Adopted: January 25, 2011 *Minnewaska Area Schools Policy 1026*
Revised:_____ *Origin: 2010*

1026 HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA): Response Procedure Policy

Introduction

Minnewaska Area Schools Day Treatment has adopted this Response Procedure Policy to comply with the Health Information Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), Subtitle D—Privacy, the Department of Health and Human Services ("DHHS") security and privacy regulations, and the Joint Commission on Accreditation of Healthcare Organizations 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. In addition, this Response Procedure Policy will assist Minnewaska Area Schools Day Treatment in fulfilling its obligation under the DHHS privacy regulations to mitigate damages caused by breach of individual privacy. All personnel of Minnewaska Area Schools Day Treatment must comply with this policy. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

Assumptions

This Response Procedure Policy is based on the following assumptions:

- Breaches of security, confidentiality, or Minnewaska Area Schools Day Treatment's policies and procedures may occur despite security and confidentiality protections.
- Early detection and response to such breaches is critical to stop any such breach, correct the problem, and mitigate any harm.
- In appropriate cases, a thorough investigation is necessary to assess the breach, mitigate any harm, determine how to prevent recurrence, and provide a basis for any necessary disciplinary action.
- Minnewaska Area Schools Day Treatment has a duty to mitigate the harm of a breach and, in some cases, has a duty to notify the subject of the breach, DHHS, and the media.
- Other federal and state laws, such as the Red Flag Rules, may also require notification and/or mitigation.

Policy

- The purpose of responding to, investigating, mitigating, and reporting health information breaches and suspected breaches is as follows:
  - Minimize the frequency and severity of incidents.
  - Provide for early assessment and investigation before crucial evidence is gone.
  - Quickly take remedial actions to stop the breaches, correct the problems, and mitigate damages.
  - Implement measures to prevent recurrence of incidents.

  - Facilitate effective disciplinary actions against offenders.
  - Properly make required notifications.
- Individuals detecting or suspecting a breach of health information security or confidentiality must report the breach or suspected breach as specified therein, including a written report to the security officer [other] as soon as possible as specified in Minnewaska Area Schools Day Treatment's Report Procedure Policy.
- Upon receiving the report, the security officer [other] will take the following steps:
  - Take any necessary immediate corrective action.
  - If the breach appears to involve gross negligence, willful misconduct, or criminal activity of a person or persons holding access privileges, immediately, in conjunction with the system administrator, suspend that person(s) access pending investigation, including taking all necessary steps to prevent access (removal of user accounts, recovery of keys, and so forth).
  - Provide copies of the report with an endorsement as to any corrective action taken, including suspensions of access, and recommendations for future action to all the following people and departments:
    - Facility administrator.
    - Director information systems[1[1]]
    - Legal department.
    - Risk management.
    - Quality assurance.
    - Human resources.
    - Health information management.
    - Privacy officer.[2[2]]
    - Concerned department directors.
    - Others _____.
- The facility administrator may appoint an investigating officer, which may be the security officer, to conduct an investigation in appropriate cases. Factors to consider in determining whether an investigation is necessary include the following:
  - Seriousness of the breach.
  - Whether the breach involved unsecured (readable) or secured (not readable—that is, encrypted) data.
  - Whether the breach resulted in actual harm.
  - Extent of any harm.
  - Whether the breach has the potential for legal liability.
  - Whether the breach involved gross negligence, willful misconduct, or criminal activity.
  - Whether the breach put patient or other individuals' welfare at risk.
  - Whether there has been a series of similar or related breaches.
  - Whether the suspected offender has committed other breaches.
  - Whether the breach must be reported to the individual who is the subject of the breach, to DHHS, or to the media.
- The investigating officer will conduct a thorough investigation into all the facts and circumstances of the breach or suspected breach and will provide the facility administrator a

[1[1]] If not also the security officer.
[2[2]] If not also the security officer.

detailed report of the facts and circumstances of the breach, including recommendations for corrective and/or disciplinary action.

- All Minnewaska Area Schools Day Treatment personnel will cooperate with any such investigation. Failure to cooperate, failure to furnish required information, or furnishing false information may result in employee discipline up to and including termination under Minnewaska Area Schools Day Treatment's sanction policy. Department directors will ensure that the investigating officer has access to necessary persons and information to conduct a through investigation.
- The investigation shall include a risk analysis of the breach, including, but not limited to, answering the following questions:
  - Who was involved?
  - How many patients/others' information was breached?
  - Did the perpetrator simply improperly access the data or copy, change, or transfer the data?
  - When did the breach happen?
  - What are the risks to the subject(s) of the breach—financial, embarrassment, loss of job, and so forth?
  - What was the motive for the breach if not accidental?
  - Does a potential for further harm exist?
  - What can Minnewaska Area Schools Day Treatment do to eliminate/limit further damage?
  - What steps can Minnewaska Area Schools Day Treatment do to prevent this type of breach in the future?
- The legal department will review the report and its recommendations for legal sufficiency.
- The facility administrator, the security officer, the investigating officer, the legal department, and other appropriate personnel will discuss the report and recommendations and decide on appropriate action to prevent recurrence of the breach, mitigate any harm caused by the breach, and take necessary disciplinary action in accordance with Minnewaska Area Schools Day Treatment's sanction policy.
- The director of information systems will keep all such reports for not less than 6 years from the date of the report.
- No such report will be made a part of a patient's medical record. The report is a risk management tool, not a patient care document.
- If the breach qualifies as a breach under the HITECH Act definition of breach in Subtitle D—Privacy, Part I, § 13400, the data is unsecured, and the breach poses a significant risk to the affected individuals, Minnewaska Area Schools Day Treatment must, without unreasonable delay and in no case later than 60 days after the discovery of the breach, notify the individual(s) whose PHI was involved in the breach.
- The notice must include the following:
  - Description of the types of unsecured PHI that were involved in the breach (such as name, Social Security number, patient number, insurance number, date of birth, home address, disability code, and the like).
  - Brief description of what Minnewaska Area Schools Day Treatment is doing to investigate the breach, to mitigate losses, and to protect against further breaches.

    - Contact information for individuals to ask questions or learn additional information, which will include a toll-free telephone number, [an email address,][our web site], or our postal address. The privacy officer shall respond to all such contacts.
- Unless the contact information is insufficient or out-of-date, the notification shall be by first-class mail to the individual or next-of-kin of the individual or, if specified as a preference by the individual, by email.
- If the contact information is insufficient or out-of-date, [name of entity] will use a substitute form of notice, such as, if the breach involves 10 or more individuals for which there is insufficient or out-of-date information, a conspicuous posting on the home page of [name of entity]'s website or notice in major print or broadcast media in geographic areas in which the individuals affected by the breach likely reside as determined by the privacy officer in conjunction with legal and risk management. Such notice will include a toll-free number where the individual can learn whether the individual's unsecured PHI was possibly involved in the breach.
- If the security officer, in consultation with the privacy officer [risk management] [legal] determines that the breach requires urgency because of the possible imminent release of unsecured PHI, immediate notification may also be made by telephone or other appropriate means.
- If the breach involves 500 or more individuals' PHI, Minnewaska Area Schools Day Treatment will provide notice to prominent media outlets in the state or jurisdiction of the individuals and immediately to DHHS. The privacy officer is responsible for reporting breaches of fewer than 500 individuals to DHHS in the form of a log not later than 60 days from the end of the calendar year. These notifications may be delayed if law enforcement represents that the notification will impede a criminal investigation or damage national security.

Enforcement

All officers, agents, and employees of [name of covered entity] **must** adhere to this policy, and all supervisors are responsible for enforcing this policy. [Name of covered entity] 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 [name of covered entity]'s medical information sanction policy and personnel rules and regulations.

_____	_____
Signature of User	Date
_____	_____
Title of User	Printed Name of User
_____	_____
Witness	Printed Name of Witness