Adopted: January 25, 2011 *Minnewaska Area Schools Policy 1012*

Revised: *Origin: 2010*

1012 HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

Workstation Use Policy

Introduction

Minnewaska Area Schools Day Treatment has adopted this Policy on Workstation Use to comply with the Health Information Portability and Accountability Act of 1996 ("HIPAA"), the Department of Health and Human Services ("DHHS") security and privacy regulation's requirement for such a policy, with the Joint Commission 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 and all covered entity personnel that use computer terminals must be familiar with the contents of this policy and follow its guidance, as appropriate, when using computer equipment. Familiarity with the plan and demonstrated competence in the requirements of the plan are an important part of every Minnewaska Area Schools Day Treatment employee's responsibilities.

Assumptions

This Workstation Use Policy is based on the following assumptions:

- Every computer workstation in the covered entity is vulnerable to environmental threats, such as fire, water damage, power surge, and the like.
- Any computer workstation in the covered entity can access confidential patient information if the user has the proper authorization.
- All computer screens may be viewed by individuals who do not have access to confidential information that may be displayed on the screen.

Preventative Measures

- All computer users will monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. For example, if air conditioning fails, so that the temperature around the computer may exceed a safe level, the user must immediately notify maintenance.
- All computers plugged into an electrical power outlet will use a surge suppresser approved by the director of information systems.
- All personnel using computers will familiarize themselves with and comply with the covered entity's disaster plans and take appropriate measures to protect computers and data from disasters.

- Personnel using computers will not smoke at or near the terminal nor eat or drink at the terminal to prevent damage due to spills and so forth.
- Personnel logging onto the system will ensure that no one observes them entering their password.
- After three failed attempts to log on, the system will refuse to permit access and generate a notice to the system administrator.
- Personnel will not log onto the system using another's password nor permit another to log on with their password. Nor will personnel enter data under another person's password.
- Each person using the covered entity's computers is responsible for the content of any that data he or she inputs into the computer or transmits through or outside the covered entity's system. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message. All personnel will familiarize themselves with and comply with the covered entity's email policy.
- No employee may access any confidential patient or other information that they do not have a need to know. No employee may disclose confidential patient or other information unless properly authorized (see the Confidentiality Policy and the Disclosure Policy).
- Employees must not leave printers unattended when they are printing confidential patient or other information. This rule is especially important when two or more computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer.
- Employees may not use the covered entity's system to solicit for outside business ventures, organizational campaigns, political activities, or religious causes. Nor may they enter, transmit, or maintain communications of a discriminatory or harassing nature or materials that are obscene or x-rated. No person shall enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall enter, maintain, or transmit any abusive, profane or offensive language.
- Personnel using the computer system will not write down their password and put it at or near the terminal, such as by putting the password on a yellow "stickie" on the screen or a piece of tape under the keyboard.
- Each computer will be programmed to generate a screen saver when the computer receives no input for a specified period. Supervisors may specify an appropriate period to protect confidentiality while keeping the computer available for use.
- Personnel must log off the system if they leave the computer terminal for any period of time. Exceptions to this policy where medically necessary must be approved in writing by the director of mental health services.
- The director of mental health services must develop a policy on hard-copy printouts, including who may generate such printouts, what may be done with the printouts, how to dispose of the printouts, and how to maintain confidentiality of hard-copy printouts. No personnel may download data from the covered entity's system without the express permission of the director of mental health services.
- No personnel may upload any unauthorized software or data. The director of information systems must approve any software or data that an employee wishes to upload. This rule is necessary to protect against computer viruses from being transmitted into the covered entity's system.

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.

Portions of this Policy on Workstation Use were adapted from Arthur D. Rutkowski, & Barbara Lang Tuttkowski, "Model Company Systems User Policy," 13 *Employment Law Update* 5 (Feb. 1998).