LINE MOUNTAIN SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: HIPAA SECURITY – ELECTRONIC COMMUNICATIONS

ADOPTED: March 6, 2018

REVISED:

829. HIPAA SECURITY – ELECTRONIC COMMUNICATIONS

Policy

This policy addresses the compliance issues regarding electronic protected health information ("ePHI") that Line Mountain School District (the "Company") creates, receives, maintains and/or transmits on behalf of its group health plans in accordance with the final HIPAA Security Rule published on February 20, 2003 by the Department of Health and Human Services (HHS).

By implementation of this policy, the Company intends, on behalf of its group health plans, to:

- Ensure the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule.
- Ensure compliance by its workforce.

The policy takes into account the Company's:

- Size, complexity, and capabilities;
- Technical infrastructure, hardware, and software security capabilities;
- Costs of security measures; and
- Probability and criticality of potential risks to electronic protected health information.

This Policy becomes effective as of September 23, 2013.

A. Definitions

1. Electronic PHI or ePHI

   Electronic PHI or ePHI is health information about a group health plan participant that is in an electronic format. Health information includes information about the individual's past, present, or future physical or mental condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual.

2. Final Rule

   The Final Rule is the final HIPAA Security Rule, 45 CFR Parts 160, 162 and 164, published February 20, 2003.

B. Administrative Safeguards

1. Security Management Process §164.308(a)(1)

a. Risk Analysis

The Company has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. The analysis included:

- Security processes (security administration, security monitoring, incident response, and virus detection).
- Physical access to the systems containing ePHI and other critical operations areas.
- Contingency planning.
- Operating system and/or platform configurations.
- Network configurations.
- Data repositories.
- Portal/web architecture.
- Assessment of potential threats.

Based on the risk analysis, the Company has determined that the ePHI that it receives, maintains and transmits is not substantial and is only an incidental part of the work that the Company performs for its clients. Most of this information is received through email transactions with insurance carriers, reinsurance companies and third party administrators. This information is used to secure or renew health insurance coverage or reinsurance coverage or to help settle claim disputes. Because the Company is most often not the originator of this information, there is little risk to the confidentiality, integrity and availability of this information.

The Company will periodically review its risk to determine if the risk has increased or decreased based on the amount and types of ePHI that it creates, receives, maintains and transmits.

b. **Risk Management**

The Company will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, and document identified risks, corrective actions taken and risks considered acceptable.

As appropriate and when necessary, the Security Officer will present all identified risks to management, along with remedial options and associated costs. Security implementation decisions will be documented along with supporting rationale.

c. **Sanctions**

Appropriate sanctions will be taken against employees who fail to comply with this HIPAA Security Policy, and all employees will be made aware of the ramifications of violating this policy. Sanctions will be applied uniformly across the workforce. Factors that may be considered in

determining disciplinary action may include, but are not limited to (1) type and severity of the violation, (2) whether the violation causes any liability or loss to the Company, and (3) the presence of any repeated violation.

2. Assigned Security Responsibility §164.308(a)(2)

The Security Officer's responsibilities include the management and supervision of:

- The use of security measures to protect data
- The conduct of personnel in protecting data

The responsibilities of the Security Officer, which will be included in the Security Officer's Job Description, will be reviewed periodically.

3. Workforce Security §164.308(a)(3)

a. **Authorization**

The Company will ensure that all employees (full-time, part-time, contractors and agents) have appropriate access to ePHI and that those who should not have access are restricted. New employees or employees changing departments will be authorized to access ePHI based on their department assignment.

b. **Workforce Clearance Procedures**

Prior to hiring a new employee, the applicable supervisor will assess the honesty and integrity of the individual and will explain the need for maintaining the confidentiality and integrity of any ePHI maintained by the Company. The Company will only hire an individual if it is determined that the individual poses no threat to the security of the Company's ePHI. Interview records and hiring documents will be maintained to substantiate this process.

c. **Termination Procedures**

Upon an employee's termination from employment, the Security Officer (or other appropriate staff) will:

- Retrieve the following from the individual prior to departure:
  - Keys (for building, filing cabinet, desk, etc.)
  - Computer system passwords
  - Company property such as laptops, cell phones, files, etc.
- Contact a locksmith to change locks, if necessary
- Change security codes, if necessary
- Retrieve pertinent Company files from the individual's hard drive
- Format the individual's hard drive
- Change or delete passwords to computer workstation, network and all email and internet accounts
- If considered necessary, conduct a limited audit of the individual's workstation/password activity prior to and/or

after termination

4. Information Access Management §164.308(a)(4)

a. Access Authorization

Access to ePHI by Company employees will be based on the department to which the employee has been assigned. Authorization will be automatic based on these criteria.

b. Access Establishment and Modification

Password management procedures will ensure the rights each employee has to the appropriate ePHI. Due to the transactional nature of the ePHI maintained by the Company and the fact that there is no need for employees to modify ePHI, the Company will not establish different access rights within a Division. The Company will consider and implement as appropriate "Read Only" access rights to certain ePHI. The Security Officer will review access rights to ePHI on an annual basis or whenever an organizational restructuring occurs.

5. Security Awareness and Training §164.308(a)(5)

The Security Officer will (in conjunction with outside consultants) develop a training program for all members of its workforce to include procedures for guarding against, detecting, and reporting malicious software such as viruses and worms including scanning and incident procedures, procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing, and safeguarding passwords. Training will include an explanation of employees' right to access ePHI, the minimum necessary standard and an explanation of the sanctions that may be imposed.

a. Security Reminders

Security reminders will be sent to employees as needed, but not on a regular basis.

b. Protection from Malicious Software

The Company will install virus detection software on its network and update the software periodically.

c. Log-In Monitoring

The Company will not specifically monitor log-in attempts, but will be aware of this issue as part of its Information System Activity Review. The nature of the ePHI maintained by the Company does not require specific attention to this issue.

d. Password Management

The Company will require employees to change their passwords on a periodic basis, but no more often than once per quarter.

6. Security Incident Procedures §164.308(a)(6)

The Company will address security incidents, which are the

attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The Company will:

- identify and respond to suspected or known security incidents by first notifying the Company's information technology vendor;
- mitigate, to the extent practicable, harmful effects of security incidents that are known to the Company; and
- document security incidents and their outcomes.

All security incidents will be reported to the Security Officer for recording in a Security Incident Log (which will be maintained by the Security Official for 6 years) and if appropriate to the contact person for the group health plan(s) with which the compromised ePHI is associated. The Company's response to the security incident will depend on the extent of the incident and the magnitude of the risk to ePHI.

All employees will be notified of the security incident, if appropriate, and will be told what they should do to respond.

7. Contingency Plan §164.308(a)(7)

The Company will respond to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI. This will include following the steps outlined in:

a. Data Backup Plan

The Company will backup all computer system data on a regular basis. This data will include ePHI. The data backup tapes will not be kept in the company offices, but will be kept at an alternative location as determined by the Company Security Committee.

b. Disaster Recovery Plan

In the event of an emergency or loss of ePHI and Customer Information, the Company will restore its most recent backup tape as soon as reasonably possible. For any ePHI that has been lost as a result of the disaster, the Company will retrieve copies of the information from the original source of the information.

c. Emergency Mode Operations Plan

In the event of an emergency, the Company will not need to re-establish immediate operations. Employees will be able to work from their homes as needed and will have access to ePHI as soon as reasonably possible. There are no critical business processes using ePHI that will be affected by any emergency.

d. Testing and Revision Procedure

The Security Officer will periodically reassess, test and revise as necessary the Company's Contingency Plans.

e. Applications and Data Criticality Analysis

The Company will periodically assess whether the ePHI maintained by the Company has changed so that the Contingency Plan will become more or less critical to the operations of the Company.

8. Evaluation §164.308(a)(8)

The Company will perform a periodic technical and non-technical evaluation, based initially upon these standards and later in response to environmental or operational changes affecting the security of ePHI, including:

- Risk analysis
- Threat assessment
- Operating system and network device security configurations
- Workforce security
- Access controls and authorization to PHI
- Security awareness
- Security incident response
- Physical security
- Transmission security
- Security model (i.e., data classification/ownership)
- Security organizational structure
- Security policies/procedures
- Security architecture and design

9. Business Associates §164.308(b)(1)

These administrative safeguards will also apply to the Company's business associate contracts and other arrangements in which ePHI is handled on the Company's behalf; such agreements will be in a written contract.

A contract between the Company and its business associates will require the business associate to implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on the Company's behalf. The contract will also require the business associate to report to the Company and security incident of which it becomes aware.

C. Physical Safeguards

1. Facility Access Controls §164.310(a)(1)

The Company will limit physical access to its electronic information systems and the facility or facilities in which they are stored, while ensuring that properly authorized access is allowed.

The Company will safeguard the facility and the computer equipment from unauthorized physical access, tampering, and theft.

The Company will document repairs and modifications to the physical components of the building that are related to security (for example, hardware, walls, doors, and locks) and those records will be maintained indefinitely. Records will include:

- Who performs the maintenance;
- Who authorizes the maintenance; and
- Details of the maintenance activities.

2. Workstation Use §164.310(b)

Workstations will be used by each Division to perform the necessary functions and responsibilities of each user. Employees are not permitted to store ePHI on PDA's. This means that emails cannot be synched from the workstation to a PDA.

3. Workstation Security § 164.310(c)

In order to secure the workstations:

- All users will be required to run virus protection check on any new information downloaded from a diskette.
- Workstations will be secured so all workstations that access ePHI restrict access to authorized users.
- Use name and passwords will be required to access any computer workstation or laptop.
- All screens should face away from unauthorized users.
- Password-protected screen-savers will be evoked after a 30-minute period of inactivity.

4. Device and Media Controls §164.310(d)(1)

The Company will further manage ePHI by managing the receipt and removal of hardware and electronic media that contain this information, and the movement of these items within the building. These steps include:

- Media will be sufficiently erased or overwritten before disposal or reuse.
- Additional actions will be taken to destroy media (such as cutting up floppy disks or drilling holes in hard drives, where appropriate).
- Intact workstations may be sold or donated with sufficient erasure of ePHI and Customer Information.
- An inventory will be made and records will be maintained of the movements of all hardware and electronic media and the persons responsible for that media.
- ePHI must be encrypted for transmittal, using Web-based applications such as use of encryption, media on portable devices, and key and certificate management (including issuance, expiration, and revocation).

D. Technical Safeguards

1. Access Controls §164.312(a)(i)

a. Unique User Identification

All Company computer systems users will have a unique user identification that is assigned by individual.

b. Emergency Access Procedure
The Company does not need emergency access procedures.

c. Automatic Logoff
A password protected screensaver will be required on all computers and laptops. A unique name and/or number will be used to identify, authorize and track user identity.

2. Audit Controls §164.312(b)
The Company will implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use ePHI, including auditing, logging, and monitoring controls to allow it to examine system activity, both routinely and as result of a possible security incident. Auditing controls may be manual, automatic, or a combination of both. Examples of audit controls include:
- User access and account activity
- Exception reports
- Dormant account reports
- System resource monitoring
- Data integrity controls
- Failed log-in reports

Monitoring tools (third party, freeware, or OS-provided) may be used to log activity and security violations against ePHI. Examples of security relevant events to monitor might include:
- Users switching user IDs during an on-line session.
- Attempts to guess passwords.
- Attempts to use privileges that have not been authorized.
- Modifications to production application software.
- Modifications to system software.
- Changes to user privileges.
- Changes to logging subsystems including the review of logs as well as standards for log retention and management.

2. Integrity §164.312(c)(1)
The Company will implement electronic means to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. Examples include:
- Error-correcting memory
- Magnetic disk storage with built-in error detection and correction
- Checksums
- Encryption

3. Person or Entity Authentication §164.312(d)
The Company will ensure that a person or entity seeking access to ePHI is the one claimed, and that access should only be granted to those who require it for their jobs.

Authentication is defined as a process utilized by a system to confirm the identity of a user by means of a user identification and password verification scheme.

4. Transmission Security §164.312(e)(1)
   Technical security measures will guard against unauthorized access to or modification of ePHI, and modification of that information that is being transmitted over an electronic communications network.

   These measures will include files transmitted to/from business associates/external entities by FTP, e-mail, dial-up, direct connection, or web access. Measures depending on the level of risk identified during the risk assessment include switched networks, point-to-point connections, digital signatures, SSH, SSL, or other forms of encryption.

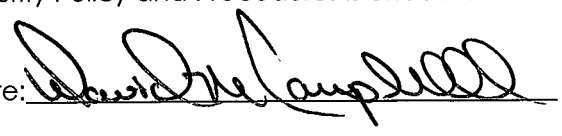
5. Policies and Procedures §164.316(a)
   The Company will implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements, will periodically review and may change our policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the Final Rule.

6. Documentation §164.316(b)(1)
   The Security Officer will document actions, activities and assessments and retain them for 6 years from the date of creation or the date when last in effect, whichever is later.

   The Security Officer or other appropriate Company staff will also retain the system/network configuration documentation, as well as any surrounding policies, procedures and training material for six years from the date of creation or the date last in effect. Such documentation will be made available to those persons responsible for implementing the procedures, including any network and systems administrators, Human Resources, Compliance, and security personnel.

   An update and review of documentation will occur periodically as needed, but could also result from a security incident, new vulnerability, updated systems, changes in personnel, or organizational changes that affect the security of the ePHI in the Company's possession.

This Security Policy and Procedures is effective as of the Effective Date shown above.

Signature: 

Name (print or type): David M. Campbell

Title: Superintendent

Date Signed: March 9, 2018