

LINE MOUNTAIN SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: PRIVACY OF HEALTH
INFORMATION (HIPAA)

ADOPTED: March 6, 2018

REVISED:

826. PRIVACY OF HEALTH INFORMATION (HIPAA)

This Policy applies to the following employee benefit plans (the "Plan") that are sponsored by Line Mountain School District (the "Employer"): Health Care FSA. This Privacy Policy is effective as of September 23, 2013 (the "Effective Date").

General Policy

It is the policy of the Plan (also known as the "covered entity" under the HIPAA privacy rule) to maintain and protect the privacy of the protected health information ("PHI") of its plan participants and to give its participants specific rights with respect to their PHI.

Purpose

This policy is intended to promote awareness of the confidential nature of the medical information that is collected, maintained and disseminated by the Plan. This policy and these procedures reflect the commitment of the Employer to protecting the confidentiality of private health information.

Structure

This Privacy Policy shall be overseen by the Privacy Official. The Privacy Official shall have authority and responsibility for implementation and operation of this policy.

Collection and Receipt of Protected Health Information

Policy

The Plan will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the collection, receipt or maintenance of PHI. The designated record set of the Plan includes all enrollment and disenrollment information, along with any claim forms, explanations of benefits, and any other information that the Plan receives as part of the operations and payment functions of the Plan.

Procedures

1. When collecting or receiving PHI, employees will request only the minimum necessary information. Prior to making such a request and at the time this policy first becomes effective, employees who collect or receive PHI will evaluate the information that is requested or received to determine that he or she is receiving or requesting the minimum necessary. The Privacy Official will make the final determination (when necessary) as to what information can be requested and received.
2. When collecting or discussing PHI, employees will comply with the following

	<p>privacy guidelines, along with any additional procedures established from time to time:</p> <ul style="list-style-type: none"> • PHI should not be discussed in any open area; • Documents containing PHI should be kept in locked files and should not be left in any open area or area where the general public has access; • Documents containing PHI should be de-identified wherever possible; and • Documents containing PHI should be shredded when they are no longer needed. <p>3. PHI will be discussed and shared with an employee only to the extent that the individual has a need to know the PHI as part of the performance of his or her job duties.</p> <p>4. The information in the designated record set will be kept in a file separate from an employee's employment file.</p> <p><u>Uses and Disclosures of Protected Health Information</u></p> <p><u>Policy</u></p> <p>1. The Plan will use and disclose the PHI it creates, collects and/or maintains for its treatment, payment and healthcare operations, including, but not limited to the following: to enroll and disenroll individuals in or from the Plan; to evaluate renewal proposals or new health plan vendors, insurance companies or administrators; to assist in claims resolution; and to conduct due diligence in connection with the sale or transfer of assets to a potential successor.</p> <p>2. All PHI collected by the Plan will be disclosed only to the following "valid recipients" or in the following situations: (1) to the plan participant; (2) to the plan participant's enrolled spouse; (3) if the plan participant is an enrolled dependent child, to the plan participant's parent or legal guardian (a Personal Representative); (4) to a Personal Representative of an individual who is incapable of making health care decisions and/or has appointed another individual to make these decisions on his or her behalf; (5) to an insurance company, reinsurance company, third party administrator or a business associate of the Plan, (6) to the plan participant's representative, agent, or any other person with a signed authorization from the plan participant; (7) in response to legal process; (8) to investigate possible insurance fraud; (9) for claims management related to nurse navigation; (10) to help settle a claim dispute for benefits under a medical benefit plan or insurance policy; or (11) to the Plan Sponsor, but only if the plan documents have been amended in accordance with the provisions of HIPAA.</p> <p>3. The Plan will obtain written authorization to disclose certain types of PHI, i.e., psychotherapy notes and to disclose PHI under certain circumstances, i.e., the sale and marketing of PHI resulting in the Plan receiving remuneration.</p> <p>4. The Plan will execute Business Associate Agreements with outside entities that create, receive, maintain or transmit protected health information in the course of performing functions on behalf of the Plan. The agreement will <i>inter alia</i> require the business associate to comply with the HIPAA Privacy</p>
--	---

	<p>Rule, report a breach of unsecured PHI to the Plan, and agree to enter into business associate agreements with any subcontractors who receive the Plan's PHI.</p> <p><u>Procedures</u></p> <ol style="list-style-type: none"> 1. To the extent reasonably possible, PHI that is requested or disclosed by the Plan will be received or distributed after it has been de-identified. The Privacy Official will oversee the de-identification process. 2. Where it is not possible or practicable to de-identify PHI that is disclosed, employees will disclose only the minimum necessary information. The Privacy Official will help, upon request, to determine that the minimum necessary information is disclosed. Minimum necessary standards will be created and followed for all routine disclosures of PHI. 3. In any situation where PHI is requested from the Plan, an employee will verify the identity of the person requesting the information and the authority of the person to have access to PHI (unless the identity and authority is already known). 4. PHI will be disclosed to a Valid Recipient as described above through the telephone, only after the identity and authority of the person who is on the other end of the call is verified. 5. PHI will be sent to a Valid Recipient by facsimile only if the employee who is sending the information can determine that the intended recipient will be the receiver of the facsimile, or that he or she is expecting the confidential facsimile at that time. 6. All fax cover sheets utilized by employees will contain a standard confidentiality statement. 7. The Plan will not use or disclose PHI that is genetic information for underwriting purposes. 8. The Plan may disclose PHI to family members or others who were involved in the decedent's health care or payment for their care prior to the decedent's death so long as the disclosure is relevant to the person's involvement and is not inconsistent with the decedent's prior expressed wishes. <p><u>Access to Protected Health Information by Plan Participants</u></p> <p><u>Policy</u></p> <p>The Plan will provide plan participants with the right to access their own PHI that has been collected and is maintained by the Plan and is part of the designated record set. This right of access does not apply to information compiled in anticipation of a civil legal action.</p> <p><u>Procedures</u></p> <ol style="list-style-type: none"> 1. A plan participant (or his or her Personal Representative, including the parent or legal guardian of an enrolled dependent child) may request a copy of his or her PHI, as long as the request is in writing and is dated and signed by the plan
--	---

	<p>participant on a form approved by the Plan. All such requests will be given to the Privacy Official for response.</p> <ol style="list-style-type: none"> 2. Within 30 days of receipt of the written request, the Privacy Official will inform the plan participant of the acceptance of the request, will provide a written denial, or will direct the plan participant to the entity that maintains the requested information. 3. The Privacy Official will provide the plan participant either with the ability to inspect the plan participant's file or will provide a copy of the file, as requested by the plan participant. The Plan may charge a reasonable fee for all copying requests. This fee will include supplies, labor and postage. 4. The Privacy Official will provide the file in the format requested by the plan participant, unless it is not readily producible in that format. 5. If the plan participant directs the Plan in writing to transmit an electronic copy of his/her PHI to another person, the Plan will generally comply. 6. The Privacy Official may provide the plan participant with a summary of the PHI or an explanation of the PHI, if the plan participant requests such a summary or explanation. <p><u>Amendment of Protected Health Information</u></p> <p><u>Policy</u></p> <p>The Plan will allow plan participants to request amendment of their PHI that is part of the designated record set. PHI that was not created by the Plan or that is accurate and complete, as determined by the Privacy Official, is not subject to amendment.</p> <p><u>Procedures</u></p> <ol style="list-style-type: none"> 1. A request for amendment of PHI must be made on a form approved by the Plan. The request must be made by the plan participant or the plan participant's personal representative, parent (for a minor or an enrolled dependent child) or guardian (collectively referred to as "plan participant"). The request must reference the information for which amendment is requested and the reason for the requested amendment. 2. When a plan participant first contacts the Plan to request an amendment, the employee who receives the request will notify the plan participant of the requirements for requesting the change. 3. All written requests for amendment will be forwarded to the Privacy Official for response. 4. Within 60 days after receipt of the request for amendment, the Privacy Official will either accept or deny the amendment request. The Privacy Official will make this determination. If the amendment request is accepted, the Privacy Official will notify the plan participant and request the agreement of the plan participant to notify business associates or other persons who have received the incorrect PHI about the plan participant from the Plan. If the amendment request is denied, the Privacy Official will notify the plan participant of the basis for the denial, the right of the plan participant to submit a written statement of
--	--

	<p>disagreement or to request that the amendment and the denial be included in any future disclosures, and a description of how the plan participant may file a complaint.</p> <p>5. If the plan participant files a statement of disagreement, the Privacy Official may prepare a written rebuttal, which must be given to the plan participant. All future disclosures of PHI for this plan participant must include both the statement of disagreement and the rebuttal, if any, and a link between these documents and the PHI that is subject to dispute.</p> <p><u>Accounting of Disclosures of PHI</u></p> <p><u>Policy</u> It is the Policy of the Plan to provide plan participants with an accounting of disclosures of PHI that were made for purposes other than the payment and healthcare operations of the Plan.</p> <p><u>Procedures</u> All disclosures of PHI, other than those conducted in the course of payment or healthcare operations of the Plan, will be reported to the Privacy Official. When requested by a plan participant in writing, the Privacy Official will prepare an accounting of all disclosures that were not part of the health care operations of the Plan. The accounting will include all disclosures made by the Plan that occurred in the past six years (or shorter period as requested by the plan participant), but excluding any disclosures made prior to April 14, 2004, and will comply with all applicable laws and regulations. The accounting will be provided within 60 days of the request. No charge will be imposed for the first accounting requested during any 12-month period.</p> <p><u>Restriction on Disclosures of PHI</u></p> <p><u>Policy</u> It is the Policy of the Plan to allow plan participants to request a restriction on the uses and disclosures of the plan participant's PHI made by the Plan.</p> <p><u>Procedures</u></p> <ol style="list-style-type: none"> 1. A request for restriction on the uses and disclosures of PHI must be made on a form approved by the Plan. The request must be made by the plan participant or the plan participant's personal representative, parent (for a minor or an enrolled dependent child) or guardian (collectively referred to as "plan participant"). The request must reference the particular type of restriction that is requested and the reason for the requested restriction. 2. When a plan participant first contacts the Plan to request a restriction, the employee who receives the request will notify the plan participant of the requirements for requesting the change. 3. All written requests for restriction will be forwarded to the Privacy Official for response. 4. Within a reasonable period of time after receipt of the request for restriction, the Privacy Official will either accept or deny the restriction request. The Privacy Official will make this determination. If the restriction request is accepted, the
--	---

	<p>Privacy Official will notify the plan participant and will document the agreed upon restriction. If the restriction request is denied, the Privacy Official will notify the plan participant of the basis for the denial.</p> <p><u>Notice of Privacy Practices</u></p> <p><u>Policy</u> It is the Policy of the Plan to create and, as required by law, to provide all employees with a Notice of Privacy Practices that describes the Plan's required and permitted uses and disclosures of PHI and the rights of plan participants with respect to their PHI.</p> <p><u>Procedures</u></p> <ol style="list-style-type: none"> 1. The employer will deliver the Notice of Privacy Practices to each employee as soon as possible after the Effective Date. If an employee has requested that benefit, enrollment or other employment information be delivered by e-mail, the notice may be given by e-mail. Otherwise, the Notice will either be hand delivered or sent by interoffice or U.S. mail. 2. If the employer maintains an employee benefits related website, the employer will also post of copy of the Notice of Privacy Practices prominently on its website. 3. Every three years from the date of the initial delivery of the Notice, the Privacy Official will be responsible for notifying employees that the Notice is available and that they can receive a copy of it on request. 4. A revised Privacy Notice will be delivered to each employee within 60 days after a material change is made, based on a change in the law or regulations or a change in internal procedures. <p><u>Notice in case of Breach of Unsecured PHI</u></p> <p><u>Policy</u> It is the Policy of the Plan to secure PHI in accordance with its Security Policy (if the employer maintains any PHI in an electronic format on behalf of the plan) and to notify individuals, the media and the Department of Health and Human Services in the event of a breach of unsecured PHI, in accordance with the HITECH Act. The Plan will presume that a reportable breach has occurred when any impermissible acquisition, access, use or disclosure of unsecured PHI has happened, unless the Plan can demonstrate there is a low probability that the information has been compromised based on a risk assessment of certain factors or the breach fits within certain exceptions.</p> <p><u>Procedures</u></p> <ol style="list-style-type: none"> 1. The employer will follow any Security Policy that it has adopted to comply with the HIPAA Security Rules and will secure any electronic PHI that it maintains in accordance with the HITECH Act. 2. The employer will document all risk assessments regarding all reportable breaches in order to demonstrate it provided all required breach notifications or, in the alternative, that the impermissible use or disclosure did not constitute a breach.
--	--

3. For any breach of unsecured PHI (as both breach and unsecured are defined in the HITECH Act, the employer will provide written notice or a substitute notice (if the last known contact address is insufficient) to each affected individual within 60 days following discovery of any breach of Unsecured PHI. The notice will include:
 - A brief description of what happened including the date of the breach and the date of discovery, if known;
 - A description of the types of unsecured PHI that were involved in the breach;
 - Any steps the individual should take to protect him/herself from potential harm resulting from the breach;
 - A brief description of what the employer is doing to investigate the breach in accordance with HIPAA breach notification requirements;
 - Contact procedures for individuals to ask questions or learn additional information
4. If a breach of unsecured PHI involves more than 500 residents of a state, the employer will provide notice to local media outlets serving the state without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
5. If a breach of unsecured PHI involves more than 500 individuals, the employer will provide notice to DHHS without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
6. If a breach of unsecured PHI involves less than 500 covered persons, the employer will provide notice to the DHHS not later than 60 days after the end of the calendar year in which the breach was discovered.

Training

Policy

The Privacy Official will train or oversee training of all new employees and current staff who have access to PHI. Training will include general information about HIPAA and will focus on the requirements of this Privacy Policy.

Procedures

1. The Privacy Official will conduct or oversee the training for all employees who have or may have access to PHI no later than the date that this Policy becomes effective. New staff will receive training on the Privacy Policy within 3 months of the start of their employment, or within 3 months of the assignment to a position in which they deal with PHI as part of their job requirements.
2. The Privacy Official will conduct training on any material changes made to the Privacy Policy within 60 days after the changes become effective.
3. Additional training sessions may be conducted by the Privacy Official as needed.
4. All training will be documented by the Privacy Official, or other employee as requested by the Privacy Official.

	<p><u>Complaints</u></p> <p><u>Policy</u> The Plan will accept and respond to complaints relating to the Privacy Policy, procedures, and compliance efforts relating to the privacy of PHI.</p> <p><u>Procedures</u></p> <ol style="list-style-type: none"> 1. Complaints regarding this Privacy Policy will be forwarded to the Privacy Official for review and response. 2. The Privacy Official will review all complaints, will discuss them (as needed) with the Controller and/or other employees, will review relevant documents and will respond to the plan participant who has filed the complaint. 3. All complaints will be logged by the Privacy Official. The log will include the complaint and a brief description of the resolution of the complaint. <p><u>Recordkeeping</u></p> <p><u>Policy</u> The Plan will retain all documentation related to this Privacy Policy for a minimum of six (6) years from the date the documentation was created or the date that it was last in effect, whichever is later.</p> <p><u>Procedures</u></p> <ol style="list-style-type: none"> 1. The following documents will be maintained in the files of the Privacy Official or other secured location: <ul style="list-style-type: none"> • This Privacy Policy • Notice of Privacy Practices (all versions) • Privacy Notice and Notice of Privacy Practices Distribution Log • All signed authorizations • PHI Disclosure Log • Record Request Log • Record Requests • Complaint Log, along with copies of any written complaints • Records of any sanctions imposed on employees • Employee training manuals and procedures • Business associate contracts • Plan document amendments • Plan sponsor certification • Record of breaches and any associated risk assessments • Breach Information 2. Every year on or about January 1, the Privacy Official will determine which records, if any, have been held for the minimum period required and should be destroyed. <p><u>Sanctions</u></p> <p><u>Policy</u> The Plan Sponsor, on behalf of the Plan, will appropriately discipline any staff member who fails to comply with this Privacy Policy.</p>
--	--

Procedures

For any failure to comply with this Privacy Policy, an employee will be subject to sanctions up to and including removal of access by the employee to PHI and termination of employment.

Miscellaneous Policies

Mitigation of Wrongful Disclosures

The Plan will attempt to mitigate any disclosures of PHI that are in violation of this Privacy Policy by, for example, requesting return of any written PHI that was improperly disclosed, or by admonishing the recipients of any wrongly-disclosed PHI of their obligation not to further disclose the PHI.

Refraining from Intimidating or Retaliatory Acts

It is the policy of the Plan to prohibit any intimidation, threats, coercion, discrimination or other retaliatory acts against any person for the exercise of his or her rights under this Privacy Policy, for filing a complaint with the DHHS, or for assisting in an investigation of any act made unlawful by the Health Insurance Portability and Accountability Act.

This Privacy Policy is effective as of the Effective Date shown above.

Signature: 

Name (print or type): David M. Campbell

Title: Superintendent

Date Signed: March 9, 2018

Summary of Privacy Practices

This Summary of Privacy Practices summarizes how medical information about you may be used and disclosed by the Line Mountain School District group health plan (the "Plan") or others in the administration and management of your claims, and certain rights that you have. For a complete, detailed description of all privacy practices, as well as your legal rights, please refer to the accompanying Notice of Privacy Practices.

Our Pledge Regarding Medical Information

We are committed to protecting your personal health information. We are required by law to (1) make sure that any medical information that identifies you is kept private; (2) provide you with certain rights with respect to your medical information; (3) give you a notice of our legal duties and privacy practices; and (4) follow all privacy practices and procedures currently in effect.

How We May Use and Disclose Medical Information About You

We may use and disclose your personal health information without your permission to facilitate your medical treatment, for payment for any medical treatments, for cost and/or claims management and for any other health care operation. We will disclose your medical information to employees of Line Mountain School District for plan administration functions; but those employees may not share your information for employment-related purposes. We may also use and disclose your personal health information without your permission, as allowed or required by law. Otherwise, we must obtain your written authorization for any other use and disclosure of your medical information. We cannot retaliate against you if you refuse to sign an authorization or revoke an authorization you had previously given.

Your Rights Regarding Your Medical Information

You have the right to inspect and copy your medical information, to request corrections of your medical information, and to obtain an accounting of certain disclosures of your medical information. You also have the right to request that additional restrictions or limitations be placed on the use or disclosure of your medical information, or that communications about your medical information be made in different ways or at different locations.

How to File Complaints

If you believe your privacy rights have been violated, you have the right to file a complaint with us or with the Office for Civil Rights. We will not retaliate against you for making a complaint.

LINE MOUNTAIN SCHOOL DISTRICT

NOTICE OF PRIVACY PRACTICES

THIS NOTICE OF PRIVACY PRACTICES DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

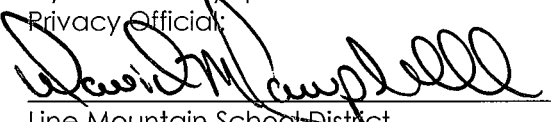
This Notice of Privacy Practices (the "Notice") describes the legal obligations of the Line Mountain School District group health plan (the "Plan") and your legal rights regarding your protected health information held by the Plan under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Among other things, this Notice describes how your protected health information may be used or disclosed to carry out treatment, payment, or health care operations, or for any other purposes that are permitted or required by law.

We are required to provide this Notice of Privacy Practices to you pursuant to HIPAA.

The HIPAA Privacy Rule protects only certain medical information known as "protected health information" or "PHI". Generally, protected health information is individually identifiable health information, including demographic information, collected from you or created or received by a health care provider, a health care clearinghouse, a health plan, or your employer on behalf of a group health plan that relates to:

- (1) your past, present or future physical or mental health or condition;
- (2) the provision of health care to you; or
- (3) the past, present or future payment for the provision of health care to you.

If you have any questions about this Notice or about our privacy practices, please contact the designated Privacy Official:



Line Mountain School District
185 Line Mountain Road
Herndon, PA 17830
(570) 758-2640

Privacy Official

Effective Date

This Notice is effective September 23, 2013.

Our Responsibilities

We are required by law to:

- maintain the privacy of your protected health information;
- provide you with certain rights with respect to your protected health information;
- provide you with a copy of this Notice of our legal duties and privacy practices with respect to your protected health information; and
- follow the terms of the Notice that is currently in effect.

We reserve the right to change the terms of this Notice and to make new provisions regarding your protected health information that we maintain, as allowed or required by law. If we make any material change to this Notice, we will provide you with a copy of our revised Notice of Privacy Practices via any reasonable method or by mailing a revised notice to your last-known address on file.

How We May Use and Disclose Your Protected Health Information

Under the law, we may use or disclose your protected health information under certain circumstances without your permission. The following categories describe the different ways that we may use and disclose your protected health information. For each category of uses or disclosures we will explain what we mean and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

For Payment. We may use or disclose your protected health information to determine your eligibility for Plan benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under the Plan, or to coordinate Plan coverage. For example, we may tell your health care provider about your medical history to determine whether a particular treatment is experimental, investigational, or medically necessary, or to determine whether the Plan will cover the treatment. We may also share your protected health information with a utilization review or precertification service provider. Likewise, we may share your protected health information with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments.

For Health Care Operations. We may use and disclose your protected health information for other Plan operations. These uses and disclosures are necessary to run the Plan. For example, we may use medical information in connection with conducting quality assessment and improvement activities; underwriting, premium rating, and other activities relating to Plan coverage; submitting claims for stop-loss (or excess-loss) coverage; conducting or arranging for medical review, legal services, audit services, and fraud & abuse detection programs; business planning and development such as cost management; and business management and general Plan administrative activities.

To Business Associates. We may contract with individuals or entities known as Business Associates to perform various functions on our behalf or to provide certain types of services. In order to perform these functions or to provide these services, Business Associates will receive, create, maintain, use and/or disclose your protected health information, but only after they agree in writing with us to implement appropriate safeguards regarding your protected health information. For example, we may disclose your protected health information to a Business Associate to administer claims or to provide support services, such as utilization management, pharmacy benefit management, claims management, nurse navigation, or subrogation, but only after the Business Associate enters into a Business Associate contract with us.

As Required by Law. We will disclose your protected health information when required to do so by federal, state or local law. For example, we may disclose your protected health information when required by national security laws or public health disclosure laws.

To Avert a Serious Threat to Health or Safety. We may use and disclose your protected health information when necessary to prevent a serious threat to your health and safety, or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat. For example, we may disclose your protected health information in a proceeding regarding the licensure of a physician.

To Plan Sponsors. For the purpose of administering the plan, we may disclose to certain employees of the Employer protected health information. However, those employees will only use or disclose that information as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized further disclosures. Your protected health information cannot be used for employment purposes without your specific authorization.

Special Situations

In addition to the above, the following categories describe other possible ways that we may use and disclose your protected health information. For each category of uses or disclosures, we will explain what we mean and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

Military and Veterans. If you are a member of the armed forces, we may release your protected health information as required by military command authorities. We may also release protected health information about foreign military personnel to the appropriate foreign military authority.

Workers' Compensation. We may release your protected health information for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public Health Risks. We may disclose your protected health information for public health actions. These actions generally include the following:

- to prevent or control disease, injury, or disability;
- to report births and deaths;
- to report child abuse or neglect;
- to report reactions to medications or problems with products;
- to notify people of recalls of products they may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- to notify the appropriate government authority if we believe that a patient has been the victim of abuse, neglect, or domestic violence. We will only make this disclosure if you agree, or when required or authorized by law.

Health Oversight Activities. We may disclose your protected health information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose your protected health information in response to a court or administrative order. We may also disclose your protected health information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Law Enforcement. We may disclose your protected health information if asked to do so by a law enforcement official—

- in response to a court order, subpoena, warrant, summons or similar process;
- to identify or locate a suspect, fugitive, material witness, or missing person;
- about the victim of a crime if, under certain limited circumstances, we are unable to obtain the victim's agreement;
- about a death that we believe may be the result of criminal conduct; and
- about criminal conduct.

Coroners, Medical Examiners and Funeral Directors. We may release protected health information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients to funeral directors, as necessary to carry out their duties.

National Security and Intelligence Activities. We may release your protected health information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Inmates. If you are an inmate of a correctional institution or are in the custody of a law enforcement official, we may disclose your protected health information to the correctional institution or law enforcement official if necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Research. We may disclose your protected health information to researchers when:

- (1) the individual identifiers have been removed; or
- (2) when an institutional review board or privacy board has reviewed the research proposal and established protocols to ensure the privacy of the requested information, and approves the research.

Required Disclosures

The following is a description of disclosures of your protected health information we are required to make.

Government Audits. We are required to disclose your protected health information to the Secretary of the United States Department of Health and Human Services when the Secretary is investigating or determining our compliance with the HIPAA privacy rule.

Disclosures to You. When you request, we are required to disclose to you the portion of your protected health information that contains medical records, billing records, and any other records used to make decisions regarding your health care benefits. We are also required, when requested, to provide you with an accounting of most disclosures of your protected health information if the disclosure was for reasons other than for payment, treatment, or health care operations, and if the protected health information was not disclosed pursuant to your individual authorization.

Other Disclosures

Personal Representatives. We will disclose your protected health information to individuals authorized by you, or to an individual designated as your personal representative, attorney-in-fact, etc., so long as you provide us with a written notice/authorization and any supporting documents (i.e., power of attorney). Note: Under the HIPAA privacy rule, we do not have to disclose information to a personal representative if we have a reasonable belief that:

- (1) you have been, or may be, subjected to domestic violence, abuse or neglect by such person; or
- (2) treating such person as your personal representative could endanger you; and
- (3) in the exercise of professional judgment, it is not in your best interest to treat the person as your personal representative.

Spouses and Other Family Members. With only limited exceptions, we will send all mail to the employee. This includes mail relating to the employee's spouse and other family members who are covered under the Plan, and includes mail with information on the use of Plan benefits by the employee's spouse and other family members and information on the denial of any Plan benefits to the employee's spouse and other family members. If a person covered under the Plan has requested Restrictions or Confidential Communications (see below under "Your Rights"), and if we have agreed to the request, we will send mail as provided by the request for Restrictions or Confidential Communications.

Authorizations. Other uses or disclosures of your protected health information not described above will only be made with your written authorization. Examples include, but are not limited to, psychotherapy notes, uses and disclosures for marketing purposes and any sale of PHI. You may revoke written authorization at any time, so long as the revocation is in writing. Once we receive your written revocation, it will only be effective for future uses and disclosures. It will not be effective for any information that may have been used or disclosed in reliance upon the written authorization and prior to receiving your written revocation.

Underwriting. If the group health plan uses PHI for underwriting purposes, the plan will not use or disclose genetic information for underwriting purposes.

Your Rights

You have the following rights with respect to your protected health information:

Right to Inspect and Copy. You have the right to inspect and copy certain protected health information that may be used to make decisions about your health care benefits. To inspect and copy your protected health information, you must submit your request in writing to the Privacy Official. If you request a copy of the information, we may charge a reasonable fee for the costs of copying, mailing, or other supplies associated with your request.

We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to your medical information, you may request that the denial be reviewed by submitting a written request.

Right to Amend. If you feel that the protected health information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan.

To request an amendment, your request must be made in writing and submitted to the Privacy Official. In addition, you must provide a reason that supports your request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- is not part of the medical information kept by or for the Plan;
- was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the information that you would be permitted to inspect and copy; or
- is already accurate and complete.

If we deny your request, you have the right to file a statement of disagreement with us and any future disclosures of the disputed information will include your statement.

Right to an Accounting of Disclosures. You have the right to request an “accounting” of certain disclosures of your protected health information. The accounting will not include (1) disclosures for purposes of treatment, payment, or health care operations; (2) disclosures made to you; (3) disclosures made pursuant to your authorization; (4) disclosures made to friends or family in your presence or because of an emergency; (5) disclosures to business associates; (6) disclosures for national security purposes; and (7) disclosures incidental to otherwise permissible disclosures.

To request this list or accounting of disclosures, you must submit your request in writing to the Privacy Official. Your request must state a time period of not longer than the past six years. Your request should indicate in what form you want the list (for example, paper or electronic). The first list you request within a 12-month period will be provided free of charge. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Right to Request Restrictions. You have the right to request a restriction or limitation on your protected health information that we use or disclose for treatment, payment, or health care operations. You also have the right to request a limit on your protected health information that we disclose to someone who is involved in your care or the payment for your care, such as a family member or friend. For example, you could ask that we not use or disclose information about a surgery that you had.

Except as provided in the next paragraph, we are not required to agree to your request. However, if we do agree to the request, we will honor the restriction until you revoke it or we notify you.

Effective February 17, 2010 (or such other date specified as the effective date under applicable law), we will comply with any restriction request if (1) except as otherwise required by law, the disclosure is to the health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

To request restrictions, you must make your request in writing to the Privacy Official. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure, or both; and (3) to whom you want the limits to apply—for example, disclosures to your spouse.

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail.

To request confidential communications, you must make your request in writing to the Privacy Official. We will not ask you the reason for your request. Your request must specify how or where you wish to be contacted. We will accommodate all reasonable requests if you clearly provide information that the disclosure of all or part of your protected information could endanger you.

Right to Be Notified of a Breach. You have the right to be notified in the event that we (or a Business Associate) discover a breach of unsecured protected health information.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice.

To obtain a paper copy of this notice contact the Privacy Official identified on the first page of this Notice.

Complaints

If you believe that your privacy rights have been violated, you may file a complaint with the Plan or with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the Plan, contact the Privacy Official. All complaints must be submitted in writing.

You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with us.

NOTICE OF AVAILABILITY OF NOTICE OF PRIVACY PRACTICES

The Line Mountain School District Group Health Plan (the "Plan") provides health benefits to eligible employees and their eligible dependents as described in the summary plan description(s) for the Plan. The Plan creates, receives, uses, maintains and discloses health information about Plan participants in the course of providing these health benefits. The Plan is required by law to provide notice to participants of the Plan's duties and privacy practices with respect to covered individuals' protected health information, and has done so by providing to Plan participants a notice of privacy practices, which describes the ways that the Plan uses and discloses PHI. To receive a copy of the Plan's notice of privacy practices you should contact your employer's Privacy Official, who has been designated as the Plan's contact person for all issues regarding the Plan's privacy practices and covered individuals' privacy rights. You can reach this contact person at: (570) 758-2460.

LINE MOUNTAIN SCHOOL DISTRICT

NOTICE OF PRIVACY PRACTICES DISTRIBUTION LOG

Plan Participant's Name	Date of Distribution of Initial Notice of Privacy Practices	Date of Distribution of Notice of Availability of Notice of Privacy Practices	Date of Distribution of Notice of Availability of Notice of Privacy Practices	Date of Distribution of Notice of Availability of Notice of Privacy Practices

LINE MOUNTAIN SCHOOL DISTRICT

PRIVACY COMPLAINT FORM

Line Mountain School District (the "Employer"), on behalf of the health plan sponsored by the Employer, maintains a privacy policy in accordance with federal privacy rules. That policy addresses how your health information is used or disclosed by the health plan and explains your rights with respect to that information. The employer also maintains a Notice of Privacy Practices on behalf of the health plan. You have a right to see a copy of this Notice upon request.

If you think your privacy rights have been violated or that the Employer has not followed the steps and procedures shown in our privacy policy or the Notice of Privacy Practices, use this form to record your complaint. This complaint form and process is an important part of your protected rights, and provides the Employer with a means to uncover any violations and/or problems with our policies.

Complaint Section	
Please describe your complaint below or attach a separate document.	
Plan Participant's Name: _____	Date: _____
Complaint: _____	

Signature: _____	

Do not write below this line.

Employer Resolution Section	
Employer will provide a written response to your complaint within 30 days using the space below or in a separate document.	
Name of employer respondent: _____	Date: _____

LINE MOUNTAIN SCHOOL DISTRICT PRIVACY COMPLAINT LOG

This log records and summarizes all complaints filed by participants in a group health plan sponsored by Line Mountain School District (the "Employer") concerning violations of the Group Health Plan's Privacy Policy and other privacy practices and procedures, as well as the resolution or disposition of each complaint by the Employer on behalf of the Group Health Plan.

All additional documentation related to the complaint will be kept in a file pertaining to the individual who filed the complaint.

Plan Participant's Name	Date Complaint filed with Employer	Brief summary of nature of complaint	Date of Complaint Resolution by Employer	Brief Summary of Resolution or Disposition

LINE MOUNTAIN SCHOOL DISTRICT RECORD REQUEST FORM

Please describe below the health information you wish to access or amend, or ways in which you wish to restrict disclosure of your Protected Health Information.

If you are requesting an accounting of disclosures, please indicate the time period for which you are requesting an accounting.

For an access request, please include whether you would like to access the information in person or have a copy emailed to you or sent to you by regular mail. You may also request a summary of this information.

For an amendment request, please include specific reasons why you believe your Protected Health Information should be amended.

For a restriction request, please describe the type of restriction and the reason for the requested restriction.

Please attach an additional page if needed.

Plan Participant's Name: _____ Date: _____

Request: _____

Signature: _____

If applicable, printed name and authority of Personal Representative:

Name: _____

Relationship to Plan Participant: _____

LINE MOUNTAIN SCHOOL DISTRICT RECORD REQUEST LOG

This log records and summarizes all requests to access, amend or restrict disclosure of Protected Health Information, filed by a participant in a Group Health Plan sponsored by Line Mountain School District.

Plan Participant's Name	Date Request filed with Employer	Brief summary of type of access, amendment or restriction requested	Request Approved or Denied	Group Health Plan's actions

LINE MOUNTAIN SCHOOL DISTRICT

PROTECTED HEALTH INFORMATION DISCLOSURE LOG

This log records and summarizes all disclosures of a plan participant's Protected Health Information (PHI) made by a group health plan sponsored by Line Mountain School District (the "Employer"), except for those disclosures that were (1) made for the payment or healthcare operations of the Employer; (2) made to the individual who is the subject of the information; (3) made incident to an otherwise permitted disclosure; (4) made pursuant to an authorization; (5) made for national security purposes, to a correctional institution or to law enforcement; or (6) made prior to April 14, 2004.

EXAMPLES OF ITEMS TO INCLUDE ON LOG: (1) disclosures made in response to a subpoena or an order of a court or administrative tribunal (if there is no official court order certain steps must be made to notify the patient); (2) disclosures made to the Department of Health for communicable disease reporting purposes; (3) disclosures made for domestic or child abuse reporting (you are required to tell the individual that you are making this disclosure, unless you think notification would put the person in greater harm); and (4) disclosures made for OSHA reporting or workers' compensation purposes.

Plan Participant's Name (person whose PHI was disclosed)	Date of Disclosure	Name of Entity or Person who Received PHI	Brief description of the PHI Disclosed	Brief Statement of purpose for making Disclosure (if written authorization was obtained, so indicate and attach copy)

**LINE MOUNTAIN SCHOOL DISTRICT
AUTHORIZATION
FOR RELEASE OF HEALTH INFORMATION**

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary.

Plan Participant Name: _____

Social Security Number: _____

Person/Company authorized to
disclose my health information: _____

Person(s)/Organization(s) authorized to
receive health information: _____

Specific description of health
information authorized for release
(include date(s) of service, if
applicable): _____

Purpose of the Disclosure (Please state
the purpose that the information is
being authorized for disclosure, or
"At the request of the individual"):

-
1. I understand that this authorization will expire on: ____ / ____ / ____ or
 2. I understand that I may revoke this authorization at any time by providing written notification to the company/person who is authorized to disclose my information. I understand that if I do revoke the authorization it will not have any affect on any actions taken by this individual/company before receipt of the revocation.
 3. I understand that after this information is disclosed, federal law might not protect it and the recipient might redisclose it.
 4. I understand that I am entitled to receive a copy of this authorization.

Signature of Plan Participant or Plan
Participant's Representative: _____

Date: _____

Printed Name of Plan Participant's
Representative (if applicable): _____

Relationship to Plan Participant: _____

LINE MOUNTAIN SCHOOL DISTRICT

PRIVACY OFFICIAL JOB RESPONSIBILITIES

The Privacy Official is responsible for developing and implementing the privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in connection with the group health plan sponsored by the Employer, developing employee training programs relating to the privacy of group health plan information, publishing and distributing the Notice of Privacy Practices for the group health plan and serving as the designated decision maker for issues and questions involving interpretation of the privacy rules as they relate to the group health plan in coordination with legal counsel as needed. The Privacy Official will be responsible for the following tasks:

1. Inventorying the uses and disclosures of Protected Health Information by the company;
2. Working with management to determine the individuals and classes of individuals who need access to PHI;
3. Implementing a training program;
4. Ensuring that compliance documents are drafted, implemented, and delivered, as applicable. The documents include amendments to plan documents, changes to business associate contracts, Privacy Policy, and the Notice of Privacy Practices;
5. Developing authorizations, complaint forms, logs and other documents to be used to comply with HIPAA's privacy requirements;
6. Establishing and administering the process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the Company's uses and disclosures of Protected Health Information;
7. Developing and implementing procedures for providing plan participants with an accounting, requesting an amendment, accessing, and requesting restrictions on uses and disclosures of Protected Health Information;
8. Maintaining documentation in accordance with the record retention provisions of the Privacy Policy;
9. Notifying or overseeing the notification of individuals, the media and the Department of Health and Human Services of any breach of unsecured PHI, in accordance with the provisions of the HITECH Act;
10. Understanding and advising staff about privacy requirements, minimum necessary uses and disclosures and future changes in laws or regulations related to privacy; and
11. Auditing and monitoring the privacy program.

LINE MOUNTAIN SCHOOL DISTRICT

HIPAA TRAINING DOCUMENTATION

The Employees of Line Mountain School District who have access to protected health information were trained on the HIPAA Privacy Policy. This training included a brief overview of HIPAA and a review of the Privacy Policy.

Date of Training: October 17, 2017

The following employees have been trained:

Printed Name:

Patty Troutman

Joanna Hovenstine

Philip Rapant

Jackie Bonawitz

Signature:

Patty Troutman

Joanna Hovenstine

Philip Rapant

Jackie Bonawitz

BREACH DOCUMENTATION

Breach notification is necessary in all situations except those in which the covered entity or business associate demonstrates that there is a low probability that PHI has been compromised or one of the other exceptions to the definition of “breach” applies.

- The unauthorized acquisition, access, use or disclosure of unsecured protected health information (PHI) is presumed to be a reportable breach (requires notification to the individual, HHS and in some cases the media) unless:
 - The covered entity or business associate demonstrates there is a low probability that the information has been compromised based on a risk assessment of certain factors, or
 - The breach fits within certain exceptions.
- A covered entity or business associate has the discretion to provide the required breach notifications following an impermissible use or disclosure of PHI without performing a risk assessment.
- Following the impermissible use or disclosure of any limited data set, even those that do not include dates of birth and zip codes, covered entities or business associates must notify affected individuals or perform a risk assessment and determine that breach notification is not required.

Use this form or a similar log to document all occurrences of breach.

1. Date of breach:
2. Source of breach:
3. Description of breach:
4. Risk assessment:
 - a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 - b. The unauthorized person who used the PHI or to whom the disclosure was made;
 - c. Whether the PHI was actually acquired or viewed; and
 - d. The extent to which the risk to the PHI has been mitigated.
5. Does the breach constitute an exception under 45 CFR §164.402?
6. Name of person who completed this document and the date it was completed: