PROCEDURE 2501-A

1. The Privacy Officer/Designee in consultation with the Chief Executive Officer, Deputy Director, Contracts Compliance/Fiscal Manager, and legal counsel will be responsible for developing and maintaining a list of North Sound Mental Health Administration (NSMHA) Business Associates.
2. All NSMHA staff will consult the Privacy Officer/Designee prior to establishment of any NSMHA business relationship with any individual or entity that will perform a function or activity on our behalf that involves the use, disclosure, creation or obtaining of PHI; or will provide specified services to NSMHA that involves disclosure of Protected Health Information (PHI) by NSMHA to them.

    a. NSMHA staff should assume that most NSMHA business relationships with outside individuals or entities that are ***not*** health care providers to whom NSMHA discloses PHI for client treatment purposes, could be Business Associate relationships requiring consultation with the Privacy Officer/Designee to determine if a Business Associate Agreement is needed.
    b. Prior notice to the Privacy Officer/Designee is critical so that the appropriate pre-contract procedures can be instituted.

3. A confidential and proprietary listing of current Business Associate relationships, including the scope of work and types of allowed disclosures of PHI, will be available to all NSMHA staff. Any questions about this list should be brought to the attention of the Privacy Officer/Designee.

    a. It is critical that management staff be aware of these relationships in order to make sure they can provide adequate understanding of the Business Associate's work for their department and/or site (including the appropriateness of disclosures of PHI) and recognize reportable non-compliance;
    b. The list will be updated periodically as needed. All Business Associate Agreements will be based upon the form of the Business Associate contract attached as Exhibit 1 (new contracts) or Exhibit 2 (Existing Contracts); and
    c. Will be subject to prior review and recommendation of NSMHA's legal counsel and its Privacy Officer/Designee, and approval by NSMHA's Board of Directors.

4. No Business Associate Agreement may be amended, modified or otherwise changed without the prior review and recommendation of NSMHA's legal counsel and its Privacy Officer/Designee, and approval by NSMHA's Board of Directors.
5. For any potential contractor, the Privacy Officer/Designee should request a copy of the vendor's privacy policies and/or other supporting information to determine the extent of that organization's awareness and understanding of, and adherence to, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules and the requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act.
6. NSMHA reserves the right to require additional information and assurances from Business Associate contractors, which may include, but not be limited to, a list of references comprised of current health care clients, and evidence of insurance against privacy breaches in coverage form and amounts and with a carrier acceptable in the sole discretion of NSMHA. The Privacy Officer/Designee will be responsible for following up on information provided by prospective Business Associates to determine their apparent ability to conduct business in accordance with the HIPAA Privacy Rules and the HITECH Act.
7. NSMHA reserves the right to require Business Associates to produce evidence of insurance against privacy breaches in coverage form and amounts and with a carrier acceptable in the sole discretion of NSMHA.

Procedures for Executing the Business Associate Agreement

Prior to Executing:

At or prior to the time any Business Associate Agreement is signed, NSMHA will:

a. Ask for a copy of the Business Associate's Privacy and Security Policies. A copy of each current policy should be maintained in the file with the original signed agreement. The Contracts Compliance/Fiscal Manager will maintain these files;
b. Provide our Business Associate with a copy of our current Notice of Privacy Practices. Any updates or new versions of this Notice must be sent to all Business Associates at least 10 days prior to the effective date; and
c. Obtain a copy of the Business Associate's insurance policy or a certificate from its insurer evidencing the required insurance coverage if required as provided in Section 6.2 of the Agreement.

8. Although NSMHA is not required to affirmatively monitor a Business Associate's compliance with the HIPAA Privacy Rules and the requirements of the HITECH Act, if, at any time any staff person becomes aware that a Business Associate is in breach of its Business Associate Agreement, they are required to contact their supervisor or the Privacy Officer/Designee directly and immediately. Awareness includes receipt of complaints or other information providing substantial and credible evidence of privacy violations by a Business Associate. Such breaches can include security lapses, privacy violations, and, in addition, non-cooperation with the agency in complying with its obligations, for example, to account for disclosures of PHI or to give individuals access to their PHI.

    a. Business Associates, as a part of their contract with us, are required to report any breaches of our contract with them or violations of our privacy practices. Any reports received from a Business Associate must be immediately forwarded to the Privacy Officer/Designee.
    b. The Privacy Officer/Designee will be responsible for logging these reports and for follow-up.
    c. If the Privacy Officer/Designee receives information of any privacy violation by a Business Associate or otherwise believes that a Business Associate has materially breached the Agreement or has been reported a number of times for smaller breaches such that the Privacy Officer/Designee is concerned about the Business Associate's ability to perform in compliance with the Agreement, the Privacy Officer/Designee ***must*** investigate such information and consult with agency's legal counsel, and provide a recommendation to the Leadership Team as to the actions to be taken, including the possible need to terminate the entire contractual relationship with the Business Associate and/or report the Business Associate's non-compliance to OCR.

9. Upon termination of a Business Associate Agreement, the Business Associate must destroy or return the PHI it has maintained, used, or stored on behalf of the agency. The Privacy Officer/Designee or their designee will be responsible for overseeing the orderly transfer or destruction of the PHI and for assuring the Business Associate's compliance with any post-contract obligations.
   If the PHI cannot be returned or destroyed, the Business Associate will be required to extend the protections of the Business Associate Agreement to the PHI still being held and limit further uses and disclosures to those purposes only that prevent the return or destruction of the PHI.
10. Business Associate Agreements will specify that protection of PHI survives termination or expiration of the Agreement, unless all PHI is returned or destroyed at that time.