Effective Date: 6/28/2005
Revised Date:
Review Date:

North Sound Mental Health Administration

Section 4000 – Information Systems: Privacy and Security Plan

Authorizing Source:
Cancels:
See Also: Approved by: Executive Director Date: 6/28/2005
Responsible Staff: IS Specialist Motion #:

POLICY #4009.00

SUBJECT: PRIVACY AND SECURITY PLAN

BACKGROUND

The use of computers and computer networks has become an integral part of the behavioral health and human services industry. These technologies have brought and will continue to bring enormous advantages to our industry and will continue to enable us to innovate in the means of delivering service to consumers. These technologies have also brought significant risks regarding consumer confidentiality and privacy. Many organizations have opted to establish security and privacy policies that give specific guidelines on an employee's use of these technologies, in all locations. The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require that such policies be established, enforced, and audited.

POLICY

It is the policy of NSMHA that all employees must preserve the integrity and the confidentiality of health and other sensitive information pertaining to our consumers. The purpose of this policy is to ensure that NSMHA employees have the necessary information to carry out its responsibilities while protecting the confidentiality of consumer information. To that end, NSMHA employees will:

1. Collect and use protected health information only for the purposes of supporting the delivery, payment, integrity, and quality of mental health services. NSMHA employees and agents will not use or supply protected health information for non-health care uses, such as direct marketing, employment, or credit evaluation processes.
2. Collect and use individual health information only:

    a. As a basis for required reporting of health information.
    b. To receive reimbursement for services provided.
    c. For research and similar purposes designed to improve the quality and to reduce the cost of health care.

3. Recognize that protected health information collected about consumers must be accurate, timely, complete, and available when needed. NSMHA employees will:

    a. Use their best efforts to ensure the accuracy, timeliness, and completeness of data to ensure that authorized personnel can access it when needed.
    b. Maintain records for the retention periods required by law and professional standards.
    c. Implement reasonable measures to protect the integrity of all data maintained about consumers.
    d. Recognize that consumers have a right of privacy. NSMHA employees will respect consumers' individual dignity at all times. NSMHA employees will respect consumers' privacy to the

extent consistent with providing the highest quality health care possible and with the efficient administration of the facility.

4. Act as responsible information stewards and treats all consumer data and related financial, demographic, and lifestyle information as sensitive and confidential. Consequently, NSMHA employees will:

    a. Treat all consumer data as confidential in accordance with professional ethics and legal requirements.
    b. Not divulge protected health information unless the consumer (or his or her personal representative) has properly authorized the disclosure or the disclosure is otherwise authorized by law.
    c. When releasing protected health information, take appropriate steps to prevent unauthorized re-disclosures, such as specifying that the recipient may not further disclose the information without consumer authorization or as allowed by law.
    d. Implement reasonable measures to protect the confidentiality of information maintained about consumers.
    e. Remove consumer identifiers when appropriate, such as in statistical reporting and in research studies.
    f. Not disclose financial or other consumer information except as necessary for billing or authorized purposes as authorized by law and professional standards.

5. Recognize that mental health information is particularly sensitive, as is HIV/AIDS information, developmental disability information, alcohol and drug abuse information, and other information about sexually transmitted or communicable diseases and that disclosure of such information could severely harm consumers, such as by causing loss of employment opportunities and insurance coverage, as well as the pain of social stigma. Consequently, NSMHA employees will treat such information with additional confidentiality protections as required by law, professional ethics, and accreditation requirements.
6. All employees of NSMHA must adhere to this policy. NSMHA must adhere to this policy. NSMHA 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 NSMHA clinical information sanction policy and personnel rules and regulations.

a. <u>Reporting Security Problems</u>

i. If sensitive NSMHA information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, Privacy Officer must be notified immediately.
ii. If any unauthorized use of NSMHA's information systems has taken place, or is suspected of taking place, the Security Officer and Privacy Officer must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Security Officer and Privacy Officer must be notified immediately.

b. Additional Responsibilities

As defined below, NSMHA employees responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

i. IS/IT Department will establish an Internet security infrastructure consisting of hardware, software, policies, and standards, and department staff will provide technical guidance on PC security to all NSMHA staff. The IS/IT Department will respond to virus infestations, hacker intrusions, and similar events.
ii. IS/IT staff will monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Program directors must ensure that their staffs are in compliance with the Internet security policy established in this document. IS/IT staff will also provide administrative support and technical guidance to management on matters related to Internet security.
iii. IS/IT staff will periodically, and no less than annually, conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.
iv. IS/IT staff will check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
v. IS/IT staff will check that user access controls are defined on these systems in a manner consistent with the need-to-know.
vi. NSMHA information owners will see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in house sensitivity classifications.
vii. NSMHA managers will ensure that:

a) Employees under their supervision implement security measures as defined in this document.
b) Employees under their supervision delete sensitive (confidential) data from floppy disks when the data is no longer needed or useful.
c) Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all NSMHA documents that address information security.
d) Employees and contract personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.

viii. Users of NSMHA Internet connections must:

a) Know and apply the appropriate NSMHA policies and practices pertaining to Internet security.
b) Not permit any unauthorized individual to obtain access to NSMHA Internet connections.
c) Not use or permit the use of any unauthorized device in connection with NSMHA personal computers.
d) Not use NSMHA Internet resources (software/hardware or data) for other than authorized company purposes.
e) Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.

f) Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess. (See Access Codes and Password policy)
g) Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
h) Report to the IS Specialist any incident that appears to compromise the security of NSMHA information resources. These include missing data, virus infestations, and unexplained transactions.
i) Access only the data and automated functions for which he/she is authorized in the course of normal business activity.

c. <u>Contact Point</u>
Questions about this policy may be directed to the Security Officer.

d. <u>Disciplinary Process</u>
Violation of these policies may subject employees or contractors to disciplinary procedures up to an including termination.

ATTACHMENTS
None