North Country Health Consortium
Northern New Hampshire AHEC

HIPAA Privacy, Security and Data Breach Notification Policies

INTRODUCTION

The federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively "HIPAA") and the American Recovery and Reinvestment Act of 2009 ("ARRA"), and the Health Information Technology for Economic and Clinical Health ("HITECH") and New Hampshire law and regulations, as any of these may be amended from time to time, each define standards to protect the privacy and security of health information. As part of the services that the North Country Health Consortium (the "Consortium") renders to its contracted providers of health care services (the "Providers"), the Consortium and its employees and contractors will handle and be responsible for protecting health information pertaining to the Providers' patients. While the Consortium may use this health information when necessary to perform services for the Providers, the Consortium is also responsible for ensuring the privacy and security of all health information that it handles. These policies establish limits on the permitted uses of protected health information ("PHI") and also state how the Consortium will ensure the privacy and security of this PHI. For purposes of this Policy, HIPAA, ARRA, HITECH and New Hampshire laws and regulations will be referred to collectively as the Privacy Laws.

PURPOSE

These Policies will govern the use, storage, transmission, disclosure and destruction of PHI by and at the Consortium, as well as what steps will be taken if unsecured PHI is disclosed in a manner prohibited under HIPAA. No third-party rights are intended to be or are created by these policies. The Consortium reserves the right to amend or change these Policies at any time (including retroactively). These Policies are solely for purposes of ensuring that Consortium employees know what is required by the Privacy Laws with respect to the treatment of PHI and are not intended to address obligations or requirements under any other law. To the extent these Policies set forth requirements above and beyond what is required by ARRA, HITECH, HIPAA or other federal or state laws, they are not binding upon the Consortium or its employees.

APPOINTMENT OF A PRIVACY OFFICER & SECURITY OFFICER

The Consortium will designate an individual within the Consortium with a position at the management level or higher to act as the Privacy Officer. The Privacy Officer is responsible for developing and implementing the Consortium's Privacy Policies, which include but are not limited to maintaining compliant polices and procedures, overseeing employee training, investigating and resolving security incidents or breaches, overseeing certain non-routine disclosures, and HIPAA compliant record retention. The Privacy Officer may designate one or more individuals to perform Privacy Officer functions, as long as a record exists and is maintained indicating the designation.

In addition, the Consortium will designate a Consortium employee with a position at the management level or higher to act as the Security Officer. The Security Officer is responsible for developing, implementing, maintaining and enforcing the Consortium's Security Policies. The Security Officer may designate one or more individuals to perform Security officer functions, as long as a record exists and is maintained indicating the designation.

The Privacy Officer and the Security Officer may be one and the same person.

TRAINING

Every employee will receive appropriate HIPAA privacy and security compliance training and will sign a written acknowledgement that he/she has received and reviewed these Policies and that he/she understands and agrees to abide by the guidelines contained herein. Employees will receive retraining and training updates at intervals i) required by applicable law; ii) corresponding to reasonable industry practices; or iii) as determined by the Privacy Officer. Employees who do not understand some aspect of the training are encouraged to contact the Privacy Officer for clarification. Additionally, certain employees in supervisory positions will receive further HIPAA training regarding discovery and prevention of security and privacy violations. The Privacy Officer will document all employee training and any training given to subcontractors.

COMPLIANCE RECORDS

North Country Health Consortium shall document its activities taken to ensure compliance with this Privacy Policy. Compliance records include evidence of training, breach logs, access monitoring, etc. and can pertain to North Country Health Consortium activities directly or to the compliance activities of subcontractors as reported to North Country Health Consortium. The Privacy Officer or her designee shall be responsible for gathering and maintaining all compliance records and for preserving them until the last of: i) six (6) years from the date the record was created; or ii) six (6) years from the date the record was in effect; or iii) such longer period as may be required by applicable law or by a contracting provider for whom the North Country Health Consortium is acting as a Business Associate. The Privacy Officer shall store the records securely and shall make them available to the Secretary of Health and Human Services (HHS) or other regulatory agencies for review on request and to Providers for whom the North Country Health Consortium is acting as a Business Associate. On receipt of a request for records from an external organization or regulatory agency, all employees shall notify the Privacy Officer. The Privacy Officer shall cooperate with the regulatory agency after consulting with counsel and (except as specifically prohibited by the regulatory agency) or the applicable provider.

DEFINITIONS

In addition to the definitions below, all capitalized terms shall have the same meaning as given by the applicable Privacy Law.

- Protected Health Information ("PHI") – means information, in any format, that is

created or received by the Consortium and relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient; and that identifies the patient or for which there is a reasonable basis to believe the information can be used to identify the patient.

- Electronic PHI ("ePHI") - a subset of PHI that is created, received, maintained or transmitted in electronic format. All ePHI is Protected Health Information and is subject to the HIPAA privacy, security and breach notification requirements.
- Secured PHI - PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals by encryption or destruction using a method approved by the National Institute of Standards and Technology.
- Unsecured PHI - any PHI that is not secured using one of the HHS-approved technologies or methods (encryption or destruction).
- Use - the sharing, employment, application, utilization, examination, or analysis of PHI, in oral, written, electronic or other format.
- Disclosure - any release, transfer, provision of access to, or divulging in any other manner of PHI to persons outside of the Consortium.
- Breach – the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Laws which compromises the security or privacy of the PHI in that the disclosure of the information poses a significant risk of financial, reputational, or other harm to the individual.
- Covered Entity - a provider, health plan or health care clearinghouse. For purposes of II.F, the Covered Entity is the Provider with whom the Consortium has a contract or the entity that transmitted the PHI to the Consortium. Covered Entity may also refer to the Consortium when the Consortium is the provider of health care services.
- Business Associate - persons or organizations that perform functions for the Covered Entity other than in the capacity as a member of the Covered Entity's workforce, that involve the creation, receipt, maintenance or transmission of PHI. Covered Entities may only share PHI with other persons or organizations (Business Associates) where the Covered Entity has signed a Business Associate Agreement ("BAA") with the Business Associate in which the Business Associate promises to treat PHI received from the Covered Entity in accordance with the provisions of the Privacy Laws.

HIPAA PRIVACY POLICIES AND PROCEDURES

I. USE AND DISCLOSURE OF UNSECURED PHI

A. Access to PHI - All Consortium employees are authorized to access PHI to the extent performance of their job functions reasonably requires such access and where access is necessary in furtherance of legitimate, HIPAA-

approved purposes of payment, treatment and health care operations. Employees may not access PHI except in accordance with these Policies and only in furtherance of proper business-related activities.

B. Employees Shall Abide by the HIPAA "Minimum Necessary" Standard - It is the policy of the Consortium that all employees abide by the HIPAA Minimum Necessary Standard, i.e. that the amount and type of PHI requested, accessed, used and/or disclosed shall be limited to the "minimum necessary" information that is needed to accomplish the intended, authorized purpose of the use, disclosure or request. Use and disclosure to other authorized Consortium employees, plan administrators, authorized representatives of the Covered Entity, brokers and / or other business associates will be made in accordance with the Minimum Necessary Standard.

PROCEDURE: Access to patient records is limited based on job responsibility. The following classes of persons within the organization permitted to use or access PHI are limited based on job responsibility. Use or access is permitted as listed below:

Job Class	Purpose or Justification
Dentists, Hygienists, or medical professionals (Covered Entity)	Render medical care
Lab or medical technicians (Covered Entity)	Render lab or technical services
Medical records personnel (Business Associate)	Maintain medical records and/or to process insurance claims
Billing personnel (Business Associate)	Maintain medical records and/or to process insurance claims
Executive, Information Systems and Quality Control (Business Associate)	Management oversight to assure quality patient care

C. Uses and Disclosures Excepted from the Minimum Necessary Standard
The following procedures should be followed where the Minimum Necessary Standard does not apply:

1. Use and Disclosure to Parent or Legal Guardian of Minor Child Patient – Employees may disclose PHI to the parent or legal guardian of a minor child patient, so long as appropriate steps are taken to verify the identity of the person making the request and to confirm relationship between that person and the minor child. The requesting parent / guardian may request an electronic copy of the records in which case the security provisions of this Privacy Policy shall apply.

2. Use and Disclosure to Third-Parties Pursuant to Written Consent of the Patient - Employees shall not disclose PHI in response to a request

from a third party claiming to have authorization from the patient unless sufficient written authorization has been verified and the disclosure has been approved by the Privacy Officer.

a. Personal Representatives - If a patient's personal representative makes a PHI disclosure request, employees shall refer the initial request to the Privacy Officer to verify that proper documentation and authorization has been obtained before making the disclosure.

b. Use and Disclosure to Spouses, Family Members or Friends - Employees shall not disclose PHI to patients' spouses, family members or friends without express written authorization from the patient. All requests for the disclosure of PHI received from a spouse, family member or friend (excluding requests from the parent or legal guardian of a minor child patient) shall be referred to the Privacy Officer to ensure that the proper authorization has been obtained before making the disclosure.

3. Disclosures to HHS, Law Enforcement or Other Administrative or Judicial Authorities - Employees shall not disclose PHI in response to requests by HHS, law enforcement agents or other government or administrative authorities. Any and all such requests (including subpoenas, court orders, discovery requests, public health, criminal or civil investigations, etc.) shall be referred to the Privacy Officer.

D. Access and Amendment to a Participant's Own PHI – HIPAA requires that patients be afforded the opportunity access certain PHI within a Designated Record Set and to amend or correct their own PHI on request. The Designated Record Set includes treatment, enrollment, payment, and claims records, and other PHI used by or for the Consortium about a patient. If a patient submits a request to access and/or amend his own PHI, the Privacy Officer will respond to such request in the manner set forth by HIPAA.

E. Verification of the Identity of the Individual Requesting PHI – Employees shall take reasonable steps to verify the identity and authority of all persons requesting access to PHI before making any disclosure. If the identity or authority of the person making the request is at all in question, employees are directed to contact the Privacy Officer.

F. Managing Subcontractor Compliance - Before disclosing PHI to an agent or subcontractor, North Country Health Consortium will sign a contract with the agent or subcontractor that requires that the agent or subcontractor follow the same restrictions that North Country Health Consortium is required to follow. There will be no exceptions to this requirement. North Country Health Consortium will ensure that each subcontractor that has access to PHI, including through custody of computers containing data, the ability to log into the data remotely, etc., is informed that the systems and

their data are subject to protection under federal and state privacy laws. Subcontractors and vendors will be asked to execute BAAs describing their responsibilities for the PHI and appropriate ways to access and use the PHI. On termination of the subcontract, the subcontractor's access to the data will be terminated and the subcontractor will return any PHI in its possession or else, with agreement of the North Country Health Consortium, maintain it securely as needed, then securely destroy it and attest to its destruction.

II. ADMINISTRATIVE, PHYSICAL & TECHNICAL SAFEGUARDS FOR SECURITY OF PHI

It is the policy of the Consortium to fully comply with the Privacy Laws, including to: (1) ensure the confidentiality, integrity, and availability of all electronic PHI ("ePHI") that the Consortium creates, receives, maintains, or transmits; (2) protect against reasonably anticipated threats or hazards to the security or integrity of ePHI; (3) protect against reasonably anticipated uses or disclosures of ePHI that are not permitted or required by the Privacy Laws; and (4) ensure compliance with the Privacy laws by all Consortium employees, agents and contractors.

It is the policy of the Consortium to exercise discretion to select security measures that the Consortium believes are best suited to reasonably and appropriately meet the standards and specifications set forth by the Privacy Laws. Those security measures include appropriate safeguards such as limiting building access, implementing firewalls and utilizing password protections, as these access controls are recognized as important for safeguarding PHI. It is the policy of the Consortium to regularly review its IT practices and infrastructure and to consider appropriate methods to enhance security measures.

A. Administrative Safeguards. It is the Consortium's policy to maintain the confidentiality, integrity, and availability of all ePHI that the Consortium creates, receives, maintains or transmits in accordance with Privacy laws.

1.Risk Analysis. Annually, and more frequently if necessary to address new security risks, security incidents or new systems used to create, maintain, receive or transmit ePHI, the Consortium shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI in its possession.

2. Security Officer Report. Following each review, the Security Officer will document the risk analysis performed and any new administrative, technical or physical safeguards identified by the review for implementation. The Consortium shall periodically perform a technical and non-technical evaluation to determine whether these policies and procedures meet the requirements of

the Security Rule. This evaluation shall be based initially on the standards implemented under the Security Rule and subsequently in response to environmental or operations changes affecting the security of ePHI.

3. Risk Management The Consortium shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R. § 164.306(a).

4.Information System Activity Review. The Consortium shall regularly review records of information system activity to assess the confidentiality, integrity and availability of ePHI. The Consortium shall audit or monitor employee access to ePHI to verify that access is appropriate and consistent with these policies and Privacy laws. Access to ePHI shall be provided by granting the least degree of information system access required to access the ePHI needed by a workforce member or Business Associate.

5. Access Privileges. The Consortium shall establish information system access privileges in accordance with this Policy and shall document, review and modify access privileges as required by these policies.

6. Monitoring of Use. The Consortium shall monitor login attempts and report discrepancies. Passwords shall be created, changed and safeguarded in a controlled manner in order to ensure authentication of information system users.

7.Security Incident Procedure. The Consortium shall identify and take responsive actions to safeguard against suspected or known security incidents promptly, and shall mitigate, to the extent practicable, any harmful effects. The Security officer shall document all identified security incidents and their outcomes.

8.Contingency Plan. The Consortium shall implement, test and update policies and procedures for responding to emergencies or other occurrences that damage information systems. The Consortium shall implement procedures to create and maintain retrievable exact copies of ePHI. The Consortium shall develop a disaster recovery plan that provides for the restoration of any lost data and includes procedures to enable the continuation of business operations for the protection of the security of ePHI while operating in emergency mode.

9. Business Associate Agreements. The Consortium shall obtain satisfactory assurances from Business Associates that create, maintain, receive or transmit ePHI that the ePHI will be appropriately safeguarded.

B. Physical Safeguards. The Consortium shall implement policies and procedures that limit physical access to information systems and the facilities in which

they are housed, while ensuring that properly authorized access is allowed.

1. Office Layout: The Consortium shall implement physical safeguards for workstations to restrict unauthorized access to electronic protected health information. These physical safeguards can include but should not be limited to passwords, screen savers, locking file cabinets, screen display protections, and secure disposal receptacles.

- Physically separating areas where protected health information is discussed from public areas.
- Asking patients, customers or others awaiting service to stand back a few feet from service area to permit private communication.
- Using signage, lines, markers or other similar communication instructions to instruct patients, customers or others awaiting service to stand back a few feet from service area to permit private communication.
- Identifying a queuing or line-up area that separates individuals receiving service from those awaiting service.
- Adding curtains or screens in areas where health professionals discuss treatment with patients.
- Using cubicles, shield, or dividers in intake, service and payment discussion areas.
- Positioning fax machines and printers in an area where incoming faxes may not be viewed by unauthorized individuals.
- Developing and using a fax transmittal sheet that asserts the confidentiality of information contained in the fax and instructs the user that any information erroneously received should confidentially be returned to the sender immediately.

2. Facilities Safeguards: The Consortium shall

- Define facility access limits and controls.
- Define medical records limits and controls.
- Establish locking systems and procedures to protect medical records.
- Define procedures to control release and transfer of medical records.
- Define login and log-out procedures to track release of medical records.
- Include medical records areas in surveillance or security check activities.
- Evaluate and define protections for record storage or warehousing of old medical records.
- Evaluate waste disposal procedures and use shredding or similar technique to destroy waste records.

C. Technical Safeguards: The Consortium shall

- Implement policies and procedures governing the receipt and removal of hardware and electronic media containing ePHI into and out of a facility and within the facility.

- Require all ePHI to be removed from hardware and electronic media prior to disposal.
- Require all ePHI to be removed from electronic media before re-use.
- Create computer passwords or access controls to medical records.
- Periodically change computer passwords or access controls to medical records.
- Monitor computer systems for security breaches.
- Position computer screens that display medical records away from public view.
- Use screen savers to protect on-screen information from public view.
- Conduct periodic system back-up and provide secure off-site storage of back-up data.
- Ensure that old computers and drive systems are “Sanitized" or re-formatted when disposing of outdated equipment.
- Conduct periodic audits to detect unauthorized access to patient records via electronic means.
- Prior to the disposal or re-use of any electronic media containing electronic protected health information, the media shall be reformatted and/or erased in a manner that complies with guidelines on securing electronic media and would prevent the restoration of the electronic protected health information.
- Maintain a record of the movements of hardware and electronic media and the person accountable therefore.
- Create an exact copy of the electronic protected health information databases prior to the movement of any computer equipment.
- Implement appropriate technical security measures to guard against unauthorized access to electronic protected health information that is transmitted over an electronic communications network.
- Implement security measures to ensure that PHI transmitted electronically is not improperly modified without detection prior to its disposition.
- Implement tools to encrypt electronic protected health information when appropriate.

III. POLICIES IN THE EVENT OF A POTENTIAL BREACH OF UNSECURED PHI

It is the policy of the Consortium that all employees will access, use and disclose PHI only as permitted under HIPAA, and that all employees shall be vigilant with respect to guarding PHI. However, if a potential breach of unsecured PHI occurs, the following policies and procedures shall be followed.

A. Step 1 – DISCOVERY

i. A breach of PHI will be deemed “discovered” as of the first day the Consortium knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.

ii. If a potential breach is discovered, it is very time sensitive and must be immediately reported.

B. Step 2 – INTERNAL REPORTING

i. If you believe that a potential breach of PHI has occurred, you must immediately notify the Privacy Officer.

ii. Please provide all of the information you have available to you regarding the potential breach, including names, dates, the nature of the PHI potentially breached, the manner of the disclosure (fax, email, mail, verbal), all employees involved, the recipient, all other persons with knowledge, and any associated written or electronic documentation that may exist.

iii. Notification and associated documentation may itself contain PHI and should only be given to the Privacy Officer.

iv. Please do not discuss the potential breach with anyone else, and do not attempt to conduct an investigation. The Privacy Officer will conduct these tasks.

C. Step 3 – INVESTIGATION

i. On receipt of notice of a potential breach the Privacy Officer, or his/her designee, shall promptly conduct an investigation. If an improper access or disclosure has taken place, the Privacy Officer will presume a reportable breach has occurred *unless* the Privacy Officer can establish that the breach presents a low probability that PHI has been compromised.

ii. The investigation shall include interviewing employees involved, collecting written documentation, and completing all appropriate documentation.

iii. The Privacy officer shall retain all documentation related to potential breach investigations for a minimum of six years.

D. Step 4 - RISK ASSESSMENT AND RECOMMENDATION TO THE COMMITTEE

The Privacy Officer will perform a risk assessment to determine whether the disclosure falls under an exception to the reporting requirement.

- Did the improperly accessed data include PHI? (No? No reporting required.)
- Was the improperly accessed data encrypted? (Yes? No reporting required.)
- Who impermissibly accessed the information, or to whom was the information impermissibly disclosed?
    - Ex. of low probability of harm: Unintentional access to PHI by a Consortium employee, if done in good faith and within the scope of the person's authority, and which does not result in further use or disclosure in a manner not permitted under the Privacy Rule. (Example: a person authorized to view PHI accidentally opens the

file containing PHI for patient X when she meant to open the file for patient Y.)
    - Ex. of low probability of harm: Inadvertent disclosure by a person authorized to access PHI to another person authorized to access PHI, if the PHI is not further used or disclosed in a manner not permitted under the Privacy Rule. (Example: a person authorized to view PHI accidentally sends a file containing PHI for patient X to an authorized recipient when she meant to share the file for patient Y.)
- Was the PHI actually acquired or viewed? (Was the impermissibly disclosed PHI returned prior to access for an improper purpose?)
    - Any disclosure where the Privacy Officer has a good faith belief that the unauthorized recipient would not reasonably have been able to use or retain the PHI. (Example: a document containing a chart of patient IDs and balances due is viewed briefly by an unauthorized person who did not retain a copy or image of the document.)
- To what extent has the risk to individuals from the impermissible disclosure been mitigated?

E. Step 5 – FINAL DETERMINATION BY THE PRIVACY OFFICER If no exception applies, the Privacy Officer will report to the affected individual(s) (if the Consortium is the Covered Entity) or the Provider (if the Consortium is the Business Associate). The Privacy Officer shall document the Risk Assessment and her conclusions. The Privacy Officer shall have final authority to determine whether a breach of unsecured PHI occurred and what, if any, further action is warranted.

F. Step 6 – NOTIFICATION

1. Notice to Individuals - If the Privacy officer determines that notice to the affected individual(s) is warranted, he/she shall promptly prepare and transmit the notice to the appropriate individuals/entities.

i. Content - The Notice shall include:

1. A brief description of what happened, including date of breach and date of discovery;

2. A description of the types of unsecured PHI that was involved in the breach;

3. Any steps the individual can take to protect himself / herself from potential harm arising from the breach;

4. A description of what the Consortium is doing to investigate the breach, mitigate harm to individuals and prevent further breaches;

5. Contact information for the individual to ask questions including a toll free telephone number, e-mail address, web site and mailing address.

6. The Notice shall be sent first class mail, return receipt requested, and the receipt and a copy of the Notice shall be kept with related documentation.

2. Notice to Covered Entity - If the Privacy officer determines that notice to the affected individual(s) / Covered Entity is warranted, he/she shall promptly prepare and transmit the notice to the appropriate individuals/entities.

ii. Content - The CE Notice shall include:

1. Identification of each individual whose Unsecured PHI is believed to have been breached, the date of the disclosure, the facts and circumstances surrounding the disclosure, and all associated documentation.

2. Any other available information known to the Consortium that the Covered Entity will be required to include in its own Notice to the individual(s).

3. If additional information regarding the breach is later discovered by the Consortium, that information will be promptly provided to the Covered Entity.

4. The CE Notice shall be sent first class mail, return receipt requested, and the receipt and a copy of the CE Notice shall be kept with related documentation.

5. On receipt of the CE Notice, it is the Covered Entity's obligation to notify affected individuals, HHS, and/or the media unless the Consortium otherwise specifically agreed upon by contract.

iii. Timing of Notification - The Consortium shall notify the Covered Entity "without unreasonable delay" but no later than 60 days after discovering the breach. Generally, if the Consortium is an independent contractor of the Covered Entity, the Covered Entity's time to respond begins to run on the date that the Consortium notifies it of the breach.

1. Unjustified Delay - If it appears to the Privacy officer that the investigation will not be completed within a reasonable time, she must notify the Covered Entity before completing the investigation.

2. Law Enforcement Delay - A delay in notice is permissible if a law enforcement official states that a breach notification would impede a criminal investigation or cause damage to national security.

a. In that event, the law enforcement statement must be in writing and must specify the length of the delay required.

b. If the request for a delay in notification is oral, the Consortium must document the statement and request written confirmation within 30 days. If no written request for a delay is received within that time, the Consortium must notify the Covered Entity of the breach.

G. Step 7 – DOCUMENTATION - All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate that all appropriate steps were completed. All supporting documentation associated with the potential breach shall be kept on file for a period of 6 years.

H. SANCTIONS Consortium employees who fail to fully comply with these

Policies will be subject to sanctions as deemed appropriate by management.

IV. COMPLAINT PROCEDURE

It is the policy of North Country Health Consortium to investigate and take reasonable action to resolve any complaints received in relation to the Privacy Rule and related matters.

PROCEDURE:

1) Any individual, patient, client, patient representative or Business Associate may present a complaint relating to a privacy practice or disclosure or other perceived or actual violation of the Privacy Laws.
2) Any Consortium employee learning of a complaint is responsible to refer the complaint to the Privacy Officer.
3) Upon learning of a complaint, the Privacy Officer shall request that the individual document the complaint on a complaint form (sample attached). If it is not practical for the complainant to complete the complaint form, the Privacy Officer or other designated individual may assist or actually prepare the written complaint based on information provided by the complainant. The complainant shall be asked to sign and date the complaint.
4) On receipt of the written complaint, the Privacy Officer is responsible to investigate the matter, and to resolve the matter in a manner that demonstrates a good-faith effort to comply with the Privacy Rule.
5) Within a reasonable time (i.e. 30 days), the Privacy Officer shall communicate a written reply to the complainant. The reply should summarize the results of the investigation and what follow-up or corrective action, if any, is being taken by the Consortium. The response should not contain information that is confidential about any other person or is proprietary information about the operations of the Consortium or its Providers.
6) The Privacy Officer or other designated individual is responsible to maintain records and files of complaints, investigations and replies.

V. DISCIPLINARY PROCEDURES

It is the policy of the Consortium to communicate information to employees about standards of conduct and to use corrective disciplinary action when needed to address policy violations, correct employee misconduct and improve job performance.

PROCEDURE:

1) The Executive Director is responsible for communicating practice policies and standards of conduct to subordinates. At time of hire, each employee shall receive new hire information such as employee handbook and practice policies.
2) Each employee is responsible for performing assigned job duties in a safe,

professional, and efficient manner while conducting him or herself in a manner that observes practice policies.

3) The Executive Director is responsible for enforcing compliance with policies and dealing with misconduct according to the guidelines of this policy. In the event of employee misconduct or disruptive behavior, appropriate corrective disciplinary action shall be taken. Corrective action may be in the form of coaching, discussion, re-training, a verbal warning, a written warning, suspension without pay, dismissal and / or reporting to a professional licensing board or other authority.
4) When conducting a disciplinary discussion with an employee, it is recommended that:
    a. The discussion is conducted in a private office or other similar area.
    b. The employee is told what actions constituted misconduct and what form of corrective or disciplinary action is being taken.
    c. An employee may request that an employee representative be present if a discussion will result in disciplinary action.
5) All disciplinary actions (including verbal warnings) are to be documented on an Employee Counseling Sheet. The counseling sheet should be signed by the employee and the Executive Director. If the employee refuses to sign, another Manager/witness shall note on the form that the employee refused to sign. One copy of the form shall be routed to the individual's personnel file, and the employee may receive a copy.
6) The following common misconduct actions may result in coaching, discussion, re-training, a verbal warning, a written warning, suspension without pay, dismissal and / or reporting to a professional licensing board or other authority:
    a) Falsification or alteration of any record, document or form;
    b) Theft or unauthorized removal of practice property, records, or possessions of others;
    c) Insubordination or refusal to follow work instructions;
    d) Unauthorized disclosure of confidential information or PHI;
    e) Failure to follow these Policies;
    f) Unauthorized accessing of confidential information or PHI outside the scope of records to which the employee has access as necessary to perform his / her legitimate job duties (i.e., snooping in another Provider's patient record);
    g) Failure to observe the Consortium's required practices to maintain the confidentiality of PHI (i.e., sharing your password with another employee).

VI. DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

Under the Privacy Laws, a Covered Entity may use PHI to create de-identified health information. Use of de-identified health information is not subject to Privacy Laws. This checklist details identifiers, which should be removed from PHI to qualify as de-

identified information under the Privacy Laws. (Reference 45 CFR Part 164.514)

De-identified information is:

- Health information that does not identify an individual, and
- There is no reasonable basis to believe that the information can be used to identify an individual.

The Privacy Officer shall develop criteria to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made. A covered entity may use or disclose a limited data set if a data use agreement is defined with the recipient of the data set. A limited data set is PHI that excludes the following identifiers of the individual or of relatives or employers or household members of the individual, including,

- Names
- Postal address information, other than town or city, state or zip code
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers, serial numbers and license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including finger and voiceprints.
- Full-face photographic images and any comparable images.

Any data-use agreement between the Consortium and the data set recipient must:

- Establish the permitted uses and disclosures of such information by the limited data set recipient;
- Limit use of data set only for purposes of research, public health or healthcare operations;
- Limit use or further disclosure of the information;
- Establish who is permitted to use or receive the limited data set, and provide that the limited data set recipient will;
    - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
    - Report to the Consortium any user or disclosure of the

information not provided for by its data use agreement of which it becomes aware;
    - Ensure that any agents, including a subcontractor to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information;
    - Not attempt to identify the information or contact the individuals.

- The Covered Entity is responsible for exercising reasonable steps to insure compliance with a data use agreement including actions to cure the breach or end the violation, or discontinue disclosures, if necessary, or report the problem to the Department of Health and Human Services.

ATTACHMENT 1
PRIVACY COMPLAINT

In the course of providing services or products to you, it is necessary for us to obtain personal medical or other relevant information about you. Government regulations define how this information may be used or disclosed to others. North Country Health Consortium is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information. Additional details about your privacy rights are described in a separate form called a Privacy Notice.

You are referred to the Privacy Notice for a more complete description of such uses and disclosures of your protected health information. If you believe that your privacy rights described on the Privacy Notice form have been violated, you have the right to file a complaint with this organization. You also have a right to file a complaint with the government. Please complete this privacy complaint form to provide details so that we may investigate and attempt to resolve your concern.

Name:

Address:

City State ZIP

Describe complaint:

Return this form to: North Country Health Consortium Privacy Officer, 262 Cottage St. Suite 230, Littleton, NH 03561. You may also register your complaint with the U.S. Department of Health and Human Services, Washington D.C. 20212.

IF YOU CANNOT COMPLETE THIS FORM, YOU MAY COMMUNICATE YOUR COMPLAINT BY TELEPHONE BY CALLING: (603) 259-3700 ext. 223.

ATTACHMENT 2
SUMMARY PRIVACY NOTICE

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This information is a brief summary of our policies relating to government regulations, which define how your protected health information may be used or disclosed to others. A detailed Notice of Privacy Practices is available on request. We are required to abide by the terms of the Privacy Notice. North Country Health Consortium reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that we maintain, including information already in our files and electronic records systems before the time of the change.

I. North Country Health Consortium is required by law to maintain the privacy of protected health information and to provide individuals with notice of our privacy practices with respect to protected health information. You may request restrictions on how your medical information will be used or disclosed. North Country Health Consortium may or may not agree with your requested restriction in which case, we will inform you that we will not or cannot follow it. But if we agree to your requested restriction, we must honor your request.

II. Except for disclosures required by law, North Country Health Consortium must agree to your request to restrict disclosure of information related to a health care item or service for which you or someone else (other than your health insurer) make payment in full. For example, you may want to prevent your health insurer or another provider from discovering an embarrassing condition and can do so by paying for it directly.

A. North Country Health Consortium is permitted to use and disclose your health information to you, to your personal representative or to your parent or guardian if you are a minor; for the purposes of providing medical treatment, receiving payment for services provided and for administration of healthcare operations related to your care. Examples of such disclosures for treatment purposes include use of your health information by primary and consulting physicians, X-ray or other diagnostic lab tests, and nursing care. Examples of disclosure for healthcare operations may include disclosure to a pharmacy for prescriptions. Examples of disclosure for payment may include patient billing and insurance claim processing.

B. North Country Health Consortium is required to disclose protected health information to you upon your request; to the Secretary of Health and Human Services, or when required by law or legal process.

C. When using or disclosing your medical information to others, we will try to de-identify personal information when possible; and we will make a reasonable effort to limit the information disclosed to the minimum amount necessary to accomplish the permitted

purpose for the disclosure.

III. North Country Health Consortium must obtain your written authorization to use or disclose health information for reasons not related to treatment, payment or healthcare operations. In addition, North Country Health Consortium must obtain your written authorization before disclosing psychotherapy notes. We will ask you to sign a separate written authorization form, which you must sign, and date. The authorization form must identify specific information about the disclosure, including what information about you will be disclosed, why we want to disclose it and to whom and the expiration date of the disclosure. You have the right to refuse to sign the authorization and you have the right to revoke any authorization you sign with respect to information that has not yet been disclosed. You may request to inspect or to copy the information being disclosed, and you may request to receive a copy of the authorization. You must recognize that any information provided to others through the authorization may not be subject to privacy protections. When your authorization is provided, we must use or disclose your information in a manner that complies with your authorization.

Ill. North Country Health Consortium may use or disclose certain information without asking for your authorization, provided that you are informed in advance and given an opportunity to agree or object to such use or disclosure of health information including –

- We may identify you in a facility directory, but you have a right to object to this disclosure.
- We may use or disclose your information in emergency circumstances if we believe it is in the best interest for your treatment or care.
- We may disclose information to your family members involved in your care.
- We may disclose information to your next of kin.

IV. North Country Health Consortium may use or disclose certain information without your authorization or opportunity to agree or object, as described below.

- We may use or disclose information as required by law.
- We may use or disclose information as required for public health purposes, law enforcement purposes or for a job-related accident report or exam.

V. North Country Health Consortium may use or disclose your health information, which are unique to our organization. If we engage in any of the activities listed below, we may use or disclose your health information in the manner described: _

VI. If North Country Health Consortium may make any of the following disclosures of your information,

You have certain individual rights with respect to privacy of protected health information. You have the right:

- to request restrictions on certain uses and disclosures of protected health information, but North Country Health Consortium is not required to agree to a requested restriction;
- to receive confidential communications of protected health information;

- to Inspect and copy your protected health information;
- to amend your protected health information;
- to receive a paper copy of this Privacy Notice, even if you have already agreed to receive this notice electronically;
- to file a complaint with us or to the Health and Human Services Department if you believe that your privacy rights were violated. In the event that you have a complaint about our handling of your private information, you may contact our Privacy Officer:

Telephone: (603) 259-3700 ext. 223

Also, you may contact the Secretary, U.S. Department of Health and Human Services, 200 Independence Ave, SW Washington, DC 20201.