## Business Associate Agreement – City of madison

This Business Associate Agreement (“BAA”) is entered into between the City of Madison, a Wisconsin municipal corporation ("Covered Entity"), and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ("Business Associate"). If this BAA is attached to a contract executed between the above parties (a “Contract”), then Covered Entity and Business Associate agree to incorporate the terms of this BAA into the Contract. This BAA shall supersede any conflicting term in the Contract to the extent stated in section 5.12 herein.

Covered Entity and Business Associate agree to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (“HITECH Act”) and the Genetic Information Nondiscrimination Act (“GINA”) and HIPAA’s implementing regulations, Title 45, Parts 160, 162 and 164 of the Code of Federal Regulations (“Security and Privacy Rule”) as amended (all such laws and regulations shall be collectively referred to herein as "HIPAA"). The BAA will address the security, confidentiality, integrity, and availability of health or health-related information as well as breach notification requirements.

1. **Definitions.** Capitalized terms used in this BAA, but not otherwise defined, have the same meaning as those terms are defined by HIPAA.

(a) Breach means the acquisition, access, Use, or Disclosure of Protected Health Information (“PHI”) in a manner not permitted under HIPAA that compromises the security or privacy of the PHI. PHI is presumed to be compromised unless the Covered Entity or Business Associate, as applicable, documents that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who accessed or Used the PHI or to whom the Disclosure was made;

(iii) Whether the PHI was actually acquired or viewed; and

(iv) The extent to which the risk to the PHI has been mitigated.

Breach excludes:

(i) Any unintentional acquisition, access or Use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business Associate if such acquisition, access, or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under the Privacy Rule.

(ii) Any inadvertent Disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized Health Care arrangement in which the Covered Entity participates, and the information received as a result of such Disclosure is not further used or disclosed in a manner not permitted under the HIPAA.

(iii) A Disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

(b) Protected Health Information or "PHI" means individually identifiable health information (including electronic PHI) of the Covered Entity that is created, used, Disclosed, maintained, or received by the Business Associate, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

(i) Past, present or future physical or mental health or condition of an individual;

(ii) The provision of Health Care to an individual; or

(iii) The past, present, or future payment for the provision of Health Care to an individual

(c) Individual means the person who is the subject of PHI, and shall include a person who qualifies under HIPAA as a personal representative of the Individual.

(d) Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HIPAA.

2. Responsibilities of Business Associate.

2.1 Use and Disclosure. Business Associate may only Use or Disclose PHI received from or on behalf of the Covered Entity as permitted or required by this BAA, by HIPAA, by state confidentiality laws, or as otherwise authorized in writing by the Covered Entity.

2.2 Minimum Necessary. Business Associate shall not request, Use or Disclose more than the minimum amount of PHI necessary to accomplish the purpose of the Use, Disclosure, or request.

2.3 De-identification of PHI.

(i) Creation and Use of De-identified Data. In the event Business Associate wishes to de-identify PHI, it must first submit its proposed plan for accomplishing the conversion to Covered Entity for Covered Entity's approval, which shall not be unreasonably withheld provided such conversion meets the requirements of HIPAA. Business Associate may use de-identified PHI only as directed or otherwise agreed to by Covered Entity.

(ii) Re-identification Prohibited. Unless otherwise agreed upon by the parties, in the event that Covered Entity provides Business Associate with de-identified PHI, Business Associate shall not be given access to, nor shall Business Associate attempt to develop on its own, any keys or codes that can be used to re-identify the data.

2.4 Safeguarding of PHI.

(iii) Business Associate shall use appropriate safeguards and comply with HIPAA, with respect to the access, Use or Disclosure PHI.

(iv) Business Associate shall review and modify its privacy and security safeguarding measures as needed to continue providing reasonable and appropriate protection of PHI.

(v) Business Associate shall maintain documentation of privacy and security safeguarding measures as required by HIPAA.

(vi) Business Associate shall cooperate in good faith in response to any reasonable requests from Covered Entity to discuss, review, inspect, or audit Business Associate's safeguards.

2.5 Subcontractors. Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate ;

2.6 Access to PHI. At the direction of Covered Entity or an Individual, Business Associate will provide access to any of the Covered Entity’s PHI held by Business Associate. Business Associate will provide or transmit the copy of PHI to a third party if directed in writing to do so by the Individual or Covered Entity.

2.7 Amendment or Correction to PHI. At the direction of Covered Entity, Business Associate agrees to amend or correct the Covered Entity’s PHI held by Business Associate.

2.8 Reporting Non-Permitted Uses and Disclosures of PHI and Breach Notification. Business Associate will report to Covered Entity any use or disclosure of PHI not provided for by this BAA of which it becomes aware, including breaches of unsecured PHI as required by HIPAA, and any security incident of which it becomes aware no later than seventy-two (72) hours from the date the Business Associate discovers the Use or Disclosure. The Business Associate report will identify: (i) the nature of the non-permitted Use or Disclosure, (ii) the PHI Used or Disclosed, (iii) who made the non-permitted Use or received the unauthorized Disclosure and (iv) what corrective action Business Associate has taken or will take to prevent future similar unauthorized Use or Disclosure, and any other information necessary for Covered Entity to satisfy the provisions of HIPAA.

In the event of a Breach of PHI by Business Associate or by the Business Associate’s subcontractor, Business Associate and any subcontractors agree to cooperate with the Covered Entity in the investigation of a Breach. Business Associate and any subcontractors will cooperate with and participate in, to the extent requested by the Covered Entity, the notification of Individuals, the media, and the Secretary. Business Associate is responsible for covering all costs associated with providing the required notices.

2.9. Breach Indemnification. The Business Associate shall indemnify, defend and hold harmless the Covered Entity and its officers, officials, agents and employees from and against all losses, claims, actions, demands, liabilities, damages, costs and expenses (including costs of judgments, settlements, court costs and reasonable attorneys’ fees incurred) arising from or related to: (i) the use or disclosure of PHI by the Business Associate, its subcontractors or agents in violation of the terms of this BAA or applicable law, and (ii) whether in oral, paper or electronic media, any Breach of unsecured PHI by the Business Associate, its subcontractors or agents (collectively, “Claims”). If the Business Associate assumes the defense of a Claim, the Covered Entity shall have the right to participate in the defense. The Business Associate shall not take any final action with respect to any Claim without the prior written consent of the Covered Entity. To the extent permitted by law, the Business Associate shall be fully liable to the Covered Entity for any acts, failures or omissions of its subcontractors and agents as if they were the Business Associate’s own acts, failures or omissions. This section, Breach Indemnification, shall survive the termination or expiration of this BAA.

2.10 Mitigation. Business Associate agrees to mitigate any harmful effect of a Breach, including, if necessary, payment of the cost of credit monitoring to the affected Individual.

2.11 Tracking and Accounting of Disclosures. Upon Covered Entity's request, Business Associate shall provide to Covered Entity an accounting of all Disclosures of PHI by Business Associate or its subcontractors according to HIPAA. At a minimum, within twenty (20) days of receipt of a written request from Covered Entity, Business Associate shall document and make available to Covered Entity or the Individual, any information necessary to provide an accounting of disclosures in accordance with the requirements of the HIPAA. Business Associate shall maintain a process to provide this accounting of disclosures for as long as Business Associate maintains PHI received from or on behalf of Covered Entity. Business Associate shall track the information specified above, and shall securely maintain the information for seven (7) years from the date of the disclosure.

2.12 Audit. For purposes of determining Business Associate's or Covered Entity's compliance with HIPAA, upon request of Covered Entity or the Secretary of Health and Human Services, Business Associate shall: (i) make its HIPAA policies and procedures, related documentation, records maintained, and any other relevant internal practices and books relating to the Use and Disclosure of PHI, available to the Secretary of Health and Human Services or to Covered Entity and (ii) provide reasonable access to Business Associate's facilities, equipment, hardware and software used for the maintenance or processing of PHI. Business Associate shall promptly notify Covered Entity of communications with the Secretary regarding PHI and shall provide Covered Entity with copies of any information Business Associate has made available to the Secretary under this BAA.

2.13 Response to Subpoena. In the event Business Associate receives a subpoena or similar notice or request from any judicial, administrative or other party which would require the production of PHI received from, or created for, Covered Entity, Business Associate shall promptly forward a copy of such subpoena, notice or request to Covered Entity to afford Covered Entity the opportunity to timely respond to the demand for its PHI as Covered Entity determines appropriate according to its state and federal obligations.

2.14 Compliance with Standard Transactions. If Business Associate conducts in whole or part Standard Transactions, for or on behalf of Covered Entity, Business Associate will comply, and will require any subcontractor or agent involved with the conduct of such Standard Transactions to comply, with each applicable requirements of HIPAA. The Business Associate will not enter into, or permit its subcontractors or agents to enter into any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that:

(a) Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;

(b) Adds any data element or segment to the maximum defined data set;

(c) Uses any code or data element that is marked “not used” in the Standard Transaction’s Implementation specification or is not in the Standard Transaction’s implementation specification; or

(d) Changes the meaning or intent of the Standard Transaction’s implementation specification.

2.15 Prohibition on Sale of Electronic Health Records or Protected Health Information. The Business Associate shall not receive remuneration in exchange for any PHI received from or on behalf of the Covered Entity.

2.16 Prohibition on Marketing Communication. The Business Associate will not use PHI received from Covered Entity to contact any individual about any product or services that encourages the recipient of the communication to purchase or use that product or service or which communication is in violation of the marketing prohibition in HIPAA.

2.17. Prohibition on Fundraising Communication. The Covered Entity will not contact any Individual regarding any fundraising activity as prohibited under HIPAA.

3. Covered Entity's Obligations.

3.10 Notice of Privacy Practices. Covered Entity will notify Business Associate of any changes or limitations in its Notice of Privacy Practices, to the extent such limitation may affect Business Associate's Uses or Disclosures. This notice will be provided by posting the Covered Entity’s Notice of Privacy Practices on its website.

3.11 Individual Revocation or Authorization. Covered Entity will notify Business Associate of changes in, or revocation of, authorization by an Individual to Use or Disclose PHI, to the extent such changes affect Business Associate's permitted Uses or Disclosures.

3.12 Restrictions. Covered Entity will notify Business Associate of any restriction in the Use or Disclosure of PHI to which Covered Entity has agreed, to the extent such restriction affects Business Associate's permitted Uses or Disclosures.

4. Term and Termination; Effect of Termination.

4.10 Term.

a. The term of this BAA shall be the same as the term of the Contract to which it is attached (if any), however the term of this BAA shall survive the termination of that Contract and remain in effect until all PHI is returned to Covered Entity or destroyed in accordance with the terms of this BAA or unless terminated under the procedures below.

b. If this BAA is not an attachment to a contract, this BAA will take effect on the date of the final signature of both parties and will remain in effect until all PHI is returned to Covered Entity or destroyed in accordance with the terms of this BAA or unless terminated under the procedures below.

4.11 Termination. If the Covered Entity reasonably determines in good faith that the Business Associate has violated a material term of this BAA, the Covered Entity, in its sole discretion, may do any or all of the following:

a. Require the Business Associate to submit to a plan of monitoring and reporting, as the Covered Entity determines is necessary;

b. Provide the Business Associate with up to thirty (30) days to cure the violation and if the violation is not cured within the time given, terminate this BAA and/or the Contract to which it is attached; and

c. Terminate this BAA and/or the Contract to which it is attached, immediately.

The termination rights in this section 4.11 shall be in addition to any other

rights or remedies provided to the Covered Entity by this BAA, and in

addition to the termination provisions in the Contract to which this BAA is

attached, if any.

4.12 Effect of Termination; Return or Destruction of PHI. Upon termination or expiration of this BAA or the Contract to which it is attached, if any, the Business Associate will, with respect to the PHI covered by this BAA:

a. Return to the Covered Entity or, if return is not feasible, destroy the PHI that the Business Associate maintains in any form;

b. If the Business Associate must retain certain PHI to continue its proper management and administration or to carry out its legal responsibilities, it will continue to use appropriate safeguards and comply with HIPAA for as long as the Business Associate retains any PHI. When the PHI retained is no longer needed, Business Associate will return the PHI to the Covered Entity or, if return is not feasible, destroy the PHI.

c. Destruction means rendering the PHI completely unusable, unreadable, and undecipherable.

d. The Business Associate will return or destroy all PHI as promptly as possible, but not later than thirty (30) days after termination or expiration of this BAA and/or the Contract to which it is attached.

5. Miscellaneous.

5.10 Automatic Amendment. Upon the effective date of any amendment to HIPAA, the Privacy Rule or the Security Rule promulgated by HHS with regard to PHI, this BAA will automatically amend so that the obligations imposed on Business Associate remain in compliance with such regulations.

5.11 Interpretation. Any ambiguity in this BAA shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with HIPAA.

5.12 Conflicts. If any provision of the underlying Contract is directly contradictory to one or more terms of this BAA, such term of the underlying Contract will be superseded by the terms of this BAA only to the extent of the contradiction, as necessary for the parties’ compliance with HIPAA.

Signature Instructions:

If this BAA is attached to a Contract the signatures on the Contract to which this BAA is attached will serve as each party’s signature and agreement to this BAA.

If this BAA is used on its own and NOT an attachment to a signed Contract, this BAA must be signed below by authorized representatives of both parties.

IN WITNESS WHEREOF, each of the undersigned has caused this Business Associate Agreement to be duly executed in its name and on its behalf.

|  |  |
| --- | --- |
| COVERED ENTITY | BUSINESS ASSOCIATE |
| By:        | By:        |
| Title:        | Title:        |
| Date:        | Date:        |