a public health authority for the purpose of preventing or controlling disease; and

**WHEREAS**, the COVID-19 virus is contagious and spreads through person-to-person contact, especially in group settings, making it a communicable disease under Chapter 81 of the Texas Health & Safety Code (the "Communicable Disease Prevention and Control Act"); and

**WHEREAS**, a health authority has the duty to administer state and local laws relating to public health and shall perform each of the duties listed in Section 121.024 of the Texas Health & Safety Code, including aiding the Department of State Health Services in relation to disease prevention and suppression; and

**WHEREAS**, Central Health and Austin Public Health are each Covered Entities, as such term is defined by the Health Insurance Portability and Accountability Act ("HIPAA") and Chapter 181 of the Texas Health & Safety Code (the "Texas Medical Records Privacy Act"), and both Parties are committed to complying with HIPAA and the Texas Health & Safety Code; and,

**WHEREAS**, in order to fulfill its mission to understand, respond to, and mitigate the spread of COVID-19, APH is in need of assistance from Coordinating Entity;

**WHEREAS**, Central Health seeks to perform certain duties to help Austin Public Health accomplish this mission;

**NOW, THEREFORE**, in consideration of the mutual covenants, representations, and warranties contained herein, the Parties agree as follows:

## A. DEFINITIONS

1. **Central Health Data** includes medical or epidemiological information in its possession regarding individuals who have been diagnosed with or suspected to have COVID-19. This may include direct identifiers, such as:
  - a) Full name of individual,
  - b) Birth date and date of death, if applicable,
  - c) Age, race, and sex,
  - d) Telephone or fax numbers,
  - e) Electronic mail addresses
  - f) Results of any COVID-19 tests administered,
  - g) Probable source of infection,
  - h) Treatment provided and name of treating provider, and
  - i) The date of disease onsets.
2. **APH Data** includes information regarding possible, suspected, or confirmed individuals with COVID-19 that APH collects from providers and other entities whom are required to report communicable diseases pursuant to 81.042. This may include direct identifiers and includes, but is not limited to:
  - a) Dates of treatment, admission, and discharge,
  - b) Full name of individual and address,
  - c) Birth date and date of death, if applicable
  - d) Age, race, and sex,
  - e) Telephone or fax numbers,
  - f) Electronic mail addresses,
  - g) Results of any COVID-19 tests administered,
  - h) Symptoms and probable source of infection,
  - i) Treatment provided and name of treating provider, and
  - j) Other personal identifiers.
3. When the term "Data" is used without an identifier, it refers to both Central Health Data and APH Data collectively.
4. **Commercial Purposes** includes the sale, lease, license, or other transfer of the Data to a for-profit organization or an insurance company and shall also include uses of the Data by any organization to perform contract research, to produce or manufacture products for general sale, or to conduct research activities that result in any sale, lease, license, or transfer of the Data to a for-profit organization.

## **B. SCOPE AND PURPOSE**

1. This Agreement sets forth the terms and conditions pursuant to which APH and the Coordinating Entity will share Data. Central Health and the City agree to send Data in native formats whenever possible.
2. The City and Coordinating Entity will only use the Data shared pursuant to this Agreement for the purposes of identifying, controlling, and preventing disease, such as case management, chemoprophylaxis, and health education, or for treatment. Any and all other uses or disclosures of the Data are prohibited by Section 81.046 of the Communicable Disease Prevention and Control Act and may not be pursued by the Coordinating Entity. For avoidance of doubt, the Data may not be used by either Party for any Commercial Purposes.
3. To assist APH, Central Health may be assigned to screen and investigate individuals exposed to, suspected of having, or confirmed to have COVID-19 and, if a person confirmed to have COVID-19 is a MAP or MAP Basic enrollee, to provide case management. This work includes, but is not limited to, managing or monitoring individuals who test positive for COVID-19, tracing contacts of such individuals as needed, and making recommendations to the City of Austin leadership and its public health partners regarding COVID-19 spread.
4. APH and Central Health will work in partnership to use and disclose protected health information created or maintained by APH and other health care providers with whom either Central Health or APH has a relationship for public health purposes to assist the City in its public health mission of preventing or controlling disease, specifically COVID-19.
5. The Parties agree to comply with the privacy standards adopted by the U.S. Department of Health and Human Services at 45 C.F.R. Parts 160 and 164, as well as, the security standards adopted by the U.S. Department of Health and Human Services at 45 C.F.R. parts 160, 162 and 164, and any applicable state confidentiality laws.

## **C. APH'S RESPONSIBILITIES AND RIGHTS**

1. The City will and does hereby grant authority to Central Health to work in partnership with APH to assist APH in its public health mission of preventing or controlling disease, specifically COVID-19.
2. The City may send APH Data regarding confirmed and suspected cases of COVID-19 to the Coordinating Entity on a regular and timely basis so that the Coordinating Entity can assist APH in its public health mission of preventing or controlling disease, specifically COVID-19.
3. The City may continue to share APH Data with the Coordinating Entity until this agreement is terminated.
4. APH will retain ownership of the APH Data sent to Central Health.
5. Within five days of the execution of the Agreement, APH will furnish Central Health with a list (List) of other entities (Partners) with whom APH has executed Data Sharing Agreements that allows Partners to assist APH's efforts at researching, investigating, and controlling current and prospective cases of Covid-19. APH authorizes Central Health to share APH Data with Partners, without cost, for the public health purposes detailed in Section B.

6. APH will provide Central Health with an updated List reflecting the most current list of Partners as changes are made to the List.

#### **D. CENTRAL HEALTH'S RESPONSIBILITIES**

1. Central Health will, in accordance with Section 81.042(e)(7) of the Communicable Disease Prevention and Protection Act and 45 CFR 164.512(b)(1), share Central Health Data, including protected health information as such term is defined by HIPAA ("PHI"), on an ongoing basis with APH in order to report that MAP and MAP Basic enrollees are suspected of having or are confirmed to have COVID-19.
2. Central Health will rely on any direction received from APH regarding minimum necessary determinations for public health purposes.
3. To ensure coordination among APH and its Partners, Central Health will notify APH of confirmed cases prior to initiating case and contact investigation. Central Health will also report any findings on surveillance that it conducts on behalf of APH. This applies both to subjects tested by Central Health's co-applicant for federally qualified health center status, CommUnityCare, and those tested by other entities with whom Central Health has a contract.
4. Central Health agrees to use appropriate data security measures and other safeguards to prevent the inappropriate use or disclosure of APH Data in accordance with relevant laws and the terms of the Business Associate Agreement, attached hereto and incorporated herein, as Attachment A.
5. Except for the public health activities described in Sections 1-4 above, Central Health will not share the APH Data with other entities without the express permission of the City or publish any surveillance findings that Central Health makes with APH Data, unless APH provides its approval for publication and Central Health lists APH as a co-author whenever appropriate. For avoidance of doubt, the word "publish" does not include presentation to the governing board of Central Health or any of its committees.

#### **E. TEXAS PUBLIC INFORMATION ACT AND OTHER DISCLOSURE REQUESTS**

1. Pursuant to Texas Health & Safety Code Sections 81.046 and 181.006, the Data is not public information subject to disclosure under Chapter 552 of the Texas Government Code, known as the Texas Public Information Act ("TPIA"). The City and Central Health agree that the sharing of Data is an intergovernmental transfer of information, and not the release of public information.
2. If either Party receives a request for the Data, including a subpoena or a TPIA request, it must inform the other Party within three (3) business days and again at least five (5) business days before responding to the request.

#### **F. TERM, TERMINATION, AND RATIFICATION**

1. The Parties agree that, if either Party begins to perform its responsibilities hereunder before receiving the approval of its governing body, the Party who has begun performance will seek ratification of the actions it has taken prior execution of this Agreement by both Parties.
2. The term of this Agreement is for a period of one (1) year, beginning on June 1, 2020. This Agreement shall automatically renew for another one (1) year term at the end of this period and

will continue to renew each year thereafter unless superseded by a supplemental agreement, the declarations of disaster referenced in the recitals have been lifted, or this Agreement as terminated as provided below.

3. Either Party can elect to terminate this Agreement by giving the other Party thirty (30) days' notice; provided, however, that such termination will not result in the termination of the Business Associate Agreement attached hereto, which will remain in effect until Central Health has destroyed the APH Data provided to it. To the extent that Data is not capable of being destroyed, the Parties' obligations to protect Data provided hereunder, or in accordance with, this Agreement shall survive the termination of this Agreement.

#### **G. REPRESENTATIONS AND WARRANTIES**

1. This Agreement is authorized and governed, in part, by the Interlocal Cooperation Act, Chapter 791 of the Texas Government Code. Each party represents and warrants that, in the performance of its respective obligations under this Agreement, it is carrying out a duly authorized governmental function, which it is authorized to perform individually under the applicable statutes of the State of Texas and/or its charter.
2. Both Parties further represent and warrant that they will comply with all federal, state, county, and city statutes, rules, regulations, and ordinances that are applicable to the covenants and responsibilities established under the Agreement, including the Communicable Disease Prevention and Control Act, HIPAA, the Texas Medical Records Privacy Act, and the Local Public Health Reorganization Act, Chapter 121 of the Texas Health & Safety Code.
3. The City represents and warrants that Central Health shall not be liable for the death of or injury to a person or for damage to property on account of Section 81.007 of the Communicable Disease Prevention and Protection Act.

#### **H. COMPENSATION**

1. The Parties agree that there will be no payment exchanged for either Party's services or for their expenses or costs, including the costs of labor. Each Party shall be responsible for its own costs and expenses.
2. Notwithstanding the foregoing, the Parties will work together to obtain any governmental reimbursement available for the activities performed under this Agreement, including reimbursement that may need to flow through one Party to the other.

#### **I. LAW AND INTERPRETATIONAL GUIDELINES**

1. Nothing in this Agreement shall be construed to create between the Parties or any of their affiliates: (a) a partnership, joint venture, or other joint business relationship; (b) any fiduciary duty; or (c) an agency or employment relationship.
2. The provisions of this Agreement shall be severable and, if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

3. This Agreement shall be construed in accordance with and governed by the laws of the State of Texas. Any suit, action or proceeding against either Party with respect to this Agreement shall be brought in the state or federal courts located in Travis County, Texas.

#### J. MISCELLANEOUS

1. Any notices pertaining to this Agreement shall be given in writing and received at the following address:
  - a) For APH  
Attn: Director, Austin Public Health  
7201 Levander Loop,  
Austin, TX, 78702
  - b) For Central Health  
ATTN: Chief Operating Officer  
1111 E. Cesar Chavez St.  
Austin, TX 78702.
2. Neither Party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed.
3. The Agreement can be modified or amended only by a writing signed by both Parties.
4. An electronic copy or facsimile of a signature hereto will be binding upon the signatory as if it were an original signature.

IN WITNESS WHEREOF, the Parties have executed this Agreement effective upon the Effective Date set forth above.

AUSTIN PUBLIC HEALTH

By: 

(Authorized Signature)

Print name: Stephanie Hayden

Title: Director

Date: 06/02/2020

CENTRAL HEALTH

By: 

(Authorized Signature)

Print name: Mike Geeslin

Title: President & CEO

Date: \_\_\_\_\_

2 June 2020

## **Attachment A**

### **Business Associate Agreement Provisions**

This Business Associate Agreement (the "BAA"), is made as of the 1st day of May, 2020 (the "Effective Date"), by and between the Travis County Healthcare District d/b/a Central Health ("Business Associate") and the City of Austin, a Texas home rule municipal corporation ("Covered Entity," "City" or "APH") (collectively the "Parties") to comply with the privacy standards adopted by the U.S. Department of Health and Human Services, as they may be amended from time to time, at 45 C.F.R. parts 160 and 164 ("the Privacy Rule") and security standards adopted by the U.S. Department of Health and Human Services, as they may be amended from time to time, at 45 C.F.R. parts 160, 162 and 164 ("the Security Rule"), and the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 and regulations promulgated thereunder, and any applicable state confidentiality laws.

### **RECITALS**

WHEREAS, Business Associate will provide the City with the assistance described in the Interlocal Cooperation Agreement for Public Health Data Sharing (the "Services Agreement"), which relates to the City's efforts to prevent and control the spread of a communicable disease, specifically COVID-19 (the "Services");

WHEREAS, in connection with these Services, Covered Entity will disclose to Business Associate certain protected health information that is subject to HIPAA; and

WHEREAS, HIPAA requires that the Covered Entity receive adequate assurances that Business Associate will comply with certain obligations with respect to the Protected Health Information (PHI) received in the course of providing Services to or on behalf of Covered Entity.

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

- A. **Definitions.** Terms used herein, but not otherwise defined, shall have the meaning ascribed by the Privacy Rule and the Security Rule.
1. **HIPAA Rules.** The Privacy Rule and the Security Rule, and amendments codified and promulgated by the HITECH Act are referred to collectively herein as "HIPAA Rules."
  2. **Incident.** "Incident" means a potential or attempted unauthorized access, use, disclosure, modification, loss, disruption, or destruction of PHI, which has the potential for jeopardizing the confidentiality, integrity, or availability of the PHI.
  3. **Sensitive Personal Information.** "Sensitive Personal Information" shall mean 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; driver's license number or government-issued identification number; or 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 b) information that identifies an individual and relates to: the physical or mental health or condition of the individual; the provision of health care to the individual; or payment for the provision of health care to the individual.

B. Purposes for which PHI May Be Disclosed to Business Associate. In connection with the Services provided by Business Associate to or on behalf of Covered Entity, Covered Entity may disclose PHI to Business Associate for the purposes of preventing or controlling disease, specifically COVID-19.

C. Obligations of Covered Entity. If deemed applicable by Covered Entity, Covered Entity shall:

1. provide Business Associate a copy of its Notice of Privacy Practices ("Notice") produced by Covered Entity in accordance with 45 C.F.R. 164.520 as well as any changes to such Notice;
2. provide Business Associate with any changes in, or revocation of, authorizations by Individuals relating to the use and/or disclosure of PHI, if such changes affect Business Associate's permitted or required uses and/or disclosures;
3. notify Business Associate of any restriction to the use and/or disclosure of PHI to which Covered Entity has agreed in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI;
4. not request Business Associate to use or disclose PHI in any manner that would be impermissible under the Privacy Rule if done by the Covered Entity;
5. notify Business Associate of any amendment to PHI to which Covered Entity has agreed which affects a Designated Record Set maintained by Business Associate; and
6. if Business Associate maintains a Designated Record Set, provide Business Associate with a copy of its policies and procedures related to an Individual's right to: access PHI; request an amendment to PHI; request confidential communications of PHI; or request an accounting of disclosures of PHI.

D. Obligations of Business Associate. Business Associate agrees to comply with the provisions of the HIPAA Rules applicable to Business Associates, including:

1. Use and Disclosure of PHI. Except as otherwise permitted by this BAA, the Services Agreement, or applicable law, Business Associate shall only use or disclose PHI to provide the Services to or on behalf of Covered Entity, and shall not use or disclose PHI that would violate the HIPAA Rules if used or disclosed by



Covered Entity. Notwithstanding the foregoing, Business Associate may use and disclose PHI as necessary for the proper management and administration of Business Associate, or to carry out its legal responsibilities. Before Business Associate may use or disclose the information for the purposes described in the immediately preceding sentences, Business Associate shall:

- (a) provide information and training to members of its workforce who will use or disclose PHI regarding the confidentiality requirements of the HIPAA Rules and this BAA;
- (b) obtain reasonable assurances from the person or entity to whom the PHI is disclosed that: (a) the PHI will be held confidential and further used and disclosed only as Required by Law or for the purpose for which it was disclosed to the person or entity; and (b) the person or entity will notify Business Associate of any instances of which it is aware in which confidentiality of the PHI has been breached; and
- (c) agree to notify Covered Entity of any instances of which it is aware in which the PHI is used or disclosed for a purpose that is not otherwise provided for in this Agreement or for a purpose not expressly permitted by the HIPAA Rules.

2. Data Aggregation. In the event that Business Associate works for more than one Covered Entity, Business Associate is permitted to use and disclose PHI for Data Aggregation purposes.

3. De-identified Information. Business Associate may use and disclose de-identified health information if it receives written approval from the Covered Entity and the PHI is de-identified in compliance with the HIPAA Rules.

4. Safeguards.

- (a) Business Associate shall maintain appropriate safeguards to ensure that PHI is not used or disclosed other than as provided by this BAA, the Agreement, or as Required by Law. 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) Business Associate shall assure that all PHI is secured when it is transmitted and stored.
- (c) Business Associate shall apply access controls to ensure that an employee's access to PHI is attendant to legitimate business needs.

5. Minimum Necessary. Business Associate shall confirm that all uses and disclosures of PHI are consistent with the principle of "minimum necessary use and disclosure," i.e., that only PHI that is the minimum necessary to accomplish the

intended purpose of the use, disclosure, or request is used or disclosed; and the use of limited data sets when possible.

6. Disclosure to Agents and Subcontractors. If Business Associate discloses PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, to agents, including a subcontractor, Business Associate shall require the agent or subcontractor to agree to the same restrictions and conditions as apply to Business Associate under this BAA.

7. Individual Rights Regarding Designated Record Sets. If Business Associate maintains a Designated Record Set on behalf of Covered Entity, Business Associate agrees as follows:

(a) Individual Right to Copy or Inspection. Business Associate will permit an Individual to inspect or copy PHI about the Individual in that Designated Record Set as directed by Covered Entity to meet the requirements of 45 C.F.R. § 164.524. If the PHI is in electronic format, the Individual shall have a right to obtain a copy of such information in electronic format, and if the Individual chooses, to direct that an electronic copy be transmitted directly to an entity or person designated by the individual in accordance with Section 13405(c) of the HITECH Act. Under the Privacy Rule, Covered Entity is required to take action on such requests as soon as possible, but not later than 30 days following receipt of the request. Business Associate agrees to make reasonable efforts to assist Covered Entity in meeting this deadline by responding to the Individual's request within 15 days following receipt of the request. The information shall be provided in the form or format requested if it is readily producible in such form or format; or in summary if the Individual has agreed in advance to accept the information in summary form. A reasonable, cost-based fee for copying health information may be charged. If Covered Entity maintains the requested records, Covered Entity, rather than Business Associate, shall permit access according to its policies and procedures implementing the Privacy Rule.

(b) Individual Right to Amendment. Business Associate agrees to make amendments to PHI at the request and direction of Covered Entity pursuant to 45 C.F.R. §164.526. If Business Associate maintains a record in a Designated Record Set that is not also maintained by Covered Entity, Business Associate agrees that it will accommodate an Individual's request to amend PHI only in conjunction with a determination by Covered Entity that the amendment is appropriate according to 45 C.F.R. §164.526.

(c) Accounting of Disclosures. Business Associate agrees to maintain documentation of the information required to provide an accounting of disclosures of PHI, whether PHI is in paper or electronic format, in accordance with 45 C.F.R. §164.528 and Section 13405(c) of the HITECH Act, and to make this information available to Covered Entity upon Covered Entity's request. Under the Privacy Rule, Covered Entity is required to take

action on such requests as soon as possible but not later than 60 days following receipt of the request. Business Associate agrees to use its best efforts to assist Covered Entity in meeting this deadline but not later than 30 days following receipt of the request. Such accounting must be provided without cost to the Individual or Covered Entity if it is the first accounting requested by an Individual within any 12 month period; however, a reasonable, cost-based fee may be charged for subsequent accountings if Business Associate informs the Individual in advance of the fee and affords the Individual an opportunity to withdraw or modify the request. Such accounting is limited to disclosures that were made in the six years prior to the request (not including disclosures prior to the compliance date of the Privacy Rule) and shall be provided for as long as Business Associate maintains the PHI.

8. Internal Practices, Policies, and Procedures, and Audit. Except as otherwise specified herein, Business Associate shall make available the internal practices, policies, books, records, and procedures relating to the use and disclosure of PHI that it has received from Covered Entity to the Secretary, or his or her agents for the purpose of determining Covered Entity's compliance with the HIPAA Rules, or any other health oversight agency, or to Covered Entity. Records requested that are not protected by an applicable legal privilege will be made available in the time and manner specified by the Secretary. Except to the extent prohibited by law, Business Associate agrees to notify Covered Entity immediately upon receipt by Business Associate of any and all requests by or on behalf of any and all federal, state, and local government authorities served upon Business Associate for PHI.
9. Notice of Privacy Practices. Business Associate shall abide by the limitations of Covered Entity's Notice of which it has knowledge. Any use or disclosure permitted by this BAA may be amended by changes to Covered Entity's Notice; provided, however, that the amended Notice shall not affect permitted uses and disclosures on which Business Associate relied prior to receiving notice of such amended Notice.
10. Withdrawal of Authorization. If the use or disclosure of PHI in this BAA 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.
11. Knowledge of HIPAA Rules. Business Associate agrees to review and understand the HIPAA Rules as it applies to Business Associate, and to comply with the applicable requirements of the HIPAA Rule, as well as any applicable amendments.

12. Incident Notification. To the extent feasible, Business Associate will use commercially reasonable efforts to ensure that the technology safeguards used by Business Associate to secure PHI will render such PHI unusable, unreadable and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with HHS Guidance published at 74 Federal Register 19006 (April 17, 2009) or such later regulations or guidance promulgated by HHS or issued by the National Institute for Standards and Technology (also known as "NIST") concerning the protection of identifiable data such as PHI. Business Associate will promptly report any successful Incident of which it becomes aware and, at the request of the Covered Entity, will identify: the date of the Incident; scope of Incident; Business Associate's response to the Incident; and the identification of the party responsible for causing the Incident.
13. Information Breach Notification for PHI. Business Associate expressly recognizes that Covered Entity has certain reporting and disclosure obligations to the Secretary and the Individual in case of a security breach of unsecured PHI. Where Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured paper or electronic PHI, immediately following the "discovery" (within the meaning of 45 C.F.R. §164.410(a)) of a Breach of such information, Business Associate shall notify Covered Entity of such Breach. Initial notification of the Breach does not need to be in compliance with 45 C.F.R. §164.404(c); however, Business Associate must provide Covered Entity with all information necessary for Covered Entity to comply with 45 C.F.R. §164.404(c) without reasonable delay, and in no case later than **fifteen calendar days** following the discovery of the Breach. Business Associate shall be liable for the costs associated with such breach if caused by the Business Associate's willful acts or omissions, or the willful acts or omissions of Business Associate's agents, officers, employees or subcontractors.
14. Breach Notification to Individuals. Business Associate's duty to notify Covered Entity of any Breach does not permit Business Associate to notify those individuals whose PHI has been breached by Business Associate without the express written permission of Covered Entity to do so. Any and all notification to those Individuals whose PHI has been breached shall be made by Covered Entity. The cost of the notification will be paid by the Business Associate.
15. Data Breach Notification and Mitigation Under Other Laws. In addition, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any Breach of individually identifiable information (including but not limited to PHI and referred to hereinafter as "Individually Identifiable Information") and Sensitive Personal Information subject to Section 521.053 of the Texas Business and Commerce Code that, if misused, disclosed, lost or stolen, would trigger an obligation under Chapter 521 of the Texas Business and Commerce Code (the "Identity Theft Enforcement and Protection Act") to notify the individuals who are the subject of the information. Business Associate agrees that in the event any Individually Identifiable Information and Sensitive Personal Information is lost, stolen, used or disclosed in violation of HIPAA or the Identity

Theft Enforcement and Protection Act, Business Associate shall promptly: (i) notify the Covered Entity within **fifteen calendar days** of such misuse, disclosure, loss or theft; (ii) cooperate and assist Covered Entity with any investigation into the loss, theft, or misuse or disclosure; (iii) cooperate and assist Covered Entity with any investigation conducted by any State Attorney General or State Consumer Affairs Department (or their respective agents); (iv) cooperate with Covered Entity regarding the obligations of Covered Entity and Business Associate to mitigate to the extent practicable any potential harm to the individuals impacted by the loss, theft, or misuse or disclosure; and (v) assist with the implementation of any decision by any State agency, including any State Attorney General or State Consumer Affairs Department (or their respective agents), to notify individuals impacted or potentially impacted by the loss, theft, or misuse or disclosure. This requirement shall survive the expiration or termination of this Agreement and shall remain in effect for so long as Business Associate maintains PHI, Individually Identifiable Information, or Sensitive Personal Information that was received from Covered Entity.

E. Permitted Uses and Disclosures by Business Associates. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI to perform functions, activities, or services for or on behalf of Covered Entity as specified in this BAA or in the Services Agreement, provided that such use or disclosure would not violate the HIPAA Rules if done by Covered Entity, or the minimum necessary policies and procedures of the Covered Entity. Also, Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with the HIPAA Rules.

1. Use. Business Associate will not, and will ensure that its officers and employees do not, use PHI other than as permitted or required by Business Associate to perform the Services or as required by law, but in no event in any manner that would constitute a violation of the Privacy Rule or Security Rule if used by Covered Entity.
2. Disclosure. Business Associate will not, and will ensure that its officers and employees do not, disclose PHI other than as permitted pursuant to this BAA, the Services Agreement or as required by law, but in no event disclose PHI in any manner that would constitute a violation of the Privacy Rule or Security Rule if disclosed by Covered Entity.
3. Right Title and Interest. Business Associate acknowledges and agrees that Covered Entity owns all right, title, and interest in and to all PHI, and that such right, title, and interest will be vested in Covered Entity. Neither Business Associate nor any of its officers, employees, agents, or assigns will have any rights in any of the PHI, except as expressly set forth above.

F. Application of Security and Privacy Provisions to Business Associate.

1. Security Measures. Sections 164.308, 164.310, 164.312 and 164.316 of HIPAA Security Rule dealing with the administrative, physical and technical safeguards as well as policies, procedures and documentation requirements that apply to Covered Entity

shall in the same manner apply to Business Associate. Any additional security requirements contained in Sub Title D of Title XIII of Division A of the HITECH Act that apply to Covered Entity shall also apply to Business Associate. Pursuant to the foregoing requirements in this Section F.1, the Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the paper or electronic PHI that it creates, has access to, or transmits. Business Associate will also ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect such information. Business Associate will ensure that PHI contained in portable devices or removable media is encrypted.

2. Annual Guidance. For the first year beginning after the date of the enactment of the HITECH Act and annually thereafter, the Secretary shall annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the Sections referred to in Section F.1 "Security Measures" and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations. Business Associate shall, at their own cost and effort, monitor the issuance of such guidance and comply accordingly.
3. Privacy Provisions. The enhanced HIPAA Privacy Rule requirements, including but not necessarily limited to accounting for certain PHI disclosures for treatment, restrictions on the sale of PHI, restrictions on marketing and fundraising communications, and payment and health care operations contained in Subtitle D of Title XIII of Division A of the HITECH Act that apply to the Covered Entity, shall equally apply to the Business Associate.
4. Application of Civil and Criminal Penalties. If Business Associate violates any security or privacy provision specified in Section 13404(a) and (b) of the HITECH Act, Sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6) shall apply to Business Associate with respect to such violation in the same manner that such Sections apply to Covered Entity if it violates such provisions.

**G. Term and Termination.**

1. Term. This BAA shall be effective as of the Effective Date and shall be terminated when all PHI provided to Business Associate by Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity.
2. Termination without Cause. Either Party shall have the right to terminate this BAA for any reason upon thirty days written notice to the other Party.
3. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

- i. Provide Business Associate with 30 days to cure the breach or end the violation and, if Business Associate does not cure the breach or end the violation within such time, to terminate this BAA; or
    - ii. Immediately terminate this BAA, if termination is feasible.
  4. Effect of Termination. Upon termination of this BAA for any reason, Business Associate agrees to return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, or maintained by Business Associate in any form. If Business Associate determines that the return or destruction of PHI is not feasible, Business Associate shall inform Covered Entity in writing of the reason thereof, and shall agree to extend the protections of this BAA to such PHI, and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the PHI not feasible for so long as Business Associate retains the PHI. This Section shall survive the expiration or termination of this BAA and shall remain in effect for so long as Business Associate maintains PHI.
- H. No Warranty. PHI IS PROVIDED TO BUSINESS ASSOCIATE SOLELY ON AN "AS IS" BASIS. COVERED ENTITY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
- I. Miscellaneous.
1. Indemnification and Insurance. Each Party is self-insured and therefore an insurance policy is not required. Each Party will provide proof of self-insurance upon request. To the extent allowed by Texas law, each Party agrees to be responsible for its own proportionate share of liability for its negligent acts and omissions.
  2. Mitigation. If Business Associate violates this BAA or either of the HIPAA Rules, Business Associate agrees to mitigate any damage caused by such breach.
  3. Survival. The respective rights and obligations of Business Associate under Section E.3 "Right Title and Interest" of this BAA shall survive the termination of this Agreement.
  4. Notices. Any notices pertaining to this BAA shall be given in writing and shall be deemed duly given when personally delivered to a Party or a Party's authorized representative as listed below or sent by means of a reputable overnight carrier, or sent by means of certified mail, return receipt requested, postage prepaid. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt. All notices shall be addressed to the appropriate Party as follows:

If to Covered Entity:  
Austin Public Health  
7201 Levander Loop  
Austin, TX 78702



Attn: Director

If to Business Associate:  
Central Health  
1111 E. Cesar Chavez St.  
Austin, TX 78702  
Attn: Compliance Officer

5. Amendments. This BAA may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties hereto. The Parties, however, agree to amend this BAA from time to time as necessary, in order to allow Covered Entity's compliance with the requirements of the HIPAA Rules.
6. Choice of Law. This BAA and the rights and obligations of the Parties hereunder shall be governed by and construed under the laws of the State of Texas, without regard to applicable conflict of laws principles.
7. Assignment of Rights and Delegation of Duties. This BAA is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns. However, neither Party may assign any of its rights or delegate any of its obligations under this BAA without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Assignments made in violation of this provision are null and void.
8. Nature of Agreement. Nothing in this BAA shall be construed to create between the Parties (i) a partnership, joint venture or other joint business relationship (ii) any fiduciary duty, or (iii) a relationship of employer and employee.
9. No Waiver. Failure or delay on the part of either Party to exercise any right, power, privilege or remedy hereunder shall not constitute a waiver thereof. No provision of this BAA may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.
10. Equitable Relief. Any disclosure or misappropriation of PHI by Business Associate in violation of this BAA will cause Covered Entity irreparable harm, the amount of which may be difficult to ascertain. Business Associate therefore agrees that Covered Entity shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining Business Associate from any such further disclosure or breach, and for such other relief as Covered Entity shall deem appropriate. Such rights are in addition to any other remedies available to Covered Entity at law or in equity.
11. Severability. The provisions of this BAA shall be severable, and if any provision of this BAA shall be held or declared to be illegal, invalid or unenforceable, the remainder of this BAA shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.



12. No Third Party Beneficiaries. Nothing in this BAA shall be considered or construed as conferring any right or benefit on a person not a party to this BAA nor imposing any obligations on either Party hereto to persons not a party to this BAA.
13. Headings. The descriptive headings of the articles, sections, subsections, exhibits and schedules of this BAA are inserted for convenience only, do not constitute a part of this BAA, and shall not affect in any way the meaning or interpretation of this BAA.
14. Entire Agreement. This BAA constitutes the entire agreement between the Parties hereto with respect to the subject matter hereof, and supersedes all previous written or oral understandings, agreements, negotiations, commitments, and any other writing and communication by or between the Parties with respect to the subject matter hereof.
15. Interpretation. Any ambiguity in this BAA shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Rules and the Texas Identity Theft Enforcement and Protection Act. The provisions of this BAA shall prevail over the provisions of any other agreement that exists between the Parties that may conflict with, or appear inconsistent with, any provision of this Agreement or the HIPAA Rules.
16. Regulatory References. A citation in this BAA to the Code of Federal Regulations, the Federal Register, or any other federal guidance or policy shall mean the cited section or reference as they may be amended from time to time.

Agreed to:

**CITY OF AUSTIN**

By: 

(Authorized Signature)

Name: Stephanie Y. Hayden

(Type or Print)

Title: Director, Austin Public Health

Date: 06/02/2020

**TRAVIS COUNTY HEALTHCARE  
DISTRICT D/B/A CENTRAL HEALTH**

By: 

(Authorized Signature)

Name: Mike Geeslin

(Type or Print)

Title: President & CEO

Date: 2 June 2020