DEPARTMENT OF HUMAN SERVICES
P.O. Box 29 • Baraboo WI 53913
(608) 355-4200 • FAX (608) 355-4299
Jessica Mijal, Director

2021 Revision
12/15/21

Dear Provider:

We would like to thank you for continuing to provide services and programs to support our mission of serving the residents of Sauk County. The Business Associate Agreement (BAA) and Business Associate Checklist are below. Please review these documents carefully. The BAA requires a signature and the checklist should be completed to the best of your ability. If you have questions on either of these documents, please feel free to contact us at the number listed above, ext. 4283.

Security measures related to Telehealth are essential as we continue our commitment around compliance with the Health Insurance Portability and Accountability Act of 1996 and our commitment to keeping our consumers information protected.

Communication between your staff and SCDHS must meet HIPAA standards for secure transmission. If your agency intends to exchange protected information with SCDHS via email, **you are required to ensure that these transmissions are secure** (for example, transmissions using personal Gmail/Yahoo accounts are NOT secure). SCDHS continues to work to establish encrypted gateways with our partner agencies who exchange protected health information when providing care for our consumers.

We will notify our partners if we identify that your electronic transmission is not secure. We will require that your agency meet HIPAA regulations for secure transmission. To assist you in determining what options may be available for your agency, the Management Information System (MIS) Department at Sauk County has offered to assist with suggestions for encryption tools. They can be contacted at 608-355-3555.

Yours truly,

SAUK COUNTY DEPARTMENT OF HUMAN SERVICES

Jessica Mijal
Director

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is made and entered into as of the 1st day of January, 2023 ("Effective date"), by and between Sauk County ("Covered Entity"), and marshall J bales ("Business Associate").

The parties to this Agreement are committed to complying with the Health Insurance Portability and Accountability Act of 1996 and its amendments and the regulations promulgated thereunder (collectively "HIPAA"). In order to ensure such compliance, this Exhibit sets forth the terms and conditions pursuant to which Protected Health Information that is provided to, or created by, the Business Associate from or on behalf of Covered Entity will be handled.

I. Definitions

A. Catch-all definition: The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Electronic Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

B. Specific definitions:

1. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" in 45 CFR 160.103, and in reference to the party to this agreement, shall mean marshall j bales.

2. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean Sauk County.

3. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164 and any amendments thereto, as set forth in section VI of this document.

4. Protected Information. "Protected Information" shall mean any information considered private, confidential, proprietary or sensitive for which access or release is restricted by policy, rule, regulation or law.

5. Telehealth. The remote provision of care utilizing specialized communication technologies.

6. Workforce. "Workforce" shall mean the Employees, volunteers, trainees, students, contractors, and other persons whose conduct, in the performance of work for Business Associate, is under the direct control of the Business Associate, whether or not they are paid by the Business Associate.

II. Obligations and Activities of Business Associate:

Business Associate agrees to:

A. Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

B. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

C. Report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware (see Section IV. IV.below);

D. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information, evidenced by written agreement with subcontractor;

E. Make available protected health information in an Individual's designated record set to the Individual as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524;

F. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526;

G. Maintain and make available the information required to provide an accounting of disclosures to the Covered Entity, a third party or individual as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528;

H. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

I. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

J. Mitigation: to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

K. Tracking and Accounting of Disclosures. So that Covered Entity may meet its accounting obligations under the Privacy Rule, Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. For each Disclosure of PHI that Business Associate makes to Covered Entity or to a third party that is subject to Disclosure under 45 CFR § 164.528, Business Associate will record (i) the Disclosure date, (ii) the name and (if known) address of the person or entity to whom Business Associate made the Disclosure, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of the Disclosure. For repetitive disclosures which Business Associate makes to the same person or entity, including the Covered Entity, for a single purpose, Business Associate may provide (i) the Disclosure information for the first of these repetitive disclosures, (ii) the frequency, duration or number of these repetitive disclosures, and (iii) the date of the last of these repetitive disclosures. Business Associate will make this log of Disclosure information available to the Covered Entity within five (5) business days of the Covered Entity's request. Business Associate must retain the Disclosure information for the six-year period preceding Covered Entity's request for the Disclosure information.

L. 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 Section of the Agreement.

M. 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.

N. Information Security. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity. At a minimum, Business Associate’s safeguards for the protection of Protected Information shall include:

1. limiting access of Protected Information to Authorized Persons;

2. securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;
3. implementing network, device application, database and platform security;
4. securing information transmission, storage and disposal;
5. implementing authentication and access controls within media, applications, operating systems and equipment;
6. encrypting Protected Information stored on any mobile media;
7. encrypting Protected Information transmitted over public or wireless networks;
8. strictly segregating Protected Information from information of Business Associate or its other customers so that Protected Information is not commingled with any other types of information;
9. implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and
10. providing appropriate privacy and information security training to Business Associate's employees.

O. Upon Covered Entity's written request, Business Associate shall provide Covered Entity with a network diagram that outlines Business Associate's information technology network infrastructure and all equipment used in relation to fulfilling of its obligations under this Agreement, including, without limitation:

1. connectivity to Covered Entity and all third parties who may access Business Associate's network to the extent the network contains Personal Information;
2. all network connections including remote access services and wireless connectivity;
3. all access control devices (for example, firewall, packet filters, intrusion detection and access-list routers);
4. all back-up or redundant servers; and
5. permitted access through each network connection.

P. Telehealth. If the Business Associate utilizes telehealth to provide services, such services must meet the same standards for information security set forth in section N. above. In addition, Business Associate must ensure that the provision of these services meets with any applicable HIPAA standards, these include, but are not limited to:

1. Only authorized users shall have access to telehealth records.
2. End to end encryption of telehealth data transmission.
3. Ability to audit telehealth session access and monitor communications to prevent either accidental or malicious disclosures.

4. Business Associate has entered into a Business Associate Agreement with platform provider, or utilizes a platform provided by Sauk County for which Sauk County has a current Business Associate Agreement.
5. Business Associate has obtained required patient consents for telehealth.

Q. Workforce Training. Business Associate shall provide Workforce members with appropriate training to comply with the HIPAA Privacy and Security Rules in accordance with 45 CFR 164.530(b)(1) and 45 CFR 164.308(a)(5) and provide records of such training to the Covered Entity upon request.

III. Permitted Uses and Disclosures by Business Associate

A. Business associate may only use or disclose protected health information as follows:

1. Necessary to perform the services set forth in Service Agreement.

2. Business associate may use or disclose protected health information as required by law.

3. 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, consistent with Covered Entity's minimum necessary policies and procedures.

4. Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity except for the specific uses and disclosures set forth below.

5. Business associate may use protected health information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

6. Business associate may disclose protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

7. Business associate may provide data aggregation services relating to the health care operations of the Covered Entity only with the written consent of the Covered Entity.

B. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

1. Covered entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.

2. Covered entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information.

3. Covered entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

C. Permissible Requests by Covered Entity

Covered entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

IV. Reports of Nonpermitted Uses or Disclosures, Security Incidents or Breaches by the Business Associate.

Reporting required under this section shall be made to the Sauk County Privacy Officer at the following address;

Sauk County Administrative Coordinator
Attn.: Privacy Officer
505 Broadway, Baraboo, WI 53913
Ph: 608-355-3273

A. Reports of Nonpermitted Use or Disclosure: Business Associate agrees to promptly report to Covered Entity any Use or Disclosure of PHI not provided for by this Agreement and cooperate with Covered Entity in its investigation of such event.

B. Reports of Security Incidents. For purposes of this Section, "Security Incident" shall have the same meaning as "Security Incident" in 45 CFR § 164.304.

1. Business Associate agrees to promptly notify Covered Entity of any Security Incident involving PHI of which it becomes aware and cooperate with Covered Entity in the investigation.

2. Business Associate will report attempted but unsuccessful Security Incidents that do not result in any unauthorized access, Use, Disclosure, modification or destruction of PHI, or interference with an information system at Covered Entity's request, at least annually even in the absence of the Covered Entity's request.

C. Reports Related to Potential Breach of Unsecured PHI.

1. Following the discovery of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity of the Breach. Such notification shall be made without unreasonable delay after discovering the Breach, but no later than ten (10) calendar days after its discovery.

2. Business Associate's notice shall include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during or as a result of the Breach. Business Associate shall also provide Covered Entity with at least the following information: a description of the Breach, including the date of Breach and the date of discovery of the Breach, if known; a description of the types of Unsecured PHI involved in the Breach; any steps Individuals should take to protect themselves from potential harm resulting from the Breach; a brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and any other information requested by Covered Entity related to the Breach. Business Associate shall promptly supplement such notice with additional information as it becomes available, even if such information becomes available after Individuals have been notified of the Breach.

3. Business Associate agrees to cooperate with Covered Entity in the investigation of a Breach of Unsecured PHI and to cooperate with and participate in, to the extent requested by Covered Entity, the notification of Individuals, the media, and the Secretary of any Breach of Unsecured PHI.

4. In the event that: (i) a Breach of Unsecured PHI occurs because of the action or inaction of Business Associate, its employees, agents, representatives, or Subcontractors; or (ii) a Breach occurs involving Unsecured PHI in Business Associate's possession, or PHI created, maintained, transmitted, or received by Business Associate or its employees, agents, representatives, or Subcontractors, Business Associate agrees that Covered Entity may, in its sole discretion, require Business Associate to provide such notification as may be required of Covered Entity by 45 CFR §§ 164.404, 164.406, and 164.408. Covered Entity shall have the right to review, direct, and approve or reject the contents or manner of such notification.

V. Term and Termination

A. Term. The Terms of this Agreement shall be effective as of January 1, 2023, and shall remain in effect until all PHI is returned to Covered Entity or destroyed in accordance with the terms of this Agreement.

B. Termination for Cause. Business associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated any term of the Agreement.

C. Obligations of Business Associate Upon Termination.

Upon termination of this Agreement for any reason, Business Associate shall, and shall ensure its Subcontractors that possess PHI or data derived from PHI shall, return to Covered Entity [or, if agreed to by Covered Entity, destroy] all protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form, as promptly as possible but not more than thirty (30) days after notice of termination of this agreement. Business associate, and subcontractor, if applicable, shall retain no copies of the protected health information, and shall certify under oath in writing to Covered Entity that such return has been completed

D. Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

VI. Miscellaneous.

A. 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 Agreement shall automatically amend so that the obligations imposed on Business Associate remain in compliance with such regulations

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

C. Independent Contractor Status. The parties agree that in performing the Services and satisfying the obligations of this Agreement, Business Associate shall at all times be an independent contractor for Covered Entity and nothing in this Agreement shall be construed as creating an agency, employment, joint venture, partnership or other relationship. Covered Entity shall neither have nor exercise any control or direction over Business Associate. Business Associate shall avoid taking any action or making any representation or warranty whatsoever with respect to its relationship with Covered Entity which is inconsistent with its independent contractor status.

D. Conflicts. Any provision of the Underlying Agreement that is directly contradictory to one or more terms of this Agreement ("Contradictory Term") shall be superseded by the terms of this Agreement only to the extent of the contradiction, as necessary for the parties' compliance with HIPAA and to the extent that it is reasonably impossible to comply with both the Contradictory Term and the terms of this Agreement.

E. Integration. This Agreement contains the entire understanding between the parties hereto relating to the subject matter herein and shall supersede any other oral or written agreements, discussions and understandings of every kind and nature, including any provision in any services agreement.

F. Waiver. No delay or failure of either party to exercise any right or remedy available hereunder, at law or in equity, shall act as a waiver of such right or remedy, and any waiver shall not waive any subsequent right, obligation, or default.

This agreement is binding upon the parties on the Effective Date indicated above:

FOR SAUK COUNTY

DocuSigned by:
Brent Miller
0A0B3AC690D7404...

Name: brent.miller@saukcountywi.gov
Title: Administrator
Date: 1/3/2023

FOR THE BUSINESS ASSOCIATE

DocuSigned by:
Marshall Bales MD
155F31C3F31B455...

Name: Marshall Bales MD
Title: md
Date: 3/30/2023

Sauk County's Protected Information is to be destroyed/disposed/Sanitized using a method that ensures the Protected Information cannot be recovered or reconstructed. The following table contains a list of acceptable methods by media type.

Medium	Method Used
Audiotapes	• Recycle (tape over), Degauss or pulverize.
Electronic Data/ Hard Disk Drives including drives found in servers, workstations, printers, and copiers	• Destroy data permanently and irreversibly through a DoD wipe, physical destruction (pulverize, shred, disintegrate, incinerate), Degaussing of it, or hard drive erasure software. • Methods of reuse: overwrite data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten.
Electronic Data/ Removable Media or devices including USB drives, SD cards, CDs, tapes, and cartridges	• Overwrite data with a series of characters or reformat it (destroying everything on it). Total data destruction does not occur until the data has been overwritten. • Magnetic Degaussing that leaves the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Magnetic Degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. • Shredding or pulverization is done for the final disposition of any removable Media when it is no longer usable.
Handheld devices including cell phones, smart phones, PDAs, tablets and similar devices.	• Activate the Software on these devices that remotely wipes ("bit-wipe") data from them. • When a handheld device is no longer reusable it is then bit-wiped and totally destroyed by recycling or by trash compacting
Optical Media	• Optical disks cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Microfilm/ Microfiche and X-rays	• Recycle through a contracted BA or pulverize.
PHI Labeled Devices, Containers, Equipment, Etc.	• Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Remove labels or incineration of the medium; or • Obliterate the information (make it unreadable) with a heavy permanent marker pen. • Ribbons used to print labels may contain PHI and are shredded or incinerated.
Paper Records	• Paper records are destroyed/disposed of in a manner that leaves no possibility for reconstruction of the information. Appropriate methods for destroying/disposing of paper records include:

Medium	Method Used
	burning, shredding, pulping, and pulverizing. If shredded, use cross cut shredders which produce particles that are 1 x 5 millimeters or smaller in size.
Videotapes	• Recycle (tape over) or pulverize.

Business Associate Compliance Questionnaire

Business Associate Information:

BA Name:	marshall J bales md		Date Completed:	2-15-23
BA Address:	2045 hickory ln			
BA Phone:	920-573-5073			
Number of employees:	1		Person Completing Questionnaire (name, title):	dr bales

Privacy Officer Name, Contact:	dr bales	
Security Officer Name, Contact:	dr bales at above address	

Compliance Questions:

1 When was the last time you updated your documented privacy and information security policies and procedures?

☐ Within the last 6 months

☒ Less than a year ago

☐ 1 to 2 years ago

☐ More than 2 years ago

☐ Never

Additional Information:

na

2 Describe how the privacy and information security policies and procedures are communicated to all personnel, and made available for them to review at any time. Check all that apply.

☐ By email

☐ By company intranet / internet

☒ Hard copy

☐ Management policy binders

☐ Via Compliance system / portal

☐ Other – Explain:

na

3 Do you provide annual training and ongoing awareness communications for information security and privacy for all your workers?

☐ Yes

☒ No

a. If No, What is your regular training interval? q yearly
b. What is the date of most recent training? 1-1-23

4 Do you conduct annual security risk assessments?

☒ Yes

☐ No

a. Date of most recent assessment: 1-1-23

5 Do you require all types of sensitive information, including personal information and health information, to be encrypted when it is sent through public networks and when it is stored on mobile computers and mobile storage devices?

☐ Yes

☐ No

6 Do you have retention policies for sensitive information?

☒ Yes

☐ No

7 Do you require sensitive information, in all forms, to be disposed of using secure methods?

☐ Yes

☐ No

a. Do you maintain records of such disposals?

☐ Yes

☐ No

8 Do you regularly make backups of business information, and have documented disaster recovery and business continuity plans?

☐ Yes

☐ No

9 How quickly are new employees trained on your privacy and security policies?

☒ Within one week

☐ within 30 days

☐ within 60 days

☐ after more than 60 days

☐ Never

☐ Other – Explain:

na

10 Do you have a formal Breach Notification process?

☐ Yes

☐ No

11 Do you have an internal team to support the Breach Notification process?

☐ Yes

☐ No

12 Do you have a documented procedure for the reporting of privacy and security incidents and breaches?

☐ Yes

☐ No

13 Do you outsource any activities involving Sauk County's protected data?

☐ Yes

☒ No

a. If "Yes" Explain:
no
_____
_____

b. If you answered yes to #13, do you have a Business Associate Agreement with each subcontractor used?

☐ Yes

☐ No

14 Check all the following standards for which you can verify compliance:

☒ HIPAA Privacy/

☐ HIPAA HITECH

☐ Other (Please Specify): na

☐ None

15 Please include any other information you consider relevant to your proof of privacy and security compliance:

none