Effective Date: April 24, 2003, Motion #03-013; April 14, 2003
Revised Date: 5/31/13
Review Date: 6/13/13

North Sound Mental Health Administration

Section 2500 – Privacy: Safeguarding Protected Health Information (PHI)

Authorizing Source: RCW 70.02; 45 CFR 165 (HIPAA)
Cancels:
See Also:
Providers must have own "HIPAA & WAC compliant policy" | Approved by: Executive Director | Date: 7/17/2013
Responsible Staff: Privacy Officer | Signature:

POLICY #2519.00

SUBJECT: SAFEGUARDING PROTECTED HEALTH INFORMATION (PHI)

PURPOSE

The North Sound Mental Health Administration (NSMHA), in compliance with the Privacy Rules of Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification provisions, sets out in this policy the requirements for safeguarding Protected Health Information (PHI) in all media, safeguarding PHI through audit controls and internal auditing, safeguarding PHI by assuring that PHI is going to, or coming from, the appropriate person or entity and that the data being processed or transmitted has not been modified intentionally or inadvertently, as well as the requirements for safeguarding PHI by controlling access to our facilities and electronic systems.

POLICY

NSMHA will assign responsibility for all safeguarding matters to a Security Officer. This position will be responsible for assuring that all PHI whether in oral, written, or electronic form is reasonably secure from accidental or intentional uses and disclosures that violate the Privacy Rules, and from inadvertent disclosures to other than the intended recipient.

The Security Officer will maintain the Policies and Procedures, for all media, around security measures to protect PHI.

The Security Officer will also be responsible for monitoring the appropriate and consistent implementation of the policies and procedures that control the conduct of the workforce, subcontractors, and Business Associates with regard to the protection of data. The Security Officer will assure that breaches of security are investigated and that members of the workforce who are responsible for those breaches will be subject to the appropriate sanctions. In addition, the Security Officer will assure that any systemic weakness uncovered during such investigations will be corrected.

NSMHA will establish and maintain ongoing processes to review records of systems activity, such as log-ins, access to files, and security incidents, for PHI in all media. We will establish documented procedures for auditing this information for the purpose of identifying security breaches and for assuring that users comply with access controls. We will assign specific individuals or job functions that will be responsible for such internal audit activity.

We will also establish audit controls that will define users, data sources, data accessed, the client, the date and time of the access, and other information we consider appropriate.

We will also establish procedures to audit configuration management practices that have been established to assure that changes to hardware and software systems do not contribute to, or create security weaknesses.

Access to audit logs will be limited to those assigned to the internal audit and control function as described above.

NSMHA will create and maintain procedures directed toward the behavior of our workforce that promote an environment for PHI that is reasonably secure from accidental, intentional, or inadvertent disclosures that violate the Privacy Rule.

It will be our policy to create and maintain guidelines on workstation use that are documented. These guidelines will address:

1. The proper functions to be performed;
2. The manner in which those functions are to be performed – the documentation of the actual function and how it is to be performed; and
3. The attributes of the physical environment in which the workstations, including laptops and other portable devices, are to be located. These attributes will vary based on the sensitivity of information that typically is accessed from that environment. Attributes include such things as physical access to the workstation itself and to the area it is located in, the removable media, such as diskettes, CD-ROMs, etc., and the practices around writing down passwords where others can find/use them.

The Security Officer will oversee this process and assure that the workforce is trained on these guidelines prior to being given access to the system.

It will be our policy to provide security awareness training to all members of the workforce and to any independent contractors who have access to our workplace and systems. Awareness training will be directed at all of these individuals, regardless of their roles or access to PHI – its purpose will be to provide education around such things as: password maintenance, security incident reporting, and virus and other forms of destructive software. Awareness training will also be accomplished by periodic environmental reminders such as: screen savers, posters, etc. The Security Officer will oversee the development of awareness training in conjunction with Human Resources.

It will also be our policy to provide training to all users of electronic systems. User training will be required prior to any user receiving access to the system. User training will focus specifically on the actual usage of security features such as: virus protection practices, addition of unauthorized hardware or software to the system, password management, login practices, automatic logoffs, etc. The Security Officer will oversee the development of awareness training in conjunction with Human Resources.

We will establish procedures in conjunction with Human Resources for terminated workforce members and for members of the workforce whose positions and work assignments have changed. These procedures will cover security for PHI in all media. We will address:

1. Physical access combinations – for locks and alarm systems;
2. Removal of access privileges – both general access and user levels of access; and
3. The collection of keys, tokens, or other objects that allow access.

NSMHA will create and maintain procedures to safeguard all of our locations from unauthorized physical access, and to safeguard hardware and other equipment from unauthorized physical access, theft, and interference.

We will limit and control physical access to any and all parts of the designated record set. Our paper medical record files will be placed in limited access spaces and access to those records will be controlled by appropriate staff.

Electronic files will be subject to access controls that will limit user access to that PHI for which they have clearance. (*See* "Minimum Necessary Policy and Procedures.") Controls for access to non-PHI data will be established and maintained in accordance with context-, role-, or user-based criteria. These controls will include a process for setting criteria for granting access and for modification of the criteria.

Our systems will maintain an access authorization record to document and review the level of access granted to a user, program, or procedure.

We will assure that systems maintenance personnel have proper access authorization. We will not transmit PHI over the Internet (open network) without some form of encryption intended to limit access to information.

NSMHA will establish and maintain procedures for assuring that recipients of PHI via electronic or other means are the intended recipients.

We will also establish and maintain procedures for data authentication. These procedures will assure that PHI contained in messages or files has not been altered or modified.

Documentation retention requirements include:

1. Policies and procedures for personnel
2. Personnel assignments
3. Policies and procedures for audit controls and internal audit
4. Policies and procedures for audit controls and internal audit
5. Policies and procedures for data and entity authentication

Other policies and procedures to review that are related to this policy:

1. Administrative requirements – Documentation
2. Designated Record Set
3. Administrative requirements – Training
4. Minimum Necessary
5. Administrative safeguards – Access Controls
6. Administrative Safeguards – Data and Entity Authentication

ATTACHMENTS

None