Adopted: January 25, 2011 *Minnewaska Area Schools Policy 1020*

Revised: *Origin: 2010*

1020 HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA): Personnel Security Policy

Introduction

Minnewaska Area Schools Day Treatment has adopted this Personnel Security Policy to comply with the Health Information Portability and Accountability Act of 1996 ("HIPAA"), the Department of Health and Human Services ("DHHS") security and privacy regulations, and the Joint Commissions on Accreditation of Healthcare Organizations ("JCAHO") accreditation standards, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All personnel of Minnewaska Area Schools Day Treatment must comply with this policy. Familiarity with the personnel security policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

Assumptions

This Personnel Security Policy is based on the following assumptions:

- In any organization, people are the greatest asset in maintaining an effective level of security.
- Likewise, poor personnel security can result in serious breaches of data integrity and confidentiality. Approximately 80 percent of all breaches of confidentiality of health information result from poor personnel security and practices.
- Physical and technical security cannot adequately compensate for poor personnel security.
- Poorly trained, poorly supervised, or dishonest employees can often defeat physical and technical security mechanisms.
- An honest employee is still a security risk if he or she does not know what is expected with regard to security and confidentiality.
- No security program can be effective without maintaining employee awareness and motivation.

Policy

Along with its other policies and procedures protecting the integrity and confidentiality of health information, Minnewaska Area Schools Day Treatment adopts this personnel security policy to ensure that its employees and others who have access to health information are properly screened, properly trained, and properly supervised regarding their access to and use of health information.

Screening of Individuals with Access to Individually Identifiable Health Information

- HIPAA and the DHHS security regulations require “appropriate clearances” for all personnel with access to individually identifiable health information. The regulations do not, however, specify what appropriate clearances consist of. Rather, they leave it up to covered entities to determine what screening is appropriate based on a risk analysis, defined as the process of selecting cost-effective security/control measures by balancing the cost of those measures against the harm that would occur if those measures were not in place.
- Thus, each department director is responsible for screening all employees and others with access to individually identifiable health information. An appropriate clearance may include, among others, the following elements:
  - Criminal background check.
  - Credit check.
  - Verification of references.
  - Verification of employment history.
  - Verification of licensure and/or certification.
  - In-depth interview.
  - Drug testing (coordinate with human resources and the legal department to ensure that such testing is legal and proper).
  - Clauses in vendor contracts, such as for computer system maintenance technicians, that requires the vendor to screen employees with access to our system and data.
  - Agreements with other entities requiring them to screen personnel with access to our system and data. For example, a nursing school could be required to certify that it would not send any nursing students to our facility for training unless it believed they could be trusted with confidential medical information.
  - Self-certification in the employment application. If approved by human resources and the legal department, such documents could ask applicants to certify that they do not have felony convictions or any convictions involving dishonesty and know of no reason why they could not be trusted with confidential health information.
- Department directors will determine what screening is appropriate for its personnel with access to confidential health information by considering the risk and then balancing the cost of the security measure against the risk. Factors to consider when evaluating the risk include the following:
  - Background of the class of employee (average age, educational experience, specialized training, licensure or certification, and the like). For example, a licensed individual may have undergone screening to be licensed that might lessen the screening required for access to our data.
  - Level of access of the class of employee or of the particular employee. An individual who has access to the entire system or to a file server poses a greater risk than one who can log in at only one workstation and who does not have access to all data.
  - Nature of the data user’s duties. Access to particularly sensitive medical data, such as information regarding AIDS/HIV, mental health, alcohol and drug abuse, sexually transmitted diseases, and the like, or to financial information, may pose greater risks than access to more routine matters, such as scheduling.
  - History of data users in that department. For example, if three employees had breached confidentiality in the past two years, two of them had sold patient information to finance

a drug habit, and two had had a past criminal record, the screening inherent in the application for employment process is obviously not sufficient for that department.

- Directors may "grandfather" (not conduct a further screening of) employees and others with access if the data user has had no breaches of confidentiality in the last three years. Directors may submit written requests to grandfather other individuals in writing to the [facility security officer] [other].
- The physician credentialing process constitutes sufficient screening for access to patient information.
- Directors will submit their standards for screening data users to the [facility security officer] [other] no later than _____. Upon approval, they will institute the screening procedures detailed therein. The [facility security officer] [other] will keep records of standards for not less than six years from their effective date.
- Directors will retain records of screening for not less than six years from the completion of the screening.

Training

HIPAA and the DHHS security and privacy regulations require training all personnel with access to individually identifiable health information. Training is an integral part of personnel security. All supervisors are responsible for training personnel with access to health information as required by Minnewaska Area Schools Day Treatment's training policy.

Supervision

Properly screening and training personnel with access to individually identifiable health information is not enough. Employees and others with access must be continually reminded of their responsibilities concerning protection of health information. Therefore, supervisors must take the following steps:

- Detail security and confidentiality requirements in position descriptions and performance evaluations. Adherence to security and confidentiality policies must be part of every data user's performance evaluation process.
- Monitor the day-to-day performance of data users to detect problems with security and confidentiality before they become serious breaches.
- Audit compliance with security and confidentiality policies in accordance with the Minnewaska Area Schools Day Treatment's Information Audit Policy.
- Report breaches of security or confidentiality in accordance with the Minnewaska Area Schools Day Treatment's Report Procedure.
- Respond to breaches of security or confidentiality in accordance with the Minnewaska Area Schools Day Treatment's Response Procedure.
- Commend data users demonstrating a high degree of proficiency in protecting data integrity and confidentiality.
- Take appropriate sanctions against data users who breach security/confidentiality in accordance with Minnewaska Area Schools Day Treatment's sanction policy.

Enforcement

All officers, agents, and employees of Minnewaska Area Schools Day Treatment **must** adhere to this policy, and all supervisors are responsible for enforcing this policy. Minnewaska Area Schools Day Treatment will not tolerate violations of this policy. Violation of this policy is grounds for disciplinary action, up to and including termination of employment and criminal or professional sanctions in accordance with Minnewaska Area Schools Day Treatment's medical information sanction policy and personnel rules and regulations.

_____	_____
Signature of Officer, Agent, or Employee	Date
_____	_____
Title of Officer, Agent, or Employee	Printed Name of Officer, Agent, or Employee
_____	_____
Witness	Printed Name of Witness