Effective Date: April 14, 2003, Motion #03-013
Revised Date: 5/31/2013
Review Date: 6/13/2013

North Sound Mental Health Administration
Section 2500 – Privacy: Confidentiality

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 #2507.00

SUBJECT: CONFIDENTIALITY

PURPOSE
To establish guidelines for the protection of confidential Protected Health Information (PHI) in compliance with state law and federal confidentiality and privacy rules.

BACKGROUND:
In its designated role as the local mental health authority, the North Sound Mental Health Administration (NSMHA) has multiple responsibilities mandated by state statute [*see* RCW 71.24.300]. The authority to gain access to PHI and/or treatment records in order to fulfill these responsibilities/duties is also granted by state statute [*see* RCW 71.05.390, RCW 71.05.630 (2)(a)(b)(e), RCW 70.02.050 (1)(b)(h), RCW 71.34.200 (6)(10)]. The privilege granted by these laws, however, carries with it a commensurate amount of responsibility for assuring that the information obtained by NSMHA in the performance of its duties is protected against further disclosure to unauthorized organizations and/or individuals.

NSMHA is acutely aware that mental illness continues to be a category of illness that may subject a person seeking services or receiving a diagnosis to discrimination and other disadvantages. It is also understood that with the growth of managed care and the increase in the amount and sensitivity of information made available to third-party payers/reviewers, there may be a corresponding decrease on the part of some individuals in their inclination or desire to seek treatment. The goal of NSMHA is to adopt policies that will assure consumers that confidentiality protections are strong and will protect their privacy within State and Federal laws.

POLICY
NSMHA, its employees, and its contracting agencies and their employees shall protect all information, records and data from unauthorized disclosure in accordance with:

1. **42 CFR 432.300 - 431.307 (Federal Statute)** - "State Organization and General Administration," "Safeguarding Information on Applicants and Recipients"
2. **RCW 70.02** - "Medical Records – Health Care Information Access and Disclosure" [RCW 70.02.020 – 70.02.060]
3. **RCW 71.05** - "Mental Illness" [RCW 71.05.325, 71.05.330, 71.05.390, 71.05.395, 71.05.400, 71.05.410, 71.05.420, 71.05.440, 7l.05.445, 1.05.610 – 71.05.680]
4. **RCW 71.34** - "Mental Health Services For Minors" [RCW 71.34.025, 71.34.100, 71.34.200, 71.34.210, 71.34.220, 71.34.225]
5. **WAC 388-865-0115 –** "Access to Clinical Records"
6. **45 CFR** The "Health Insurance Portability and Accountability Act of 1996" (HIPAA)

and

For service recipients receiving alcohol and drug abuse services, in accordance with:

42 CFR Part 2 (Federal Statute) – "Confidentiality of Alcohol and Drug Abuse Patient Records"

[Any program that specializes in the treatment, diagnosis, referring, or prevention of alcohol and drug abuse and receives direct or indirect federal financial assistance must comply with 42 CFR Part 2. A Mental Illness and Chemical Abuse program (MICA) program located in a mental health agency would be subject to 42 CFR Part 2. A mental health agency that does ***not*** specialize in alcohol and drug abuse services is ***not*** subject to 42 CFR Part 2. On the other hand, if a mental health agency enters into a Qualified Service Organization Agreement (QSOA) with an agency providing substance abuse services, the mental health agency must promise, in writing, to abide by the federal confidentiality regulations for information related to those clients covered under the QSOA. Additionally, if mental health staff participate in a case review group for substance abuse clients, the members of the group are subject to 42 CFR Part 2.]

Note: In considering issues related to confidentiality, it is important to note that any state provision that would permit or require a disclosure prohibited by the federal rules is invalid. If, however, a state statute is more stringent than a federal rule, the state statute prevails.

NSMHA will obtain a signed authorization that meets the standards of the Privacy Rules from individuals prior to using or disclosing PHI in those situations, for those uses that are not otherwise permitted or required under the Rule. A copy of the authorization form presently in use at NSMHA is attached to the Authorization policy.

Any NSMHA employee who is contemplating the disclosure of PHI without the consumer's authorization for those uses that are not otherwise permitted or required under the Rule must first consult with his or her supervisor, the Privacy Officer and/or a member of NSMHA Leadership Team. Additional consultation with legal counsel may also be required, but a decision to do so will be at the discretion of NSMHA Executive Director.

Employee Oath of Confidentiality:
All NSMHA employees shall sign an annual Oath of Confidentiality statement. This statement will affirm that the employee will not make unauthorized disclosures of any information they may acquire in the performance of their duties as an employee of NSMHA. The employee shall acknowledge that she/he has read all policies related to confidentiality and privacy and that she/he understands that violation of this policy, the Oath, or any state or federal regulation may be cause for discipline, including dismissal.

PHI protected from unauthorized use and/or disclosure includes any information acquired about a patient, whether or not it is in writing or recorded in some other form, including the patient's identity, address, medical or treatment information, and all communications made by him or her to program staff. PHI also means any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

All disclosures, and especially those made pursuant to an authorization form, must be limited to information that is the ***minimum necessary*** to accomplish the need or purpose for the disclosure. It would be improper to disclose everything in a patient's file if the recipient of the information only needs one specific piece of information. In completing an authorization form, it is, therefore, important to determine first, the purpose or need for the communication of information. Once this has been identified, it is easier to determine how much and what kind of information will be disclosed, tailoring it to what is essential to accomplish the need or purpose that has been identified. A general guideline for disclosure of confidential information is to disclose, only what is the ***minimum necessary***, for only as long as is necessary, in light of the purpose of the communication.

Any minor thirteen years of age or older may request and receive outpatient mental health [RCW 71.34.030] or chemical dependency [RCW 70.96A.095] treatment without the consent of the minor's parent. If parental consent was not required for treatment, parental authorization is not required to make disclosures. Parental consent is required for any treatment of a minor under the age of thirteen. If parental consent was required for treatment, parental authorization is also required to make disclosures.

Information about applicants for service, whether or not they are admitted to treatment, former consumers, and deceased consumers is protected from disclosure without proper authorization.

Disclosure of records related to alcohol or drug abuse services:
Except under certain specified conditions, Federal law [i.e., 42 CFR Part 2 ("Confidentiality of Alcohol and Drug Abuse Patient Records")] prohibits the disclosure of records or other information concerning any consumer in a federally assisted alcohol or drug abuse program. Any state laws that permit or require a disclosure prohibited by the federal law are invalid. A general medical release form or any consent form that does not contain all of the elements specified in 42 CFR Part 2, § 2.31 ("Form of Written Consent") is not acceptable. Each disclosure made with the consumer's written consent must be accompanied by a written statement about prohibition of re-disclosure as outlined in 42 CFR Part 2, § 2.32 ("Prohibition on Redisclosure").

Disclosure to the Department of Corrections:
Consumer consent is not required for release of relevant records regarding inmates of correctional institutions from mental health service providers to the Washington State Department of Corrections (DOC) when such information is necessary to carry out DOC responsibilities, as authorized in RCW 71.05.445 and 71.34.225 (WAC 388-865-0600). Relevant records (specifically defined under WAC 388-865-0610) include agency records and reports, except where prohibited by federal laws or regulations. For purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release or is no longer in lawful custody.

Written requests from DOC personnel must include the purpose for which information is intended, proper identification of the person to whom records are to be sent, specifics regarding what relevant information is requested, and the name, title, date, and signature of the requester (WAC 388-865-0640). The scope of the information is dependent on the reason for the request (WAC 388-865-0620), and must be provided to the DOC within the specified time frames (WAC 388-865-0630).

Disclosure of testing or treatment for HIV or other sexually transmitted diseases:
Release of information related to testing or treatment of sexually transmitted diseases must be ***specifically authorized*** in accordance with RCW 70.24.105.

Disclosure to Family Members:

It is the policy of NSMHA to promote the involvement of family members in the treatment of consumers of all ages, whenever possible. This is particularly important when family members are in the role of primary caretaker for the consumer. Families need information about illness management, medications and their side effects, and other areas of information that are relevant to providing knowledgeable care giving and support.

Nevertheless, the intent is not to promote family involvement at the expense of the consumer's right to privacy. Kinship does not grant family members an exemption from the laws governing the release of PHI. Consumers thirteen years of age and older must give authorization before PHI can be shared with their family members. Parental consent/authorization is required for outpatient treatment of a minor under the age of thirteen; therefore, parents/guardians have the right to access PHI about the minor.

Disclosure to Protect Third Parties:

1. **Mandatory Reporting of Child and Vulnerable Adult Abuse and/or Neglect:**
   Social service/mental health personnel [as defined in RCW 26.44.020(8) and RCW 74.34.020(8)] are **required** by Washington State law to report suspected incidents of abuse and neglect of children [RCW 26.44.030 (1)] and vulnerable adults [RCW 74.34 035 (1)]. In doing so, they have civil immunity under the law for good faith reporting [RCW 26.44.060 (1)(a); RCW 74.34.050 (1)]. Failure to report can result in a gross misdemeanor charge [RCW 26.44.080; RCW 74.34.053 (1)].

   PHI may be disclosed to Department of Social and Health Services (DSHS) protective services or investigating law enforcement for purposes consistent with mandatory reporting requirements [RCW 26.44.030; RCW 74.34.067]. Information considered privileged by statute and not directly related to reports required by RCW 26.44 and RCW 74.34, however, ***must not*** be divulged without a valid written waiver of the privilege [RCW 26.44.030(7); RCW 74.34.067(3)]. Persons or agencies exchanging information under RCW 26.44.030(7) or RCW 74.34.067(3) are not permitted to further disseminate or release the information except as authorized by state or federal statute.

2. **Imminent Danger to an Identified Third Party**
   Washington State law provides that a mental health professional who concludes that his or her client represents an imminent danger to an identified third party may take steps, including notifying the individual and/or law enforcement officials, to protect the third party without becoming liable for a breach of confidentiality. The law does not mandate such reporting; rather it gives the clinician discretion in deciding how to proceed. The clinician will not be liable if he or she decides not to act. **NSMHA supports staff in taking all reasonable steps to protect any identifiable individual or group of people from significant and imminent risk or danger.** [RCW 70.02.050(1)(d); RCW 71.05.390(10); RCW 71.34.200(12)].

   A similar statute allows for the release of all necessary and relevant information, upon request from appropriate law enforcement agencies, in the event of a crisis or emergent situation that poses a significant and imminent risk to the public [RCW 71.05.390(11), RCW 71.34.200(11)].

3. **Disclosure to Protect the Consumer**
   Disclosure of privileged communication is permitted if the professional reasonably believes that disclosure will avoid or minimize an imminent danger to the health or safety of the consumer [RCW 70.02.050(d)].

4. **Ombuds Staff**
   Ombuds staff must have the consumer's written authorization to obtain PHI and/or treatment records from a provider agency or NSMHA and/or its staff. This policy is not required by state or federal statute, but is supported by NSMHA in order to reinforce the functional independence of the Ombuds and to strengthen consumer confidence. The Ombuds staff is otherwise subject to all other aspects of NSMHA Confidentiality Policy as described herein.
5. **County Staff and NSMHA Board of Directors**
   The Interagency Agreements and/or Business Associate provisions between NSMHA and each of its member counties permit exchange of PHI without the written authorization of the consumer, unless an exception created by law exists, for purposes directly related to the administration of the Agreement and the state Medicaid plan.

   Members of NSMHA Board of Directors are county representatives, and as such, are subject to the conditions of the Interagency Agreements and/or Business Associate provisions between NSMHA and its member counties. Nevertheless, dissemination of PHI to Board members must be done in accordance with all confidentially and privacy policies and only after approval by NSMHA Executive Director.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA):
HIPAA mandates the establishment of standards for the privacy of Individually Identifiable Health Information. The regulation entitled, "Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Rule") became effective on April 14, 2001, and was applicable to NSMHA two years later. The Privacy Rule establishes a federal floor of safeguards to protect the confidentiality of medical information. Any law, whether local, state or federal, that provides ***more*** stringent privacy protections, will continue to apply over and above HIPAA Privacy Rule.

The Privacy Rule requires NSMHA to:

Provide information to patients about their privacy rights and how their information can be used;

1. Adopt clear privacy procedures for our organization;
2. Train employees so that they understand the privacy procedures;
3. Designate an individual (Privacy Officer) to be responsible for seeing that the privacy procedures are adopted and followed;
4. Secure patient records containing Individually Identifiable Health Information so that they are not readily available to those who do not need them; and
5. Designate an individual to be responsible for the security of all-electronic utilization, storage and transmission of Personal Health Care Information data.

ATTACHMENTS
2507.01 – Form 2507-A