HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY AND SECURITY

BARABOO SCHOOL BOARD POLICY

526.1

The School District of Baraboo (“District”) is committed to compliance with the health information privacy and security requirements set forth by federal law and the regulations of the U.S. Department of Health and Human Services. These requirements dictate that the privacy of protected health information received by or generated through certain District employee health plans be protected from improper use or disclosure. Protected health information is all personally identifiable health information, including information in writing, electronic medium, and oral communications. The information security rule applies to personally identifiable health information that is in electronic form. The District offers its eligible employees a Flexible Health Care Spending Account Plan (Plan #1) and a Dean Care Medical Health Plan (Plan #2) that includes reimbursement of related deductible expenses through a Health Reimbursement Account (“HRA”) Plan (Plan #3), where each of the Plans are health plans that must comply with the Privacy and Security Rules pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the District HIPAA policy. For purposes of this policy, the District is the “Plan Sponsor” of these plans.

District as Plan Sponsor

For purposes of compliance with HIPAA, the District is the Plan Sponsor for each of the Plans, and each Plan is considered to be a separate legal entity from the District. Certain District employees may perform administrative functions related to the Plans, and the District may receive disclosures of information from the Plans consistent with its role as the Plan Sponsor. In these roles, the District and those District employees who are involved in the District’s activities as a Plan Sponsor are subject to the HIPAA Privacy and Security Rules. Each Plan is also subject to those rules. However, the District is not primarily engaged in the business of providing health care, and the District’s other operations and functions that are not related to the District’s role as a Plan Sponsor are not covered by the HIPAA Privacy and Security Rules.

Purpose of HIPAA

HIPAA legislation was passed to help govern the portability of health care coverage, especially in the area of preexisting conditions, and to create a more consistent health care delivery system. It provides for the standardized exchange of health information to make it easier for employees to change jobs without disrupting their health care. However, in order to ensure the privacy and security of employee health information, employers must comply with the HIPAA Privacy and Security Rules.
Enrollment and Disenrollment Information

Enrollment and disenrollment information held by the Plan is considered protected health information. However, enrollment and disenrollment information held by The District in its role as an employer is not considered protected health information.

Privacy and Security Official

The Human Resources Specialist or his/her designee, is designated as the Privacy and Security Official, whose responsibilities will include development and implementation of these policies and related procedures, including ensuring internal compliance with the Privacy and Security Rules governing participating employees’ (“Plan members”) protected health information and receiving complaints.

Limited Access to Protected Health Information

The Plans are primarily administered by third-party administrators (“TPAs”) or health insurance companies. The TPAs and insurer (for the Dean Plan) are responsible for nearly all Plan administrative functions involving individually identifiable health information. District employees who are involved in plan administration perform only limited functions involving health information. The District therefore relies primarily on the Plans’ TPAs and insurer (and their respective HIPAA privacy and security policies and procedures) for purposes of the Plans’ compliance with the HIPAA Privacy and Security Rules. To that end, the District has entered into and maintains HIPAA-compliant business associate agreements with the TPAs, which require the TPAs to comply with the applicable HIPAA Privacy and Security Rules. In addition, the insurer is directly subject to the HIPAA Privacy and Security Rules as a HIPAA covered entity.

The District, as the Plan Sponsor, and District employees who are involved in plan administration, create and receive health information only in limited circumstances. In those circumstances, the information involved will be limited to the minimum necessary for the function being performed (or the scope of an individual’s written authorization, if applicable). Health information may be used and disclosed to the District only in a manner consistent with the HIPAA Privacy and Security Rules and these HIPAA Privacy and Security Policies. In general, access to health information by the District and its employees who perform plan administrative functions will be limited to the following types of circumstances:

- Performance of enrollment and disenrollment functions.
- Use of summary health information (with individual identifiers removed) for purposes of modifying, amending, or terminating a Plan.
- Receipt of de-identified information.
- When authorized by a signed authorization that meets the requirements of HIPAA.

Administrative Privacy and Security Safeguards

The Plans will implement reasonable and appropriate privacy and security safeguards to
protect the confidentiality, integrity, and availability of protected health information, including electronic protected health information, whether it is being stored or transmitted. The Plans shall implement and maintain these policies and related procedures to manage the selection, development, implementation, and maintenance of security measures to protect health information and manage the conduct of the District employees in relation to the protection of the protected health information as follows:

1. **Authorization:** Only District employees designated by the Privacy and Security Official as requiring access to Plan information will be given such access. Access to protected health information will be limited to the TPAs and insurer for purposes of performing duties related to the payment, treatment, or health care operations of the Plan. The role of District employees in handling Plan information will be limited to the use and disclosure of enrollment and disenrollment and summary information in a manner consistent with HIPAA requirements. Protected health information shall not be disclosed to the District or its employees unless done pursuant to a HIPAA-compliant individual authorization or as otherwise permitted by HIPAA.

2. **Training:** District employees, including management, authorized to obtain access to Plan information will receive training, including security awareness at a minimum by providing them with a copy of the privacy policy and notice and documenting that they have reviewed the policies on an annual basis.

3. **Response and Reporting:** Suspected or known security incidents, breaches, or instances of unauthorized use or disclosure of protected health information must be reported immediately to the Privacy Official. The Plans will implement reasonable and appropriate measures to identify, respond to, and document in writing any identified security incidents, breaches, or unauthorized uses or disclosures of protected health information. The harmful effects of such instances will be mitigated to the extent practicable and known to the Plans, and the Plans will take reasonable and appropriate steps to prevent the reoccurrence similar instances. When required, the Plans will comply with the notice requirements of the HIPAA Breach Notification Rule to provide notice of breaches to affected individuals, the Department of Health and Human Services, and (if appropriate) the media.

4. **Physical Safeguards:** The Plans will implement reasonable and appropriate physical safeguards as required under the HIPAA Privacy and Security Rules. Plan information in the District’s control will be stored in a secure manner, such as by being secured in a locked file cabinet used solely for the purpose of storing such information (for paper documents) or encrypted (for electronic information). The District will dispose of Plan information in a secure manner, such as by shredding for paper documents and the use of appropriate deletion techniques for electronic information. Work stations used to access Plan information will be protected to prevent unauthorized access through automatic logoff procedures or other appropriate mechanisms. Any facsimile machines used to transmit and receive Plan information shall be in a secure location.
5. **Technical Safeguards:** To the extent Plan information is maintained electronically, access to electronic information systems or software programs will be provided to only those persons who have been granted access rights. Procedures for controlling and tracking the handling of hardware and software, and for data backup, storage, and disposal shall be implemented. This includes the receipt, handling, and disposal of Plan information. The District will implement additional security measures, including encryption, appropriate for the type of Plan information used, maintained, or accessed by District employees or with District equipment or systems. The District shall have a contingency plan to maintain the continuity of operations in an emergency or disaster, and to enable recovery of data following disaster. An annual internal audit of data security will be conducted, including the execution of security measures to protect data, review of personnel compliance with the policy and procedures, and data authentication.

6. **Sanctions:** The District will impose appropriate sanctions for District employees who use or disclose protected health information in violation of the HIPAA Privacy or Security Rules or these HIPAA Privacy and Security Policies in accordance with District’s discipline policies, up to and including termination of employment. The Privacy Official is responsible for implementing each Plan’s sanctions program. Issues of non-compliance may be resolved by reporting such non-compliance to the District Administrator for appropriate action.

### Authorizing Use and Disclosure of Protected Health Information

Written authorization will be required to use a Plan member’s protected health information or to disclose it to anyone for any purpose except as noted in “Uses and Disclosure of Protected Health Information.” If the Plan member provides written authorization, the Plan member may revoke it at any time.

The Plan member may appoint a representative to act on his/her behalf. Information will only be disclosed to the formally appointed representative designated by the Plan member. A written designation of such must be provided to the Privacy Official.

### Uses and Disclosure of Protected Health Information

The Plans may use and disclose protected health information only as permitted by the HIPAA Privacy and Security Rules. In general, those rules permit or require the Plans to use or disclose protected health information without a Plan member’s written authorization in the following circumstances:

1. **For Treatment:** Treatment includes providing, coordinating, or managing health care by one (1) or more health care providers or doctors.

2. **For Payment:** Payment includes activities by a Plan, other plans, or providers to obtain premiums, make coverage determinations and provide reimbursement for health care.
3. **For Health Care Operations:** Health care operations include activities by a Plan (and in limited circumstances other plans or providers) such as wellness and risk assessment programs, quality assessment and improvement activities, customer service, and internal grievance resolution.

4. **As Required by Law:** The Plans may use or disclose the Plan member’s protected health information when required to do so by law, including disclosures to worker’s compensation and specialized government or military functions and investigations.

5. **Disclosure to Plan Sponsor:** The Plans may disclose protected health information to the Plan Sponsor. The Plan Sponsor may only use the information to perform appropriate plan administration functions as they relate to the Plan member and may not use the information for employment-related purposes.

6. **Disclosure to Family and Friends:** If a Plan member is unable to communicate in an emergency or disaster relief situation, a Plan may disclose the Plan member’s protected health information to a family member or friend to the extent necessary to facilitate the reimbursement of the Plan member’s health care.

7. **For Public Health and Safety:** A Plan may disclose a Plan member’s protected health information to the extent necessary to prevent a serious threat to the Plan member’s health or the health and safety of others.

**Plan Member's Rights and Obligations**

Plan members have the following rights regarding protected health information as described in more detail in the Privacy and Security Notice:

1. The right to request restrictions on certain uses and disclosures of protected health information. The Plan is not required to agree to a requested restriction, however.

2. The right to receive confidential communications of protected health information and to request to receive communications by alternative means or at alternative locations. The Plans will accommodate reasonable requests and are required to accommodate reasonable requests if a Plan member clearly states that disclosure of all or part of the information could endanger the individual.

3. The right to inspect and copy protected health information. Such a request must be done in writing. Within thirty (30) business days of a written request by a Plan member for access to his/her protected health information, the Plan will make such information available to the Plan member or his/her representative for so long as such information is maintained by the Plan. The Plan shall inform the Plan member of the acceptance of the request and provide access to the Plan member for inspection or copying of the protected health information at an agreeable time and location, or mail the copy of the information at the Plan member’s request. The Plan may impose a reasonable, cost-based fee on the Plan member.
4. The right to amend protected health information that is inaccurate or incomplete. The Plan shall act on a Plan member’s request for an amendment no later than 60 days after receipt of such a request. If the Plan accepts the requested amendment, it shall make such amendment, inform the Plan member that the amendment is accepted, and obtain information and agreement from the Plan member to notify the relevant persons with whom the amendment needs to be shared. If the Plan denies the request to amend protected health information, in whole or in part, it shall provide the Plan member with a timely, written denial. The denial shall include the basis for the denial, a statement of the Plan member’s right to submit a written statement disagreeing with the denial and how to file such a statement; a statement that if the Plan member does not submit a statement of disagreement, the Plan member may request that the Plan provide the Plan member’s request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and a description of how the Plan member may complain to the Plan or the Secretary of the U.S. Department of Health and Human Services.

5. The right to receive an accounting of disclosures of protected health information for up to six (6) years prior to the date on which the accounting is requested. No later than sixty (60) days after receipt of a written request, the Plan shall provide the Plan member with an accounting of the disclosures of protected health information as required by law. The Plan will provide the following information: (a) the date of the disclosure; (b) the name of the entity or person who received the protected health information, and if known, the address of such entity or person; (c) a brief description of the protected health information disclosed; and (d) a brief statement of the purpose of such disclosure that includes an explanation of the basis for such disclosure. Disclosures made to the Plan member, or for the purpose of carrying out treatment, payment, or health care operations, or pursuant to an authorization, or incident to a use or disclosure otherwise permitted, will not be included in such accounting.

6. The right to obtain a paper copy of the “Notice of HIPAA Privacy and Security Practices” upon request.

**Plan Obligations**

1. Each Plan is required by law to maintain the privacy and security of protected health information and to provide Plan members with notice of the Plan’s legal duties, privacy and security practices with respect to protected health information, and, no less frequently than once every three years, notify Plan members of the notice and how to obtain a copy of the notice.

2. Each Plan is required to abide by the terms of this policy and the “Notice of Privacy and Security Practices.”

3. The Plans reserve the right to change the terms of this Policy and the “Notice of Privacy and Security Practices.” The new provisions will be effective for all
protected health information that the Plans maintain.

4. The Plans will provide Plan members with revised copies of their “Notice of Privacy and Security Practices” when required.

5. The Plans will ensure that any agents, including subcontractors to whom the Plans provide protected health information, agree to the same restrictions and conditions that apply to the Plan with respect to protected health information.

Security Rule

It is the policy of the District, as Plan Sponsor, and the Plans, working together with the Plans’ TPAs and insurer to:

- Ensure the confidentiality, integrity, and availability of the Plans’ electronic protected health information.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of the Plans’ electronic protected health information.
- Protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted by the HIPAA Privacy and Security Rules.
- Ensure workforce compliance with the Security Rule these Policies.

Reliance on Security Policies and Procedures of the TPAs and Insurer

Because of the limited involvement of the District and its employees in plan administrative functions that involve protected health information, the Plans rely primarily on the TPAs and insurer for compliance with the Security Rule (see “Limited Access to Protected Health Information” above).

Additional Security Measures

In addition to relying on the TPAs and insurer, the District and its employees involved in plan administration will do the following to protect the security of the Plans’ electronic protected health information:

- Ensure that the Plans execute and maintain HIPAA-compliant business associate agreements with Plans’ business associates.
- Reasonably and appropriately safeguard electronic Plan information created, received, maintained, or transmitted on behalf of the Plans.
- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Plan information that the District and its employees create, receive, maintain, or transmit on behalf of the Plans.
- Ensure that any agent to whom the District provides electronic protected health information agrees to implement reasonable and appropriate security measures to protect the information.
• Report to the appropriate Plan any “security incident” of which the District becomes aware (“security incident” is defined by the HIPAA Security Rule to include attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system).

Risk Analysis

Consistent with the requirements of the Security Rule, the District has conducted the following risk analysis for the Plans to make an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the Plans’ electronic protected health information:

• The Plans themselves have no employees. The primary plan administrative functions involving protected health information are performed by the TPAs and insurer, which control their own employees, agents, and subcontractors who have access to electronic protected health information. Certain authorized the District employees are also involved in plan administration to a limited degree, as described in these HIPAA Privacy and Security Policies. However, these District employees are not involved in Plan functions that require the use and disclosure of protected health information.

• The Plans themselves do not own or control the primary equipment and media used to create, maintain, receive, and transmit the Plans’ electronic protected health information or the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the TPAs and insurer. Because the District and its employees are not involved in Plan functions that require the use and disclosure of protected health information, any equipment, media, or facilities owned or controlled by the District that are used to perform Plan administrative functions do not contain protected health information.

• In regard to the TPAs’ and insurer’s functions involving electronic protected health information, the Plan has no ability to directly assess or modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information relating to the Plans, as that ability lies with the TPAs and insurer. The TPAs are, however, “business associates” under the HIPAA Privacy and Security Rules and, as such, are required by those rules to implement appropriate security measures with respect to the Plans’ electronic protected health information. The TPAs are also contractually obligated to implement appropriate security measures under the terms of their business associate agreements with the Plans.

• In regard to the Dean Care Medical Health Plan (Plan #2), the Plan provides benefits solely through a fully insured contract with the Plan’s insurer, Dean, and the District does not receive any individually identifiable health information from Dean other than summary health information and enrollment/disenrollment information. As such, the District has determined that the Dean Plan is a “hands-off” fully insured plan not subject to certain HIPAA administrative requirements, including the designation of a privacy
official and contact person, training, safeguards, complaint procedures, sanctions, duty to mitigate, and policies and procedures. Nevertheless, the District intends for the Dean Plan to also comply with these HIPAA Privacy and Security Policies. As described elsewhere in these Policies, the District relies primarily on the insurer for compliance with the Dean Plan’s HIPAA privacy and security obligations based on the insurer being directly subject to the HIPAA Privacy and Security Rules as they relate to the Plan.

In sum, because the District and the Plans have no direct access to or control over the TPAs’ or insurer’s employees, equipment, media, facilities, policies, procedures, and documentation affecting the security of electronic protected health information, and the TPAs and insurer are both legally and contractually obligated to comply with the Security Rule in regard to the Plans’ electronic protected health information, to the extent the TPAs and insurer are responsible for Plan administrative functions involving protected health information, the Plans adopt their security policies and procedures for purposes of Security Rule compliance.

**Risk Management**

The Plans manage risk to electronic protected health information by limiting vulnerabilities, based on the Plans’ risk analysis, to a reasonable and appropriate level, taking into account the following:

- The size, complexity, and capabilities of the Plans;
- The Plans’ technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and
- The criticality of the electronic protected health information potentially affected.

As addressed in the risk analysis above, the District has made a reasoned, well-informed, and good-faith determination in regard to the implementation of the Security Rule that:

- For the electronic protected health information created, received, maintained, or transmitted by the TPAs and insurer, the Plans may reasonably rely on the TPAs and insurer for purposes of compliance with the Security Rule.
- The District and its employees do not use or disclose electronic protected health information for purposes of plan administration, and, to the extent the District creates, receives, maintains, or transmits any Plan information, the District has taken reasonable and appropriate steps to protect the security of that information.

**Complaints**

Plan members who feel that their rights under the HIPAA Privacy and Security Rules have been violated or who have other concerns with the Plans’ or the District’s compliance with the HIPAA Privacy and Security Rules may submit written complaints to the Privacy and Security Official. The Privacy and Security Official is responsible for taking prompt and appropriate action to respond to and address any complaints. Plan members may also submit complaints to the Secretary of the U.S. Department of Health and Human Services (HHS).
No Intimidating or Retaliatory Acts

The District strictly prohibits any retaliation against a Plan member who exercises their rights under the HIPAA Privacy and Security Rules, including:

- Seeking to exercise rights related to the Plan member’s protected health information (e.g., access, amendment, accounting of disclosures, or confidential communications).
- Making a good faith complaint regarding a Plan’s or the District’s compliance with the HIPAA Privacy and Security Rules.
- Opposing any act or practice that is illegal under HIPAA, if the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA Privacy and Security Rules.
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the HIPAA Privacy and Security Rules.

In addition, the Plans will not require a Plan member to waive their rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility for benefits.

Plan members who feel that they may have been subject to retaliation or wrongful treatment in violation of this policy should contact the Privacy and Security Official.

LEGAL REF.: 42 U.S.C. ss. 1320d-1329d
45 C.F.R. Parts 160 and 164

CROSS REF.: 526.1-Exhibit, Notice of HIPAA Privacy and Security Practices

ADOPTED: April 13, 2009

REVISED: August 26, 2013
September 28, 2015
February 11, 2019