HIPAA INTERNAL PRIVACY AND SECURITY PROCEDURES
STEVENS POINT AREA PUBLIC SCHOOL DISTRICT

Introduction

These procedures were developed to define how the Stevens Point Area Public School District (SPAPSD) will comply with the HIPAA Privacy and Security Rules. SPAPSD sponsors the Stevens Point Area School District Group Dental Plan and the Stevens Point Area Public School District Flexible Benefit Plan ("the Plan"). Employees may have access to the individually-identifiable health information of Plan Participants, on behalf of the Plan themselves, on behalf of the employer, or for administrative functions related to the Plan. (For the purposes of HIPAA compliance, "employees" are defined as those who are listed on Attachment A as internal personnel with access to the listed protected health information.)

Protected health information (PHI) included under the Act is defined as follows:

> Protected health information means information that is created or received by the Plan and (a) relates to the past, present, or future physical or mental health or condition of a participant; (b) relates to the provision of health care to a participant; (c) relates to the past, present or future payment for the provision of health care to a participant; or (d) identifies the participant and suggests a reasonable likelihood that the information might be used to identify the participant. Protected health information includes information of persons living and those deceased within the last 50 years.

Employees with access to PHI must comply with these procedures. The District reserves the right to amend or change the procedures at any time without notice. To the extent that these procedures establish requirements and obligations above and beyond those required by HIPAA, the procedure shall not be binding upon the District. These procedures do not address requirements under other federal or state laws.

Internal Policies for HIPAA Compliance

I. Designation of Privacy Officer and Security Officer

The Director of Human Resources is the designated Privacy Officer for the Plan. The Privacy Officer may be contacted via email at bbakunow@pointschools.net or in person at 1900 Polk Street, Stevens Point, WI. The Privacy Officer is responsible for ensuring that the Plan complies with the provisions of the HIPAA privacy rule, including those provisions regarding business associates, and this Privacy Policy. The Director of Human Resources is the designated Security Officer. The Security Officer may be contacted via mail at bbakunow@pointschools.net or in person at 1900 Polk Street, Stevens Point, WI. The Security Officer is responsible for ensuring the Plan protects the confidentiality of electronic protected health information.

II. Enforcement of Privacy and Security Policy

All privacy violations relating to the administration of the Plan are to be reported to the Privacy Officer per the guidelines outlined earlier in this document. Any employee or group of employees who are looked upon, as a "whistleblower" shall not be retaliated against and their claims shall be investigated to the fullest measure necessary. Each reported violation will be investigated.

A document of each complaint and the outcome of each complaint shall be kept on file for six years after the date of the resolution of the complaint.

III. Notice of Privacy Practices

The Privacy Officer will create and maintain on behalf of the Plan a Notice of Privacy Practices describing permitted uses and disclosures of PHI, individual participant rights, and the Plan's legal duties regarding PHI.

The Plan will distribute this notice to participants:

- At the time of an individual's enrollment in the Plan
- Within 60 days after a material change to the notice,
- Upon request, and

The Plan will also provide a notice of the availability of the Notice of Privacy Practices at least every three years.

IV. Technical and Physical Safeguards and Firewall

The Plan Sponsor will establish appropriate technical and physical safeguards to prevent unauthorized uses or disclosures of PHI. Examples of technical safeguards include password protection on computers and restricted logins; examples of physical safeguards include locking doors or filing cabinets.

The Plan Sponsor will also set up "firewalls" to ensure that access to PHI is limited only to the employees who are authorized to access PHI, and only to the extent that such access is necessary to carry out plan administrative functions.

A full listing of the Plan Sponsor's Technical and Physical Safeguards and a description of the firewalls set up by the Plan Sponsor are included as **Attachment B**.

V. Employee Training

All employees with access to PHI are listed in **Attachment A**. Only those employees listed will have access to PHI, and such access shall be limited to the minimum necessary to perform administration functions on behalf of the Plan. Any employee included on that list will be trained on this policy to the degree necessary based on their interaction with PHI. Such training will include:

- Basics of HIPAA Privacy
    - Definitions
    - Permitted uses and disclosures by the Plan
    - Reporting violations of HIPAA Privacy
    - Sanctions for violating HIPAA Privacy
- Examples of PHI that each area views, uses or discloses
- Effect of the HIPAA Privacy Act on particular job duties

All other employees will receive training and be made aware of general privacy and security policies and procedures related to the protection of individually identifiable information. A copy of each training document and a signed acknowledgement of each employee who receives training shall be kept on file permanently.

VI. Breach of PHI & Notification

Any Plan Employee who believes they have observed a breach of confidentiality must report the incident to the Privacy Officer. The Privacy Officer shall conduct an investigation into the existence of a breach of PHI. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity demonstrates that there is a low probability that the protected health information has been compromised. All reported breaches and the subsequent investigation and risk assessment must be documented and kept on file for six years.

Unless a legal exception applies, the Plan will, via first-class mail, notify any affected individual of a breach, where it cannot be shown that there is a low probability that the PHI has been compromised and no later than 60 days after discovery and investigation of the breach. If a breach affects 500 or more individuals, the Plan will also notify the Department of Health and Human Services (HHS), and follow regulations on media notice when applicable. In any case, the Plan will submit an annual log of breaches to HHS within 60 calendar days after the end of the calendar year.

See Breach Notification Policy for more specific requirements on responding to a breach.

SPAPSD will periodically conduct unscheduled audits to ensure compliance with this section.

VII. Documentation and Retention

The HIPAA Privacy related documentation, which includes but is not limited to:

- Policies and procedures
- Training materials and acknowledgements
- Complaints and resolutions
- Authorization requests
- Business Associate Agreements
- Accounting of Disclosures of PHI
- Record of Breaches of PHI and Breach Notification Efforts

Shall be kept by the Privacy Officer in a locked filing cabinet for a minimum of six years once the document has ceased being used or has had a material change, which precipitated the need for a new, updated document.

VIII. Complaints

Any individual who is the subject of PHI may file a written complaint regarding the use, disclosure or handling of their PHI by the Plan. This complaint must be filed within 90 days of the occurrence and turned into the Privacy Officer. The complaint form must be signed, dated and include a description of what the complaint is in regard to.

The Privacy Officer will respond to the complainant in writing as to the outcome of the complaint within 45 days.

The Plan also has the right to refer the individual to the Third Party Administrator if they are the more appropriate party to handle the complaint.

Each complainant has the right to appeal the final outcome of the complaint. The appeal must

be in writing and sent to the Privacy Officer within 30 days of receiving the outcome of the original complaint.

The complainant also has the right to file a complaint with the Secretary of Health and Human Services.

IX. Sanction Process

Any employee that is found to violate the provisions listed in the HIPAA Privacy Rule or this Policy shall be subject to the standard sanction process of SPAPSD, up to and including dismissal. Sanctions issued for a violation of HIPAA Privacy shall be documented on a standard form and a copy shall be kept in the employee's file indefinitely.

X. Mitigation of Inadvertent Disclosures of PHI

SPAPSD will mitigate, to the extent possible, any harmful effects that become known of disclosing an individual's PHI in violation of the policies and procedures set forth. The Privacy Officer must be contacted immediately of any incorrect use or disclosure of PHI.

XI. Non-Retaliation

The Plan will not retaliate against any individual for filing a complaint or reporting unauthorized uses or disclosures of PHI.

XII. Plan Document Provisions and Certifications

The Plan document will include provisions describing permitted uses and disclosures of PHI for administrative purposes. The Plan document will also require that SPAPSD certify to the Plan that the documents have been amended consistent with HIPAA privacy, that SPAPSD agrees to the provisions, and that SPAPSD will provide adequate firewalls consistent with HIPAA Privacy.

Procedures for Use and Disclosure of PHI

I. How Use and Disclosure are Defined

The District and the Plan will use and disclose PHI only as permitted under HIPAA. Use means the sharing, employment, application, utilization, examination, or analysis of individually-identifiable health information by any person working for or with the employer's Benefits, Payroll, or Information Management Department or by a Business Associate of the Plan.

Disclosures of information that is PHI means any release, transfer, provision or access to, or divulging in any other manner any individually-identifiable health information to persons not employed by or working within the employer's Benefits, Payroll, or Information Management Department or a Business Associate.

Employees with access to PHI, as identified in **Attachment A**, may use and disclose PHI for Plan administrative functions, and may disclose PHI to other employees with access to this information for Plan administrative functions in accordance with these procedures only.

II. Payment and Health Care Operations

The Plan may disclose PHI for its own payment purposes, or to another covered entity for the payment purposes of that covered entity. The Plan may also disclose PHI for its own health care operations, and the health care operations of another covered entity if that entity has a relationship with the individual who is the subject of the PHI and the PHI pertains to that relationship.

Payment includes activities undertaken to obtain Plan contributions, to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations, including coordination of benefits and adjudication or subrogation of health benefit claims,
- risk adjusting based on enrollee status and demographic characteristics, and
- billing, claim management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing.

Health care operations means activities directly related to the provision of health care or the processing of health information, including but not limited to any of the following activities to the extent that they are related to Plan administration:

- conducting quality assessment and improvement activities,
- reviewing health plan performance,
- underwriting and premium rating,
- conducting or arranging for medical review, legal services, and auditing functions,
- business planning and development, and
- business management and general administrative activities.

Procedure

An employee may use and disclose a Plan Participant's PHI

- to facilitate the Plan's own payment activities or health care operations,
- to another covered entity or health care provider so as to perform the other entity's payment activities, and
- for purposes of the other covered entity's quality assessment and improvement, for

case management or health care fraud and abuse detection programs, and/or if the other covered entity has a relationship with the individual and the PHI requested pertains to that relationship.

All disclosures must be approved by the Privacy Officer, must comply with the minimum necessary standard, and must be documented on the Accounting of PHI Disclosures form.

Unless an authorization from the individual has been received, an employee may not use a Participant's PHI for the payment or operation of the District's non-health benefits (e.g. disability or life insurance). If an employee requires Participant's PHI for payment or health care operations on non-plan benefits, follow these steps:

- Obtain an authorization.
- Have the disclosure approved by the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard.
- Document the disclosure on the Accounting of PHI Disclosures form.

III. PHI Disclosures to Individuals & Department of Health and Human Services

Procedure

An individual may request a copy of their own PHI. The employee must follow the "Procedure for Complying with Individual Rights" (p. 10). If there is a request from the Department of Health and Human Services, the employee must follow the procedure set forth in "Verification of Identity of Those Requesting Protected Health Information" (Section IX). The disclosure must be approved by the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard. All disclosures must be documented on the Accounting of PHI Disclosures form.

IV. Legal Disclosures of PHI

Procedure

Disclosures about victims of abuse, neglect, or domestic violence can be met only if (a) the individual agrees with the disclosure; (b) if the disclosure is expressly authorized by statute or regulation (and the disclosure prevents harm to the individual); or (c) the individual is incapacitated and unable to consent, the information will not be used against the individual, and the information is necessary for an imminent enforcement activity.

Disclosures for judicial and administrative proceedings are covered if they are in response to an order of a court or administrative tribunal, or are a subpoena, discovery request, or other lawful process not accompanied by a court order or administrative tribunal. The individual must first have been given notice of the request, or the party seeking the information must have made reasonable efforts to receive a qualified protective order.

Disclosures to a law enforcement Officer for law enforcement purposes are permitted under the following conditions:

- Pursuant to a process and as otherwise required by law, but only if the information sought is relevant, the request is specific and limited to reasonable amounts, and it is not possible to use de-identified information.
- Information requested is limited information used to identify or locate a suspect, fugitive, material witness, or missing person.
- Information is about a suspected victim of a crime if the individual consents to the disclosure, or without the individual's agreement, if the information is not to be used against the victim, if the need for the information is urgent, and if disclosure is in the individual's best interest.
- Information is about a deceased individual arising upon suspicion that the individual's death resulted from criminal conduct.
- Information sought constitutes evidence of criminal conduct that occurred on the District's premises.

Disclosures are allowed to the appropriate public health authorities, to a health oversight agency, to a coroner or medical examiner about decedents, for cadaveric organ, eye or tissue donation purposes, and for certain limited research purposes. Disclosures also may be made to avert a serious threat to health or safety, for specialized government functions, and for worker's compensation programs.

Legal disclosures must be approved by the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard. All disclosures must be documented on the Account of PHI Disclosures form.

V. Disclosures Pursuant to an Authorization

Procedure

Any requested disclosure to a third party (not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required (under the Use and Disclosure Procedures) may be made pursuant to an individual's authorization. When there is a disclosure via an authorization, the following procedures apply:

Verify the individual's identity. Determine that the authorization is valid. It should (1) be signed properly and dated, and must not be expired; (2) include a description of the information to be used or disclosed, along with the name of the entity or person authorized to use or disclose the PHI; (3) include the name of the recipient; (4) include a statement regarding the individual's right to revoke the authorization and the procedure for such, along with a statement regarding the possibility for any subsequent re-disclosure of the information.

A use or disclosure made pursuant to an authorization must be consistent with the terms of the

authorization itself. The disclosure must be approved by the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard. The disclosure must be documented on the Accounting of PHI Disclosures form.

VI. Disclosures of PHI to Business Associate

A Business Associate is an entity or person who performs or assists in performing a Plan function or activity involving the use and disclosure of PHI. A Business Associate is also one who provides legal, accounting, actuarial, consulting, data aggregations management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Procedure
All uses and disclosures must be consistent with the Business Associate agreement. The disclosures must be approved by the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard. The disclosure must be documented on the Accounting of PHI Disclosures form.

VII. Disclosures of PHI from Spouses, Family Members and Friends

The Plan and employer will not disclose PHI to an individual's family members and friends except as permitted by HIPAA.

Procedure
If an employee receives a request for disclosure of an individual's PHI from an individual's spouse, family member, or personal friend, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then the person's identity must be verified, using the appropriate steps outlined in Section IX, "Verification of Identity of Those Requesting Protected Health Information". The disclosure must be approved by the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard. The disclosure must be documented on the Accounting of PHI Disclosures form.

VIII. Disclosures of De-Identified Information

De-identified information is health information that does not identify an individual and is not reasonably expected to be used to identify an individual. A covered entity can determine whether the information is de-identified in two ways: either by professional statistical analysis or by removing 18 specific identifiers (see **Attachment C**, HIPAA Individual Identifiers).

Procedure
Obtain approval for the disclosure from the Privacy Officer. The Privacy Officer will verify that the information is de-identified. The Plan may freely use and disclose de-identified information and de-identified information is not PHI.

IX. Verification of Identity of Those Requesting Protected Health Information

Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person who is to have access to PHI, if the identity or authority of said person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, by a parent seeking access to the PHI of their minor child, by a personal representative, or by a public Officer seeking access.

A. When an individual requests access to their own PHI:
- Request a form of identification from the individual.
- Verify that the identification matches the identity of the individual requesting access to the PHI.
- Make a copy of the identification provided by the individual and file it with the individual's designated record set.

B. When a parent requests access to PHI of their minor child:
- Seek verification of the person's relationship with the child.

C. When a personal representative requests access to an individual's PHI:
- Require a valid power of attorney or Appointment of Personal Representative for HIPAA purposes.
- Copy this documentation and file it with the individual's designated record set.

D. If a public Officer requests access to PHI, and if the request is for one of the purposes set forth in Section III and IV, then the steps following should be taken to verify the Officer's identity and authority:
- If the request is made in person, request presentation of an agency identification badge, other Officer credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.
- If the request is in writing, verify that the request is on the appropriate government letterhead.
- If the request is by a person purporting to act on behalf of a public Officer, request a written statement (on appropriate government letterhead) that the person is acting under the government's authority, or other evidence or documentation of agency (such as a contract for services, memorandum of understanding, or purchase order), that

establishes that the person is acting on behalf of the public Officer.

- Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impractical, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or administrative tribunal, contact the Privacy Officer.

X. Complying with the "Minimum-Necessary" Standard

SPAPSD will make every effort to limit the use or disclosure of, and requests for, PHI, to the minimum amount necessary to accomplish the intended purpose. The minimum necessary standard does not apply to any of the following:

- Uses or disclosures made to the individual
- Uses or disclosures made pursuant to a valid authorization
- Disclosures made to the Department of Health and Human Services
- Uses or disclosures required by law
- Uses or disclosures required to comply with HIPAA

XI. Procedure for Recurring Disclosures and Requests

Identify recurring disclosures. For each recurring disclosure, identify the types of PHI to be disclosed, the types of person who may receive the PHI, the conditions that would apply to such access, and the standards for disclosures to routinely-hired types of Business Associates. Contact the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard. Document the disclosure on the Accounting of PHI Disclosures form.

Identify recurring requests. For each recurring request, identify the information that is necessary for the purpose of the requested disclosure. Contact the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard. Document the disclosure on the Accounting of PHI Disclosures Form.

Procedures for Complying with Individual Rights

I. Request for Access

An individual has a right to request an inspection and copy of medical information contained in a Designated Record Set for as long as the Plan maintains the medical information in the Designated Record Set. A Designated Record Set is a group of records maintained by or for a health plan and includes the enrollment, payment, claims adjudication, and case or medical

management record systems maintained by or for a health plan; or used in whole or in part by or for the Plan to make decisions about individuals.

Procedure

For disclosure of an individual's PHI, the employee must take the following steps:

- Verify the individual's identity.
- Determine whether the PHI is held in the Designated Record Set.
- Determine whether an exception to the disclosure requirement might exist. See the Privacy Officer as to whether any exception exists.
- Get approval from the Privacy Officer, who will ensure that the amount of information disclosed meets the minimum necessary standard.
- Provide or deny the request within 30 days. If the PHI cannot comply with such a deadline, the deadline may be extended for 30 days by providing written notice to the individual within the original 30 days.
- A denial notice must contain the basis for the denial, a statement of the individual's right to request a review, and directions to the individual for filing a complaint concerning the denial. The information should be provided in a readable format or provided in a format agreed to by the employee.
- At the discretion of the employer, additional fees may be charged for copying, postage, and preparation.
- Disclosures must be documented on the Accounting of PHI Disclosures form.

II. Request for Amendment

Procedure

Upon receipt of a request from an individual, from a parent of a minor child, or from a personal representative for an amendment to an individual's PHI in a Designated Record Set, the employee must take the following steps:

- Verify the individual's identity.
- Determine whether the PHI at issue is held in the employee's Designated Record Set. See the Privacy Officer if the information does not seem to be held in Designated Record Set.
- Determine whether the amendment is allowable under HIPAA's right to access.
- Determine whether the request for the amendment is appropriate.
- Get approval from the Privacy Officer.
- Respond to the request in 60 days by informing the individual whether the request has been accepted or denied. If a decision cannot be made within 60 days, the deadline may be extended for 30 more days.
- Upon acceptance of the amendment, make the change in the designated record set.
- Denied requests must do the following:
    1. The Privacy Officer must review the denial. The denial must include the reason for

the denial, information about the individual's right to disagree, an explanation that the individual may ask that the request for amendment and its denial be included in future disclosures of the information, and directions for filing a complaint concerning the denial.

2. Under circumstances where the individual provides a statement of disagreement, include all specifics relating to the denial.

III. Request for an Accounting of PHI

Procedure

Upon the receipt of a request for an accounting of disclosures, the following procedures must be followed:

- Verify the identity of the individual.
- Inform the individual that there may be a fee charged if the employee has requested this information more than once in the last twelve months.
- Respond to the request within 30 days by providing the accounting or by informing the individual that there have been no disclosures that must be included in an accounting. The 30 day deadline may be extended for an additional 30 days by written notice.
- The accounting must include any disclosure made by the Plan or by a Business Associate for up to six years prior to the request. Disclosures not included are:
    1. To carry out treatment, payment and health care operations.
    2. To the individual about their own PHI.
    3. Incidental to an otherwise permitted use or disclosure.
    4. Pursuant to an individual authorization.
    5. For specific national security or intelligence purposes.
    6. To correctional institution or law enforcement when the disclosure was permitted without an authorization.
    7. As part of a limited data set.
    8. Uses or disclosures made prior to the Plan's compliance date.

The accounting must include the date of disclosure, the name of the entity or person to whom the information was disclosed, a brief description of the PHI disclosed, and a brief statement explaining the purpose for the disclosure (see attached Accounting of PHI Disclosures form).

If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement Officer indicating that notice to the individual of disclosures of PHI would likely impede the agency's activities, then disclosure may not be required. The employee must contact the Privacy Officer under these circumstances for more guidance.

IV. Request for Confidential Communications

Procedure
Upon receipt of request for confidential communications, such as sending it to a different location, or via an alternate means, the following steps must be followed:

- Verify the individual's identity.
- Determine whether the request could endanger the individual.
- Take steps to honor the request.
- If the request cannot be accommodated, the employee must contact the individual explaining why.
- All confidential requests will be maintained by the Privacy Officer.
- Document requests and their dispositions.

V. Requests for Restriction on Use and Disclosures of PHI

Procedure
Upon receipt of request for restrictions of use or disclosure of PHI, the following steps must be followed:

- Verify the individual's identity.
- Take steps to honor the request. If we agree to the restrictions, we cannot later violate such agreement.
- If the request cannot be accommodated, the employee must contact the individual explaining why.
- Track all requests on use or disclosure.
- Notify all Business Associates that may have access to the individual's PHI and the Privacy Officer of any agreed-upon restrictions.
- Document requests and their disposition.

Policies and Procedures for Complying with HIPAA Security Rule

Employees of SPAPSD may create, transmit, receive, or maintain electronic protected health information for Plan administration functions on behalf of the Plan. Electronic protected health information (e-PHI) is defined as protected health information (see introduction to this Privacy Policy) that is transmitted by or maintained in electronic media.

Electronic Media includes:

- Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- Transmission media used to exchange information already in electronic storage

media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

I. Designation of Security Officer

The Director of Human Resources is the designated Security Officer for the Plan. The Security Officer may be contacted via email at bbakunow@pointschools.net or in person at 1900 Polk Street, Stevens Point, WI. The Security Officer is responsible for the initial and ongoing compliance with the HIPAA security rule under this Privacy Policy and related security documentation.

II. Risk Analysis

All of the Plan's functions are carried out by employees of SPAPSD and business associates of the Plan; the Plan does not own or control any equipment or systems used to create, maintain, receive, or transmit e-PHI relating to the Plan. All relevant equipment and systems, and facilities in which such equipment or systems are housed, are owned or controlled by SPAPSD and/or the business associates of the Plan. As a result, the ability to assess any potential risks and vulnerabilities to e-PHI associated with the Plan lies solely with SPAPSD and/or the business associate. Because the Plan does not own and cannot control the equipment or systems used for creating, maintaining, receiving or transmitting e-PHI relating to the Plan, this Policy does not address the many implementation specifications set out as part of the HIPAA Security Rule. SPAPSD and any business associates of the Plan have certain obligations relating to the security of e-PHI that is handled while performing administrative functions for the Plan, as set out in the Plan Document.

III. Plan Document

The Plan document will include provisions requiring SPAPSD to:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the e-PHI that SPAPSD creates, receives, maintains, or transmits on behalf of the Plan;
- Ensure that reasonable and appropriate security measures provide adequate separation between the Plan and SPAPSD;
- Ensure that any agents or subcontractors of SPAPSD that may encounter e-PHI of the Plan agree to implement reasonable and appropriate security measures to protect the e-PHI; and
- Report any security incident(s) to the Security Officer.

IV. Disclosures of e-PHI to Business Associates

A business associate, as defined in Section VI of *Procedures for Use and Disclosure of PHI*, above, may be permitted by the Plan to create, receive, maintain, or transmit e-PHI on its behalf only if the Plan first obtains satisfactory assurances from the business associate that it will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract providing that the business associate will:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the e-PHI that the business associate creates, receives, maintains, or transmits on behalf of the Plan;
- Ensure that any agents or subcontractors of the business associate that may encounter e-PHI of the Plan agree to implement reasonable and appropriate security measures to protect the e-PHI;
- Report any security incident(s) to the Plan; and
- Provide for termination of the contract at the Plan's option if the Plan determines that the business associate has violated a material term of the contract.

V. Documentation

Any documentation relating to the security of e-PHI may appear in either written or electronic form, and will be maintained in accordance with Section VI of *Internal Policies for HIPAA Compliance*, above. The Plan will make its policies, procedures, and other documentation available to the Security Officer, SPAPSD, business associates, or other persons or entities responsible for implementing any procedures referenced herein.

ATTACHMENT A

EMPLOYEES OF STEVENS POINT AREA PUBLIC SCHOOL DISTRICT
WITH ACCESS TO
PROTECTED HEALTH INFORMATION
INCLUDING
ELECTRONIC PROTECTED HEALTH INFORMATION

1. Lyndel Ahles, Benefits Assistant
2. Beth Bakunowicz, Director of Human Resources
3. Brian Casey, Director of Information Technology
4. Mick Kluz, Payroll Specialist
5. Mike Kurtz, Finance Manager
6. Amy Mayek, Human Resources Specialist
7. Jan Northcraft, Human Resources Coordinator/Employment
8. Tom Owens, Director of Business Services
9. Alexa Schultz, Human Resources Coordinator/Benefits

ATTACHMENT B

STEVENS POINT AREA PUBLIC SCHOOL DISTRICT
TECHNICAL AND PHYSICAL SAFEGUARDS AND FIREWALLS

Administrative

- *The Privacy Policy and Notice of Privacy Practices will be reviewed annually by the Privacy Officer at the time of the Plan's renewal.*
- *The Privacy Officer will review Attachment A and add or remove employees needing to have access to PHI, ensure that any added employees receive training on the HIPAA Privacy Policy, and ensure that any employee who is not on Attachment A does not have access to PHI.*
- *Employees named on Attachment A will be required to follow a "clean desk" policy, which means that during breaks and at the end of the workday, all PHI will be stored/filed in filing cabinets or desk drawers.*

Technical

- *All computers will be protected by passwords that only the employee and the Information Management Department personnel know.*
- *Employees listed on Attachment A will minimize PHI information on their computer screen when leaving the work area at any time.*
- *Employees listed on Attachment A will have a password-protected screen saver appear when they are away from their desks for five minutes or longer.*

Physical

- *Hard copies of PHI will be maintained in a locked filing cabinet in the Benefits Office.*
- *Computer back-ups of PHI will be kept in a locked closet accessible only to the Information Technology Director listed on Attachment A.*

ATTACHMENT C

LIST OF INDIVIDUAL IDENTIFIERS

- Names
- All elements of dates (except year) for dates related to an individual, such as date of birth or death, admission or discharge dates, and any age over 89 and any dates indicating such age, except if grouped together by “90 or over”.
- Telephone numbers
- Fax numbers
- Social Security numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Internet protocol numbers (IP addresses)
- Full facial photographic images or any comparable images
- Certain postal address information (town/city or state is ok)
- Account numbers
- Device identifiers and serial numbers
- Email addresses
- Medical records numbers
- Vehicle identifiers, license plate, or serial numbers
- Web Universal Resource Locators (URLs)
- Biometric identifiers (voice or finger print recognition)
- Any other unique identifying number, characteristic, or code