Privacy Policies for the Use and Disclosure of Protected Health Information

Responsible Individual: Vice President, Compliance and Risk Management
Approved By: NCH CEO Cabinet
October 30, 2024

Appendix of Attachments:

A. Information Security Agreement
B. Confidentiality and Privacy Statement of Acceptance
C. Release of Medical Records of a Deceased Patient Flow Chart
D. Authorization for Release of Information
E. Assessing the Breach Notification Requirements Flow Chart
F. NCH Joint Notice of Privacy Practices
G. Request for Amendment of Medical or Billing Records Form
H. Request for Restrictions on the Use and Disclosure of Protected Health Information Form
I. Privacy Complaint Form
J. Business Associate Agreement Template
K. Business Associate Decision Tree
L. Confidentiality Attestation

I. General Policies Regarding Use and Disclosure of Protected Health Information:

a. General Privacy Policy.

North Country Healthcare and all its affiliates, including Androscoggin Valley Hospital, North Country Home Health and Hospice Agency, Upper Connecticut Valley Hospital and Weeks Medical Center (collectively, "NCH", "We", "Us", or "Our"), are fully committed to protecting the privacy of patients, and to complying with all applicable laws, rules and regulations governing the use and disclosure of Protected Health Information ("PHI"). PHI is individually identifiable information that is transmitted or maintained in any form or medium, including electronic medium. Individually identifiable information is information that is created by us and relates to the past, present, or future physical or mental condition of a patient, the provision of health care to a patient, or the past, present, or future payment for the patient's health care. It is the general policy of NCH to disclose PHI only as necessary for the purpose of providing treatment to the patient, obtaining payment for services rendered and conducting the normal operations of NCH. Other uses and disclosures of PHI will be governed by NCH policies, applicable laws, rules, and regulations. Except as otherwise allowed by law, the use and disclosure of PHI will be limited to the minimum necessary to accomplish the intended purposes of the use, disclosure, or request.

To assist NCH in implementing and maintaining appropriate privacy policies and practices, NCH has designated a Privacy Officer. The Privacy Officer will be responsible for ensuring that all NCH workforce members are aware of and comply with the privacy policies and practices and will also be responsible for responding to inquiries and concerns of patients and others regarding our privacy practices. Inquiries by you or others regarding privacy practices should be directed to the Privacy Officer.

NCH's Privacy Officer may be reached by mail, phone, or email at:

Privacy Officer
8 Clover Lane Whitefield, NH 03598
Telephone: (603)-326-5608
Email: privacy@northcountryhealth.org

This Privacy Policy Manual has been developed to assist you to be aware of your responsibilities with respect to the use and disclosure of PHI. You are expected to read, understand, and comply with these policies. All NCH workforce members are expected to sign and comply with the terms of the Information Security Agreement (Attachment A) and the Confidentiality and Privacy Statement of Acceptance (Attachment B) which further defines NCH's expectations regarding the use and disclosure of PHI.

This Privacy Policy Manual and all attachments apply to the NCH workforce. "Workforce" or "Workforce Member" means NCH and its Affiliates' officers, board members, employees, volunteers, trainees, credentialed professionals, and other health care practitioners and their staff.

If you have any questions or concerns regarding these policies or the use and disclosure of PHI, please contact the Privacy Officer.

II. Use and Disclosure of PHI:

a. General Policies Regarding the Use and Disclosure of PHI.

NCH may use or disclose PHI as follows:

(1) To the patient or the patient's personal representative: PHI may be disclosed to the patient or the patient's personal representative and, in fact, except in limited circumstances, the patient has a right to such information. A patient may also request an electronic copy of their electronic health record ("EHR").

(2) At the direction of the patient or the patient's personal representative: The patient or the patient's personal representative may authorize the use or disclosure of PHI or EHR by completing an Authorization for Release of Information form.

(3) To a personal representative: NCH may disclose PHI to a personal representative such as the patient's guardian, agent under an activated Durable Power of Attorney for Healthcare document, surrogate decision-maker, parent or legal guardian of a child, representative of the patient's estate, or, under certain circumstances, the patient's surviving spouse or next of kin. If you have any questions about whether the person seeking PHI is entitled to receive such information, you should consult with the Privacy Officer.

(4) For treatment: NCH may disclose PHI to provide, coordinate, or manage the patient's health care needs and any related services. This includes, but is not limited to, disclosing PHI to consulting providers, laboratories, ancillary service providers, pharmacies, etc.

(5) For payment: Except as specified below, PHI may be disclosed in order to bill and collect payment for the treatment and services provided. This allows the disclosure of information for the purpose of obtaining reimbursement, making coverage determinations, obtaining prior authorization, participating in case management and other utilization review processes, as well as other payment related activities. If a patient pays for the services we have provided in full and requests that we not disclose PHI to their health plan, we must honor that request.

(6) For the operation of NCH: NCH may use and disclose PHI in order to carry out the operations of NCH, which may include administrative support activities, including quality assessment and improvement, peer review activities, training and credentialing and legal and auditing functions.

(7) Others involved in the patient's health care: If the patient is present for, or otherwise available prior to NCH's disclosure of PHI to a family member, other relative, or close personal friend, and has the capacity to make healthcare decisions, the provider may disclose PHI to any of these people to the extent the PHI is directly relevant to the person's involvement with the patient's care or payment for that care only if either (a) the provider obtains the patient's consent; (b) the provider provides the patient with the opportunity to object to the proposed disclosure, and the patient does not express an objection; or (c) the provider reasonably infers from the circumstances, based on the exercise of professional judgment, that the patient does not object to the disclosure. The patient may, for instance, bring a spouse or other family member into the physician's office to discuss his or her condition and treatment options. If the patient is unable to agree or object due to an emergency or incapacity, the provider may disclose PHI, as necessary if, based on the provider's professional judgment, the disclosure is found to be in the patient's best interest. NCH may also disclose PHI to notify, or assist in the notification of, a family member, a personal representative, or another person responsible for the care of the patient of the individual's location, general condition, or death.

(8) Following the patient's death: PHI may be disclosed following a patient's death as described in the attached Release of Medical Records of a Deceased Patient flow chart (Attachment C).

(9) As required by law or in compliance with judicial or administrative proceedings: PHI may be used or disclosed as necessary to comply with applicable, state or federal law, to assist in disaster relief efforts, for public health activities (e.g., preventing or controlling disease or injury, reporting vital events, etc.), to report neglect, abuse or domestic violence, to health oversight agencies such as the U.S. Department of Health and Human Services' Office of Civil Rights, to alert law enforcement to criminal activity, or in response to a valid court order or any purpose required by law. In the event such a disclosure is necessary, the workforce member should consult with the Privacy Officer to ensure the manner and the substance of the disclosure is in compliance with all applicable laws, rules and regulations, in consultation with NCH legal counsel.

(10) To the patient's employer: If NCH is providing the patient with health care at the request of the patient's employer in order to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury, NCH may disclose findings concerning a work- related illness or

injury or a workplace-related surveillance to the employer, provided that NCH provides the patient with separate written notice of the disclosure at the time the health care is provided.

There may also be disclosures that are incidental to these permitted disclosures. For example, if you call a patient's name in the waiting room, other patients will hear the name. This is a permissible incidental disclosure, but you should always take precautions to make these patient announcements as discreetly as possible. Except for certain other exceptions provided by law, all other uses and disclosures of PHI require the patient's authorization.

b. Policies Regarding Authorized Use and Disclosure of PHI.

Except as set forth above, NCH may not use or disclose PHI without a valid authorization. NCH has developed an authorization form to be completed by the patient or their personal representative (Attachment D). The form must be filled out completely. The authorization is valid only through the expiration date designated on the form. The authorization may be revoked at any time.

c. Release of Sensitive Information.

State and Federal laws contain special confidentiality provisions regarding sensitive diagnoses. These include, but are not limited to, HIV test results, mental health records, and records of patients who have been diagnosed or treated for drug or alcohol abuse. These laws require special authorizations or court orders for release of information. NCH System Document, "Protected Health Information Uses and Disclosures," describes how to handle these situations. Please contact the Privacy Officer with any questions or concerns.

d. Verification of the Identity and Authority of Person Requesting Disclosure of PHI.

Whenever NCH makes an authorized disclosure of PHI, it has an obligation to ensure that the person requesting the disclosure is authorized to do so and that the disclosure is made to the intended recipient. It is the policy of NCH to verify the names and addresses of recipients of PHI through review of valid photo identification or other like measures if they are not already known to NCH. In the case of a telephone inquiry, NCH must take appropriate steps to verify the identity of the caller. This may include verifying the telephone number and calling the person back. If the requestor is not the patient, authority may be verified by reviewing legal documentation such as a guardianship order or advance directive.

e. Minimum Necessary Rules.

Except as described below, access to PHI will be limited to the minimum amount necessary to accomplish the intended purpose. Workforce members within NCH will access only that information necessary to complete the task or to fulfill their job responsibilities. Workforce members must not access PHI except, when necessary, in the course of their employment responsibilities. A workforce member shall not view their own protected health information, either through the electronic medical record or the paper medical record. If a workforce member wishes to obtain their own protected health information, they must follow the same process as any other patient (either access through the Patient Portal or see appropriate Release of Information personnel).

Whenever NCH permits a disclosure, it must be done in a manner that limits the amount of information disclosed to the minimum amount necessary to accomplish the intended purpose. Likewise, when requesting PHI from another covered entity, NCH will limit the scope of the request to the minimum amount of PHI necessary to accomplish the intended purpose.

The minimum necessary policy does not apply to:

(1) Disclosures to, or requests by, a health care provider for treatment.
(2) Disclosures to the patient.
(3) Disclosures made in accordance with a valid authorization signed by the patient or their personal representative.
(4) Disclosures required by law.
(5) Disclosures to regulatory authorities investigating NCH's compliance with the privacy requirements.

f. Breach.

In general, PHI can only be disclosed without a patient authorization as necessary for the purpose of providing treatment to the patient, obtaining payment for services rendered and conducting the normal operations of NCH. Other uses and disclosures of PHI will be governed by our policies and applicable laws, rules and regulations. If you suspect that an unauthorized use or disclosure has occurred, either at NCH or by one of our business associates, you should report the matter to the Privacy Officer immediately. An unauthorized use or disclosure of PHI may be considered a breach. NCH will investigate all reports of unauthorized use or disclosure. We will determine if the use or disclosure constitutes a breach and conduct a risk assessment to determine whether there is a low probability that the PHI has been compromised. If appropriate, NCH will notify individuals and authorities as required and make every reasonable effort to mitigate the harm.

(1) Risk Assessment & Notification: In the event the Privacy Officer, the Security Officer, or a NCH workforce member suspects a breach of confidentiality of PHI, they should follow the reporting, risk assessment, and notification procedures set forth in the NCH System Document, "Information Security Breach Notification."

III. Patient Rights Regarding Their PHI:

a. Right to Notice of Privacy Practices.

Patients have a right to receive adequate notice of the uses and disclosures of PHI that may be made by NCH and of their legal rights and NCH's legal responsibilities with respect to PHI. To ensure patients are provided adequate notice, NCH has developed a Joint Notice of Privacy Practices ("Notice"). This Notice will be posted in our reception area and on our website. The Notice will also be posted on the websites of our affiliates. A copy of the Notice must be provided to every patient at the time of their first visit except in an emergency, in which case notice must be provided as soon as reasonably practicable after the emergency. The patient's file must reflect that the patient received the Notice. To document that the patient has received the Notice, NCH has developed an acknowledgment that must be signed by the patient or their personal representative and kept with the patient's file. If the patient or their personal representative is unwilling or unable to sign the acknowledgment, NCH must document that the Notice was given and must document the good faith efforts to obtain an acknowledgement. In the event the Notice is revised, the revised Notice must be made available to the patient or representative upon request.

See NCH Joint Notice of Privacy Practices (Attachment F).

b. Right to Access PHI.

Except in limited circumstances, a patient is entitled to inspect and obtain a copy of their PHI or an electronic copy of their EHR or to direct that a copy of PHI be sent directly to another person designated by the patient, provided the request is made in writing, signed by the patient or their personal representative, and clearly identifies the designated recipient and where the PHI should be sent. Ordinarily, NCH must respond to such a request within 30 days. Under certain circumstances NCH may deny the requested access. For example, when a licensed health care professional determines that providing the requested access is reasonably likely to endanger the life or physical safety of the patient or another person, the request may be denied. NCH may impose a reasonable fee to cover the cost of copying and postage or the cost of labor and portable electronic media to provide an electronic document. If you have any questions about whether the PHI should be provided, or whether access should be granted, you should consult with the Privacy Officer.

c. Right to Request Amendments to PHI.

A patient has the right to amend their PHI if the information is maintained in a designated record set. See Request for Amendment of Medical or Billing Records (Attachment G). A designated record set includes the patient's medical and billing records, payment records, case management records or any other PHI used by NCH to make decisions about the patient. NCH may deny the request if it finds that the PHI subject to the request was not created by NCH, is not part of a designated record set, is not available for inspection under law or is found to be already accurate and complete. NCH must act on the

patient's request within 60 days after receipt. If NCH grants the request, it must make the appropriate amendment to the PHI by identifying the records affected and appending the amendment. NCH must also take reasonable steps to notify persons whom NCH knows received the PHI and may have relied on it to the detriment of the patient. In the event NCH denies the amendment, it must provide the patient with a written denial setting forth the basis of the denial. It must also state the patient's right to submit a written disagreement or request that a copy of the requested amendment and denial be provided with future disclosures. The patient must also be informed regarding the process for filing a complaint. You should consult with the Privacy Officer regarding any requests for amendments.

d. Right to Request Restriction of Uses and Disclosures of PHI.

A patient has the right to request restrictions on certain uses and disclosures of PHI about the patient such as disclosures for treatment, payment, or health care operations purposes. If a patient has paid in full for services and requests that we not disclose related PHI to his or her health plan, we must honor that request. In all other situations, it is within the discretion of NCH to agree to such a request. All requests for restricted use or disclosure of PHI should be referred to the Privacy Officer or designee. See Request for Restrictions on The Use and Disclosure of Protected Health Information Form (Attachment H).

e. Right to Request Confidential Communications.

NCH must accommodate a reasonable request by a patient to receive communication of PHI from NCH by alternate means or at alternate locations without requiring the patient to explain the basis for the request. For example, the patient may request that appointment reminders be sent via e-mail or to an alternate address. The request may be made orally or in writing. If made in writing, NCH will retain documentation of the request. If it is an oral request, NCH will document the request and seek the patient's signature as soon as possible thereafter. If the patient makes a reasonable request to receive PHI by alternate means or at an alternate location, NCH must accommodate the request. There are certain circumstances when NCH can terminate its agreement to send PHI through alternative means or to an alternative location, for example, if an e-mail address given by the patient is no longer functional. In the event a patient cannot be contacted or does not respond to communications sent by alternate means or to an alternate location, please contact the Privacy Officer or designee for further direction.

f. Right to an Accounting of Disclosures.

A patient has a right to an accounting of certain disclosures of PHI made by NCH within the six years preceding the request. NCH must ordinarily provide such an accounting within 60 days of a patient request. In order to accommodate these requests, NCH must keep an accurate record of such disclosures including the date of the disclosure, the name and, if known, the address, of the entity or person who received the PHI, a brief description of the PHI and a brief statement of the purpose of the disclosure. There are also specific accounting requirements regarding multiple disclosures and disclosures made for research purposes. Not all disclosures need to be included in the accounting. It is not, for example, necessary to account for disclosures made to the patient, their personal representative or to others involved in their health care, or disclosures authorized by the patient. Similarly, disclosures made for the purpose of treatment, payment or health care operations need not be included in an accounting of PHI, except if these disclosures were made through an EHR. Examples of disclosures which must be accounted for whether or not the PHI is part of an EHR include: reports made pursuant to mandatory abuse reporting laws PHI reviewed as part of a financial or quality of care audit, PHI provided as part of a licensing or certification application or review, or information provided under court order or to public health authorities. Please refer all requests for accounting to the Privacy Officer.

g. Complaints about Privacy Practices.

Patients may file complaints about privacy practices with the Privacy Officer and/or with Secretary of the U.S. Department of Health and Human Services. NCH has prepared a Complaint Form a patient may use to file a complaint. See Privacy Complaint Form (Attachment I).

IV. Administrative Protection of PHI:

a. General Policies Regarding Business Associates.

A business associate is a person or entity that provides certain functions for NCH requiring access to PHI but who is not an employee of NCH. Examples of business associates include persons or entities that perform claims processing or administration, transcription, accounting, legal, consulting or quality assurance functions. NCH shall enter into agreements with its business associates requiring the business associates' compliance with certain requirements regarding the handling of PHI. See Business Associate Agreement Template (Attachment J). A business associate may only use or disclose PHI as permitted or required by its Business Associate Agreement or as required by law. In the event you become aware of any concerns regarding a business associate's handling of PHI, you should report your concerns to the Privacy Officer.

b. Business Associate Agreement.

NCH has developed a template for contracting with business associates (see Attachment J). NCH has also included a Business Associate Decision Tree (Attachment K) in these policies to aid NCH workforce members and affiliates in determining which entities qualify as business associates.

c. Destruction of PHI.

As part of its Compliance Plan, each NCH facility has adopted policies which address the proper storage and destruction of PHI. NCH reminds all workforce members of the importance of properly disposing of PHI. If it is necessary to dispose of hard copies of PHI, it must be disposed of in a proper manner to prevent improper distribution. Each NCH facility has provided specific containers for the disposal of PHI. Please contact the Privacy Officer if you have questions about the proper manner of disposing or destroying PHI.

d. E-mail Policies.

E-mail has become a routine part of our business interactions, but it is important to remember that e-mail messages can easily be intercepted, misaddressed, and forwarded. E-mail addresses must be verified before sending, and PHI should ordinarily be transmitted to those recipients outside of NCH using secure e-mail. If you discover that PHI has been delivered to an incorrect address in error, notify the Privacy Officer. If a patient requests that NCH e-mail their PHI using unsecure e- mail, please contact the Privacy Officer to discuss how to respond to the request.

e. Text Messaging Policies.

(1) Sending Text Messages Containing PHI to Patients: NCH and its workforce members shall not send text messages to patients containing PHI unless through a secure text messaging platform or after the patient signs a consent form authorizing the unsecure disclosure and acknowledgement of associated risks.

(2) Receiving Text Messages Containing PHI from Patients: When a patient sends a text message to an NCH workforce member containing PHI, the recipient shall maintain the security and privacy of the text message at all times. Although HIPAA does not apply to NCH patient's actions, the patient's PHI becomes protected upon receipt by NCH or its workforce members. The recipient shall not respond via unsecured text message unless the patient has consented to same or if the patient is in serious medical emergency and it is essential that PHI be shared for the health of the patient.

(3) Sending Text Messages Containing PHI to Other Workforce Members: NCH workforce members shall not text each other unsecured PHI except under serious emergency medical emergencies in which it is essential that PHI be shared for the health of the customer, and there is no other way to communicate the necessary information under the circumstances.

f. Facsimile Policies.

Use of fax machines to transmit information has greatly increased the delivery of PHI when there is an immediate need.

There are, however, security issues presented by the faxing of PHI. The information can be sent in error to the wrong recipient or can be faxed to a fax machine that is located in an insecure location. All faxes containing PHI shall be accompanied by a cover sheet prominently displaying the following statement: **"This transmission may include confidential patient information. If you have received this transmission in error, please contact the sender immediately."** You must always verify the fax number before sending and also verify that the information is being transmitted to a machine in a secure location. Unless other arrangements are made in advance, you should notify the recipient you are sending the confidential information before transmitting the facsimile to be sure someone is there to receive it. Upon learning that a fax containing PHI has been mis-routed, the sender of the fax shall immediately contact the unintended recipient and request either the return or destruction of the document. The recipient shall be sent a Confidentiality Attestation (Attachment L) with a postage paid envelope to be returned to the sender of the fax. Steps shall be taken to remedy the problem that caused the misdirection. The sender shall complete an Event Report which will provide written notice to the NCH Privacy Officer, or designee, that a misrouting has occurred. The signed Confidentiality Attestation will be scanned as an attachment to the Event Report. Each of these steps shall be documented in writing by the sender of the fax. For more information see NCH System Document, "Protected Health Information Transmittal via Facsimile."

g. Training Requirements and Sanctions.

All workforce members are required to participate in training regarding the privacy policies and procedures of NCH upon engagement or hire and periodically thereafter. You will also be required to participate in retraining if there are revisions to the policies and procedures that materially affect your job responsibilities. Documentation of your training will be maintained in the online healthcare training solutions program. You are required to comply with the privacy policies of NCH. If you fail to comply, you may be subject to disciplinary action up to and including termination.

Rescission:

This policy rescinds and replaces the System Document, Privacy Policies for the Use and Disclosure of Protected Health Information, dated November 28, 2022.

_____ _____

Vice President, Compliance and Risk Management Chief Executive Officer

Attachment A

INFORMATION SECURITY AGREEMENT

North Country Healthcare and its affiliates (the "NCH System") are dedicated to safeguarding and maintaining the confidentiality, integrity, and availability of its patient protected health information, employee information, and organizational information (collectively "confidential information"). This Information Security Agreement ("Agreement") is required to be read, signed, and complied with by all users that access any of the NCH System's information systems as a condition of access to any information system. The information system user signing this Agreement may only access, use, and disclose confidential information in any medium as needed to perform their job responsibilities as allowed by law, organization policies and procedures, and/or as agreed upon between said user and the NCH System as delineated below.

1.	I understand and agree that I must safeguard and maintain the confidentiality, integrity, and availability of all confidential information I access, use, and/or disclose at all times, whether or not I am at work and regardless of how it was accessed.
2.	I will only access or use NCH System hardware and information systems that I have been authorized to access and agree not to demonstrate the operation or function of any Hospital information systems or devices to unauthorized individuals.
3.	I will only access, use, and/or disclose the minimum necessary confidential information needed to perform my assigned duties. I will not disclose confidential information to others who do not have a need to know it. I will disclose confidential information to other individuals and/or organizations who need it to perform their assigned duties or as allowed by law.
4.	I will not discuss patient, workforce member, or organizational information where others can hear the conversation (e.g., in hallways or elevators, in the cafeteria, at restaurants, at social events, etc.). It is not acceptable to discuss confidential information in public areas. This can raise doubts with patients and visitors about our respect for their privacy.
5.	I will not discuss any patient information on social media, understanding that even without the use of a patient name, it may be possible to identify a patient.
6.	I will not view my own protected health information through the electronic medical record or the paper medical record. If I wish to obtain my own protected health information, I must follow the same process as any other patient (either access through the Patient Portal or see Release of Information personnel).
7.	I will not knowingly in any way divulge, copy, release, sell, loan, alter, or destroy any confidential information except at properly authorized.
8.	I will not knowingly remove or copy NCH System software or data to electronic storage media (including, but not limited to, CDs, DVDs, external disk drives, zip drives, flash drives, thumb drives, SD cards, etc.), or introduce software or data onto NCH System information systems or applications via electronic storage media, or move hardware or electronic storage media outside of the direct control of NCH, or dispose of or reuse hardware of electronic storage media other than through the Information Technology Department. I will submit written requests for exceptions to use electronic storage media or to transfer any hardware or electronic storage media outside NCH's control to the Information Security Officer. If I receive permission to proceed, I will assume sole and absolute responsibility to manage and protect the hardware and/or data based upon the NCH System's policies and procedures and according to the law.
9.	I understand that access to all NCH System workstations and information systems including e-mail and internet is intended only for business purposes.
10.	I will practice secure electronic communications by transmitting confidential information only to authorized users or organizations in accordance with approved privacy and security standards. I agree not to make any unauthorized transmissions, inquiries, modifications, or purging of data in the system. Such unauthorized transmissions include, but are not limited to removing and/or transferring data from the facilities' computer systems to unauthorized locations, e.g. home.
11.	I will never use tools or techniques to break/exploit security measures. I will not use NCH System information systems to subvert or break into other information systems.
12.	I will never knowingly connect to unauthorized networks through NCH System information systems or devices.
13.	I agree to take special precautions with portable workstation(s) assigned to me.

14. If authorized to use remote access, I will take steps to ensure that unauthorized individuals do not access the NCH System networks.
15. I understand that I have neither an ownership interest nor expectation of privacy in any information accessed or created by me during my relationship with NCH and its Affiliates. The NCH System may audit, log, access, review, and otherwise utilize information stored on or passing through its information systems for many reasons, including to maintain the confidentiality, security, and availability of confidential information and to ensure compliance with the provisions of this agreement.
16. I will not use NCH System workstations or information systems to engage in any activity that is illegal or is in violation of the NCH System's policies.
17. I will report immediately any unauthorized individuals found in restricted areas at any time as well as any incidents or breaches of physical security for investigation and action.
18. I will only use my officially assigned, personal user login IDs, passwords, and PIN. I understand that I must maintain my user login IDs, password, and PIN in strictest confidence and will not disclose them to anyone, at any time, for any reason except in connection with activities conducted by NCH or its affiliates' information security departments. I will not use another user's login ID, password, and PIN instead of my own for any reason.
19. I understand that I may be held accountable for all entries, inquiries, changes, and data purges made to any NCH information system using my user login IDs, passwords, and PIN.
20. I understand that my user login IDs, passwords, and PIN are used to control access to NCH information systems and that my electronic signature is equivalent to my legal signature.
21. I agree to immediately notify the Information Technology Department if my password or PIN has been impermissibly viewed or disclosed, or otherwise compromised.
22. I will not knowingly connect non-NCH System owned hardware (i.e., PC, laptop, tablet, printer, scanner, keyboard, mouse, etc.) to the NCH System networks for any purpose, without permission from the Information Technology Director, or designee.
23. I will not download executable programs without the approval of the Information Technology Director, or designee.
24. I will not e-mail PHI from my NCH or hospital e-mail address to my personal e-mail address or e-mail PHI from my personal e-mail address to an NCH or hospital e-mail address.
25. I agree to not knowingly disable anti-virus software running on PCs and/or the NCH System network.
26. I agree to immediately report any suspected or known activity that violates privacy or information security policies, procedures, or controls or any incident that could have an adverse impact on NCH System operations to the Information Technology Department staff (or on call IT staff member), the Information Security Officer, the Privacy Officer, or a senior manager (Administrator On Call).
27. I agree to sign off or lock my computer workstation before leaving it unattended.
28. I understand that I will be given a badge at the time of hire that will allow access to external doors and internal doors based on need to access. I will not allow my badge to be used by anyone else. If I lose my badge, I will notify HR, the Security Officer or IT immediately.
29. I agree to not make inquiries about confidential information for other personnel who do not have proper authorization to access such confidential information.
30. I agree to participate in NCH System information privacy and security training and awareness programs.
31. I agree that I will maintain the confidentiality, integrity, and availability of all confidential information even after termination, completion, cancellation, expiration, or other conclusion of access to NCH System information systems. Upon termination of my employment, I will immediately return any documents or other media containing confidential information to NCH System.
32. I understand that violation of any privacy or information security policy, procedure, or control may result in disciplinary action, up to and including termination of employment or business relationship, suspension and loss of privileges, termination of authorization to work within the NCH System as well as legal actions such as civil liability and/or criminal penalties.

ACKNOWLEDGMENT BY SIGNATURE

By signing this document, I agree to the statements listed above of the Information Security Agreement.

By signing this document, I also confirm the following:

- I have not had a felony conviction in New Hampshire or any other state.
- I have not been convicted of a sexual assault, other violent crimes, assault, fraud, abuse, neglect, or exploitation nor do I pose a threat to the health, safety, or well-being of a patient.
- I have not had a finding by the health and human services department or any administrative agency in New Hampshire or any other state for assault, fraud, abuse, neglect, or exploitation of any person.

_____ _____

User Signature Date

_____

Printed Name

Attachment B

CONFIDENTIALITY AND PRIVACY STATEMENT OF ACCEPTANCE

Pursuant to the Privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (45 CFR PARTS 160 AND 164), the Health Information Technology for Economic and Clinical Health Act of 2009, and applicable state laws including, but not limited to, RSA 151, RSA 332-I, and RSA 359-C, North Country Healthcare and its Affiliates (collectively, "NCH"), and their respective workforce members—NCH and its Affiliates' officers, board members, employees, volunteers, trainees, credentialed professionals, and other health care practitioners and their staff—are responsible for ensuring the privacy of individually identifiable and protected health information.

In addition to protected health information, NCH and its workforce members are responsible for maintaining the confidentiality and security of information that they may be exposed to or acquire during the course of performing business with, or on behalf of, the organization. This confidential information includes, but is not limited to, all information data, reports, records, summaries, tables and studies, proceedings, whether written or oral, fixed in hard copy or contained in any computer database or computer readable form, as well as any information that is identified as "confidential" between individuals (hereinafter "Confidential Information").

ACKNOWLEDGEMENT

I, the undersigned, hereby acknowledge and agree that I will not disclose protected health information or Confidential Information that I may be exposed to or acquire during the course of performing my duties and responsibilities during my tenure as a workforce member except in connection with authorized activities.

Breaches of protected health information will be reported to the appropriate state and federal agencies as well as the affected patient(s). Breaches of protected health information may result in civil and/or criminal action and liability.

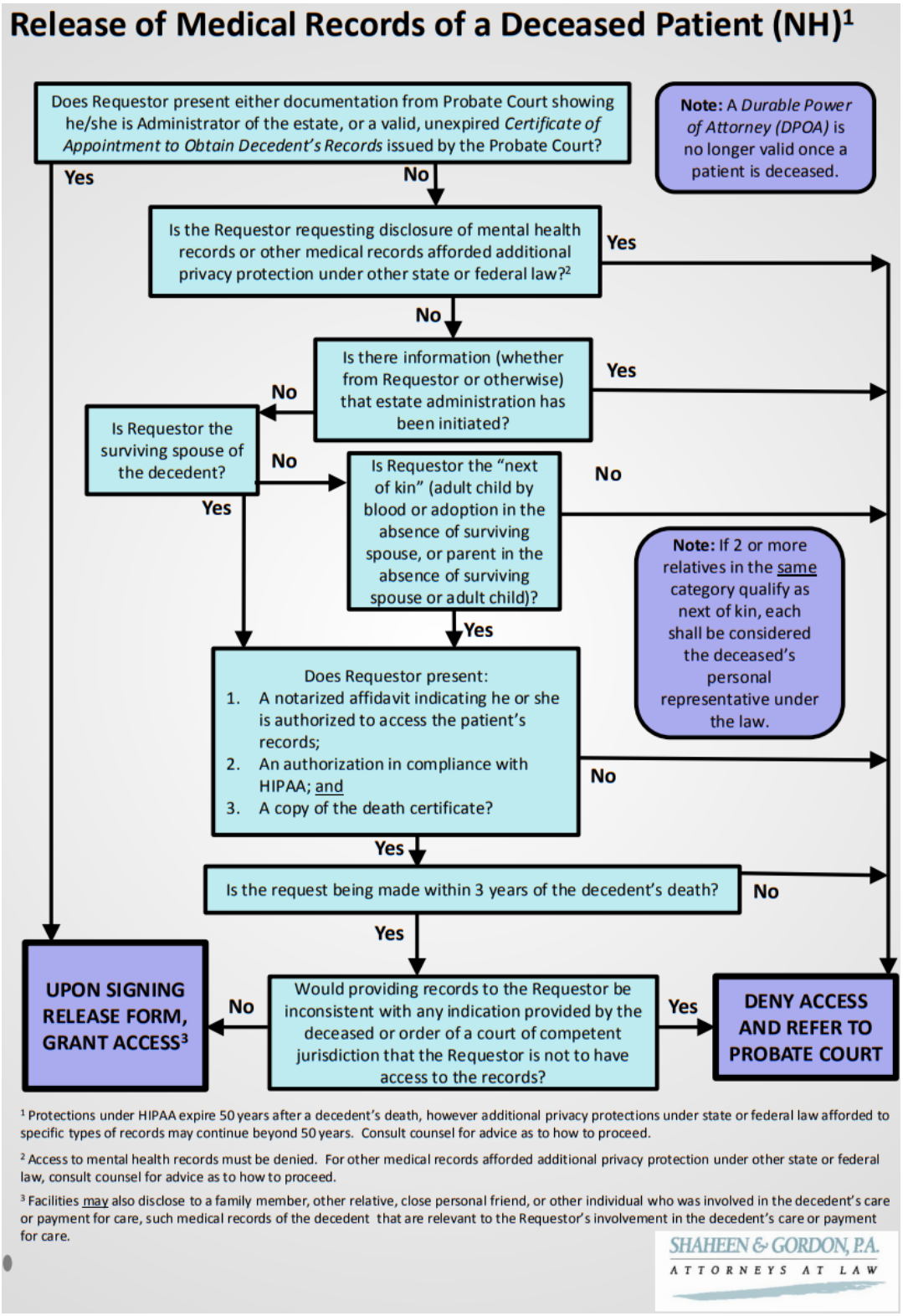
If I am a workforce member, I further understand that any unauthorized disclosure and/or breach of protected health information or Confidential Information may lead to disciplinary action against me by NCH, its officers, or Board of Directors/Trustees and that such breach of confidentiality may be cause for my dismissal or termination.

_____
Signature

_____
Printed Name

_____
Date

Attachment C



Attachment D

Authorization For Release of Information

Please complete all sections. Missing information may cause delays or the inability to retrieve your records. Release may take up to 30 days to process.

Please Print Patient Information *must be fully completed*	Name:_____ Previous Name:_____ Date of Birth:_____ Address:_____ Phone:_____ City:_____ State:_____ Zip Code:_____
Who *has the information you want released.* **Please list the specific hospital, physician office, and/or home health agency.**	☐ Androscoggin Valley Hospital, 59 Page Hill Road, Berlin, NH 03570 ☐ Indian Stream Health Clinic, 181 Corliss Lane, Colebrook, NH 03576 ☐ Upper Connecticut Valley Hospital, 181 Corliss Lane, Colebrook, NH 03576 ☐ Weeks Medical Center, 173 Middle Street, Lancaster, NH 03584 ☐ North Country Home Health & Hospice Agency, 536 Cottage Street, Littleton, NH 03561 ☐ Other Facility/Provider:_____ Address:_____ Phone:_____ City:_____ State:_____ Zip Code:_____ Fax:_____
Who *do you want to receive your information?*	I hereby authorize the above-named hospital/physician office to release medical records as described below: Name:_____ Attention to:_____ Address:_____ Phone:_____ City:_____ State:_____ Zip Code:_____ Fax:_____
Information to be released: **What** *do you want shared? Check appropriate boxes*	**Date(s) of Service** From:_____ To:_____ **We do not accept "ALL" for date of service, if left blank the last 2 years will be sent.** Description of information to be released: (check all that apply) ☐ Discharge Summary ☐ Laboratory Report ☐ Physician Orders ☐ Cardiology/EKG ☐ Emergency Dept. ☐ Radiology Report ☐ Rehab PT/OT/ST ☐ Xray films/CD ☐ History & Physical ☐ Pathology ☐ Consultations ☐ Billing Records ☐ Operative Reports ☐ Medication Lists ☐ HH/Care Plans ☐ Immunizations ☐ Progress/Office Notes ☐ HH/Treatment Notes **Sensitive Information** 42 CFR Part 2 **(INITIAL all that apply)** ____ Drug and Alcohol Testing ____ HIV/AIDS/STD Testing ____ Drug and Alcohol Treatment Records ____ HIV/AIDS/STD Treatment Records ____ Psychiatric Evaluations ____ Mental Health Progress Notes ____ Treatment Plan ____ Medication List ____ Intake Assessment/Screening
Purpose of release: **Why** *is it needed?*	☐ Continuing Care ☐ Transfer of Care ☐ Personal Use/Review ☐ Insurance ☐ Workers Compensation ☐ Attorney ☐ Temporary Transfer of Care (school/winter away) ☐ Other (Specify):_____ **Fees may be charged in accordance with State and Federal Statutes**

I understand that:

- I can refuse to disclose some or all of the information in my record, but refusal may result in an improper diagnosis or treatment, denial of coverage for a claim for health benefits, or other insurance or other adverse consequences.

- I can revoke all or part of this authorization at any time during this time period by providing written notice to the Health Information Management Department, except where this authorization already has been acted on for release of my protected health information. Such revocation may be the basis for denial of health benefits of other insurance coverage or benefits.
- I understand that if protected health information is disclosed to a third party, the information may no longer be protected by the federal or state privacy laws and may be re-disclosed by the individual or entity that receives this information.
- I understand I am entitled to a copy of this authorization, upon request.
- If any of the information disclosed pursuant to this request is from records protected by Federal confidentiality rules at 42 CFR Part 2, those rules prohibit the recipient from making any further disclosure of this information unless I expressly permit it through my written consent or redisclosure is performed as otherwise permitted in 42 CFR Part 2.

Expiration: Unless otherwise revoked, this authorization will expire on the following date, event, or condition:_____
I understand that if I fail to specify an expiration date, event or condition, this authorization will expire 1 year from date signed, unless revoked in writing.

Signature of Patient or Personal Representative: _____

Printed Name: _____

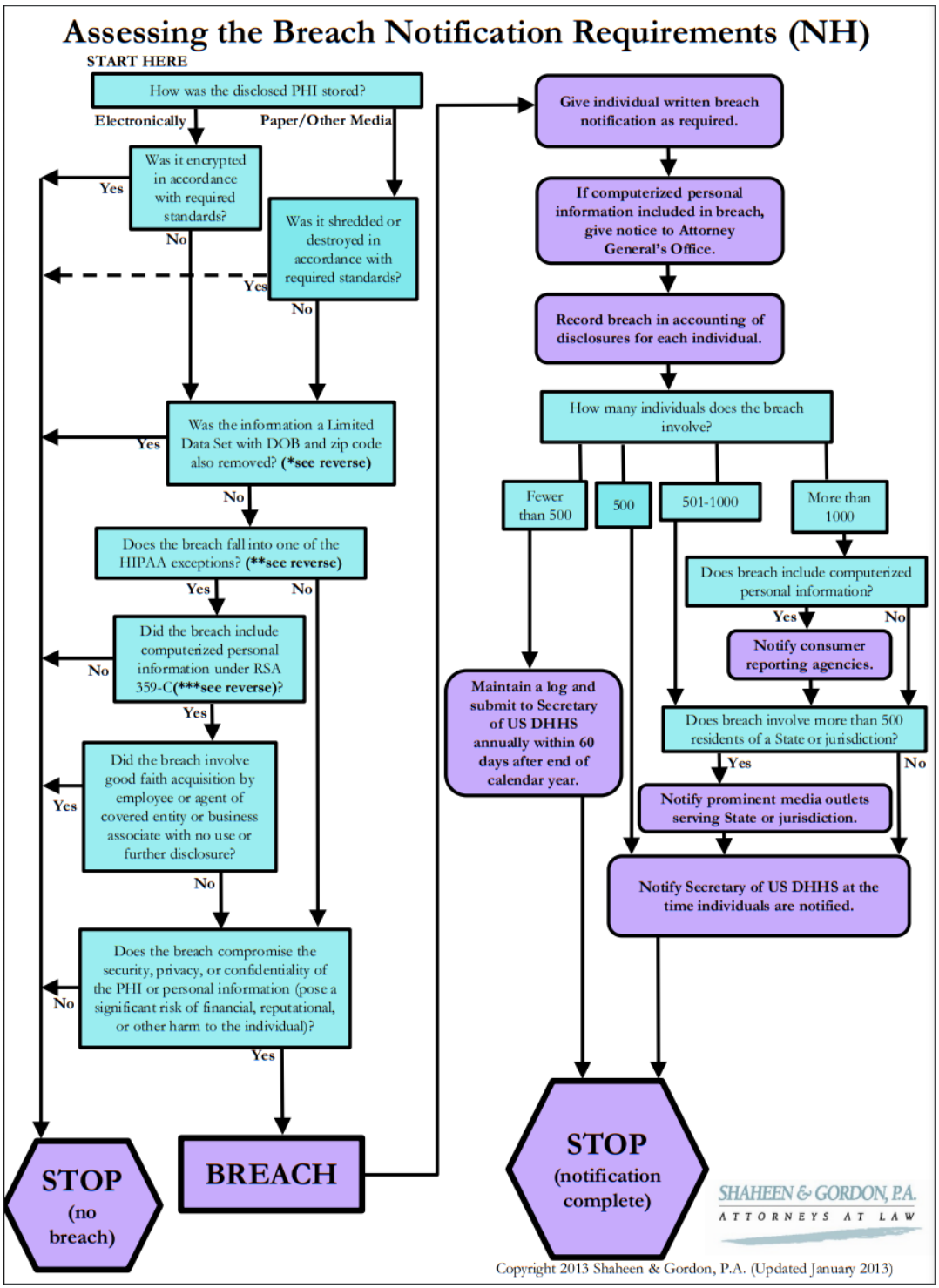
Relationship of Personal Representative (e.g. Parent, Guardian, Power of Attorney): _____

Date: _____ Time: _____

FOR OFFICE USE ONLY

Medical Record #: _____
Visit ID: _____
Telephone Request ☐ Date: _____
Charge: Yes or No
By Whom: _____
Info to be: ☐ Faxed ☐ Mailed ☐ Picked up ☐ Handed
Date/Time to be mailed, etc.: _____
Date Completed: _____

Attachment E



Assessing the Breach Notification Requirements (NH)

(definitions below are applicable to chart on reverse)

***Limited Data Set**

HIPAA permits covered entities to create a "limited data set" "for the purposes of research, public health, or health care operations." A "limited data set" is protected health information that excludes certain direct identifiers of information: Names; Postal address information, other than town or city, State, and 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 and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; and Full face photographic images and any comparable images.

If the inadvertently disclosed PHI is part of such a "limited data set," *and* also does not include dates of birth or zip codes, then there is no "breach" and no notification need take place.

****HIPAA Exceptions**

HIPAA contains three exceptions to the definition of "breach":

1) Unintentional acquisition, access or use of PHI by a workforce member of a covered entity or business associate if made in good faith and within the scope of authority and information is not further used or disclosed in a manner that is prohibited.

2) Inadvertent disclosure by a person who is authorized to access the PHI at a covered entity or business associate or organized health care arrangement to another at the same entity and the PHI is not further used or disclosed in a manner which is prohibited.

3) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

*****Personal Information (RSA 359-C)**

"Personal information" means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number.
- Driver's license number or other government identification number.
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

ADDITIONAL INFORMATION

Breach Notification Requirements (HIPAA)

Individual notification must occur without unreasonable delay and no later than 60 days after discovery

Covered entity's written notification of the breach must be written in plain language (may have to translate and communicate in Braille, large print, and audio as necessary), and include:

- Brief description of what happened;
- Date of the breach and date of discovery of the breach, if known;
- Description of information disclosed;
- Any steps individuals should take to protect themselves;
- Brief description of what the covered entity is doing to investigate the breach, mitigate any harm and prevent future breaches; and
- Toll free number, email address, website or postal address where individuals can receive additional information.

You do not necessarily need to indicate to whom PHI was disclosed, although you may need to do so to mitigate harm. In considering whether to indicate to whom PHI was disclosed, consider whether doing so would constitute a further breach.

Practical Tips for Handling Breaches

- Hire a forensic expert, if necessary.
- Notify your insurance carrier if you have insurance.
- Work with counsel, particularly if you lack experience in handling breaches. (Insurer may provide counsel.)
- Use a mailing company to assist with large mailings.
- Work with public relations staff.
- Designate contact person(s) to handle calls from patients and media.
- Make sure your policies are in order. A breach affecting 500 or more individuals will trigger an OCR investigation. Certain breaches may also trigger a Medicare review.

Website for reporting breaches of unsecured PHI to the Secretary of US DHHS: http://ocmotifications.hhs.gov/

Attachment F

NORTH COUNTRY HEALTHCARE

JOINT NOTICE OF PRIVACY PRACTICES

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 Joint Notice describes the privacy practices of the three hospital facilities and the home health and hospice agency that comprise the North Country Healthcare affiliated covered entity, or "ACE": Androscoggin Valley Hospital, Upper Connecticut Valley Hospital, Weeks Medical Center, and North Country Home Health and Hospice Agency, Inc. The ACE designation permits the members of the ACE to share health information which was created or received while you were a patient at one of the hospitals among themselves for purposes of treatment, payment or health care operations. This enables us to better address your health care needs.

In addition, each of the hospitals participates in an organized health care arrangement (OHCA) with independent practitioners on their medical staffs. Those independent practitioners participating in this arrangement have agreed to abide by the practices described in this Notice with respect to care they provide to you in the hospital and the medical information in your records at the hospital. The participants in each OHCA will share information with each other as necessary to carry out treatment, payment or health care operations relating to the OHCA.

This joint Notice applies to the three hospitals and home health and hospice agency comprising the North Country Healthcare ACE, and their OHCAs, at all of their service delivery sites. All service delivery sites are listed at the end of this Notice.

If you have any questions about this Notice, please contact the Privacy Officer listed toward the end of this Notice.

Protected Health Information ("PHI") is information, including demographic information, that may identify you and that relates to health care services provided to you, the payment of health care services provided to you, or your physical or mental health or condition, in the past, present or future. This Notice of Privacy Practices describes how we may use and disclose your PHI. It also describes your rights to access and control your PHI.

As providers of health care, we are required by Federal and state law to maintain the privacy of PHI. We are also required to notify you following a breach of the privacy of your PHI.

We are required to provide you with this Notice of our legal duties and privacy practices. We are required to abide by the terms of this Notice of Privacy Practices, but reserve the right to change the Notice at any time. Any change in the terms of this Notice will be effective for all PHI that we are maintaining at that time. We will provide you with any revised Notice of Privacy Practices upon request; you may either call the office and request that a revised copy be sent to you in the mail or ask for one at the time of your next appointment. We will also promptly post the revised Notice of Privacy Practices on our websites and at our facilities.

PERMITTED USES AND DISCLOSURES

General Rules

Federal law allows a health care provider to use or disclose PHI as follows:

- You. We will disclose your PHI to you, as the covered individual, at your request.
- Authorization. We will disclose your PHI pursuant to the terms of an authorization signed by you.
- Personal representative. We will disclose your PHI to a personal representative designated by law such as the parent or legal guardian of a child, agent under a durable power of attorney for health care, representative of the estate of a deceased individual, court-appointed guardian or, in certain circumstances, your surviving spouse or next of kin.
- Treatment. We will use and disclose your PHI to provide, coordinate, or manage your treatment. Treatment refers to the

provision and coordination or management of health care and related services by one or more health care providers, including consultation or referral, whether in person or via telemedicine. For example, we may disclose your PHI from time-to-time to another physician or health care provider (e.g., a specialist laboratory or pharmacy) who, at the request of your physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment.

- Payment. We may use and disclose your PHI in order to bill and collect payment for the treatment and services provided to you. Payment refers to the collection of premiums, reimbursements, coverage, determinations, billing, claims management, medical necessity determinations, utilization review, and preauthorization services. For example, we may provide portions of your PHI to our billing services provider and your health plan to get paid for the health care services we provided to you.
- Health care operations. We may disclose your PHI in order to operate our hospitals and the home health and hospice agency. Health care operations refer to specified administrative support activities by or for a health care provider, including quality assessment and improvement, peer review, training and credentialing of providers, and legal and auditing functions. For example, we may use your PHI in order to evaluate the quality of health care services that you received or to evaluate the performance of the health care professionals who provided health care services to you.
- Appointment reminders and other notifications. We may use or disclose your PHI, as necessary, to contact you to remind you of your appointment. We may use or disclose your PHI, as necessary, to provide you with information about treatment alternatives.
- Business Associates. We will share your PHI with third party "business associates" that perform various activities (for example, billing or transcription services) for the hospitals or the home health and hospice agency, including North Country Healthcare, Inc., the system parent. Whenever an arrangement with a business associate involves the use or disclosure of your PHI, we have a written contract that contains legally required terms that will protect the privacy of your PHI.
- Fundraising. We may send you fundraising notices and appeals, unless you opt out of receiving fundraising communications. With each communication, we will provide you with an opportunity to opt out of any further fundraising communications. Or, you may contact our Privacy Officer to opt out of fundraising communications.

Uses and Disclosures Allowed Without Authorization or Opportunity to Agree or Object

Federal law also allows a health care provider to use and disclose PHI, without your consent or authorization, or opportunity to agree or object, in the following ways:

- As required by law. When a disclosure is required by Federal, state, or local law, judicial or administrative proceedings, or by law enforcement. For example, we make disclosures when a law requires that we report information to government agencies and law enforcement personnel about victims of abuse, neglect, or domestic violence; when dealing with gunshot and other wounds; or when ordered in a judicial or administrative proceeding.
- For public health activities. For example, we report information about births, deaths, and various diseases to government officials in charge of collecting that information, and we may provide coroners, medical examiners, and funeral directors necessary information relating to an individual's death.
- For health oversight activities. For example, we will provide information to assist the government when it conducts an investigation or inspection of a health care provider or organization.
- For purposes of organ donation. We may notify organ procurement organizations to assist them in organ, eye, or tissue donation and transplants.
- For research purposes. In certain circumstances, we may provide PHI in order to conduct medical research.
- To avoid harm. In order to avoid a serious threat to the health or safety of a person or the public, we may provide PHI to law enforcement personnel or persons able to prevent or lessen such harm.
- For specific government functions. We may disclose PHI of military personnel and veterans in certain situations. And, we may disclose PHI for national security purposes.
- For workers' compensation purposes. We may provide PHI in order to comply with workers' compensation laws.
- Correctional Institutions. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release PHI about you to the correctional facility or law enforcement official, under certain, limited circumstances permitted by law. These situations may arise when the institution needs to offer you healthcare services, ensure the health and safety of you and others, or maintain the security of the correctional facility.

The examples of permitted uses and disclosures listed above are not provided as an all-inclusive list of the ways in which PHI may be used. They are provided to describe in general the types of uses and disclosures that may be made.

Permitted and Required Uses and Disclosures That May Be Made with Your Authorization or Opportunity to Object

We may use and disclose your PHI in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your PHI. If you are not present or able to agree or object to the use or disclosure of the PHI, then your physician may, using professional judgment, determine whether the disclosure is in your best interest. In this case, only the PHI that is relevant to your health care will be disclosed.

- Others Involved in Your Healthcare. If you agree or do not object, we may disclose to a member of your family, a relative, a close personal friend or any other person you identify, your PHI that directly relates to that person's involvement in your health care or payment for your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We also may use or disclose your PHI to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your health care.
- Directories. We may maintain a directory of patients that includes your name and location within the facility, your religious affiliation, and information about your condition in general terms that will not communicate specific medical information about you. Except for your religious affiliation, we may disclose this information to any person who asks for you by name. We may disclose all directory information to members of the clergy. You have the right to object, in writing, upon admission to the hospital, and any time during hospitalization, to the use or disclosure of your medical information from the hospital directory to family members, friends, visitors, clergy, and others who may ask for you by name, and, if you do so, we will follow your wishes. As allowed by law, we may use your personal information from the hospital directory in the event you are incapacitated or undergoing emergency medical treatment, but only consistent with your prior expressed wishes.
- Following your death. After your death, we may disclose to a member of your family, a relative, a close personal friend or any other person you identify, your PHI that directly relates to that person's involvement in your health care or payment for your health care prior to your death. We will not make such disclosures to the extent you inform us, prior to your death, that you object to some or all such disclosures. Notwithstanding the above, when there is no estate administration, the surviving spouse or next of kin of the deceased will be designated your personal representative for the limited purpose of obtaining your medical records if the requestor provides us with (a) a notarized affidavit indicating that they are authorized to access your records; (b) a signed NCH authorization for use and disclosure of PHI; and (c) a copy of your death certificate.

ALL OTHER USES AND DISCLOSURES REQUIRE YOUR PRIOR WRITTEN AUTHORIZATION

In any other situation not described in this notice, we will ask for your written authorization before using or disclosing any of your PHI. If you choose to sign an authorization to disclose your PHI, you can later revoke that authorization in writing to stop any future uses and disclosures.

Specific examples of uses or disclosures that require authorization include:

- Psychotherapy Notes. Most uses and disclosures of psychotherapy notes require your written authorization. "Psychotherapy notes" are the recorded notes (in any form) of a mental health professional that document or analyze the contents of conversations during a counseling session, if kept separately from the rest of your medical record.
- Sensitive Data. Some information, such as HIV information, genetic information, reproductive health information, and mental health information is entitled to special restrictions related to its use and disclosure.
- Marketing. Uses and disclosures of your PHI for marketing require your written authorization. Marketing is a communication that encourages you to purchase or use a product or service. However, it is not marketing if we communicate with you about health-related products or services that we offer, as long as we are not paid by a third party for making the communication. Nor is your written authorization required for us to communicate with you face-to-face or for us to give you a gift of nominal value.
- Sale. We may not sell your PHI without your written authorization, except as permitted by law.

YOUR RIGHTS IN RELATION TO PROTECTED HEALTH INFORMATION

You have the following rights with respect to your PHI:

- To Request Restrictions. You have the right to request restrictions on the use and disclosure of your PHI for treatment, payment, or health care operations purposes or notification purposes. We are not required to agree to your request, with one exception: If you have paid out of pocket and in full for a health care item or service, you may request that we not disclose your health information related to that item or service to a health plan for purposes of payment or health care operations. If you make such a request, we will not disclose your information to the health plan unless the disclosure is otherwise required by law. If we do agree to a restriction, we will abide by that restriction unless you are in need of emergency treatment and the restricted information is needed to provide that emergency treatment. To request a restriction, submit a written request to the Privacy Officer listed on the final page of this Notice.
- Alternative Modes of Communication. You have the right to ask that we send PHI to you at an alternate address (for example, sending information to your work address rather than your home address) or by alternate means (for example, e-mail instead of regular mail). We must agree to your request so long as we can easily provide it in the format that you request.
- Access. In most cases, you have the right to look at or obtain copies of your PHI that we have, but you must make the request in writing. You also have the right to have us provide a copy of your PHI directly to another person whom you designate by providing us with a completed authorization form. You are also entitled to an electronic copy of your Electronic Health Record ("EHR"), if one exists. We will respond to you within 30 days after receiving your written request. In certain situations, we may deny your request. If we do, we will tell you, in writing, our reasons for the denial and explain your right to have the denial reviewed.
- Copies. If you request paper copies of your PHI, we may charge you a reasonable, cost-based fee for each page in accordance with state and federal law. For EHR, you may be charged the cost of labor to produce the electronic copy or make the electronic transmission, and the cost of any portable media device on which the copy is provided. Instead of providing the PHI you requested, we may provide you with a summary or explanation of the PHI as long as you agree to that and to the cost in advance.
- Accounting of Disclosures. You have the right to an accounting of instances in which we have disclosed your PHI for a period of up to six years prior to the date of the request, except for certain disclosures, including disclosures that you have authorized, and disclosures made for the purpose of carrying out treatment, payment, or health care operations. We will respond within 60 days of receiving your request. The list we will give you will include disclosures made in the last six years unless you request a shorter time. The list will include the date of the disclosure, to whom PHI was disclosed (including their address, if known), a description of the information disclosed, and the reason for the disclosure. We will provide the list to you at no charge, but if you make more than one request in the same year, we will charge you a reasonable fee for each additional request.
- Amendment of Records. If you believe that there is a mistake in your PHI or that a piece of important information is missing, you have the right to request that we correct the existing information or add the missing information. You must provide the request and your reason for the request in writing. We will respond within 60 days of receiving your request. We may deny your request in writing if the PHI is (i) correct and complete, (ii) not created by us, (iii) not allowed to be disclosed, or (iv) not part of our records. Our written denial will state the reasons for the denial and explain your right to file a written statement of disagreement with the denial. If you do not file one, you have the right to request that your request and our denial be attached to all future disclosures of your PHI. If we approve your request, we will make the change to your PHI, tell you that we have done it, and notify others that need to know about the change to your PHI.
- Paper Notice. You have the right to request a paper copy of this Notice.
- To Receive Notice of Breach. You have the right to be notified upon a breach of any of your unsecured health information.

Information relating to your substance use disorder ("SUD") care is protected by federal regulations to SUD, which are issued by a government agency called "SAMHSA" and found at 42 C.F.R. Part 2. (They are often referred to simply as "Part 2"). These regulations protect the confidentiality of information relating to the identity, diagnosis, prognosis, or treatment of any client with a SUD. NCH and its affiliated entities may not disclose records relating to your SUD treatment without your written consent, except in narrowly limited circumstances. Pursuant to Part 2, the terms of a written consent to disclose information must specify the scope and types of SUD information to be disclosed, the parties to whom the information may be disclosed, the purpose of the disclosure and the timeframe of the consent. You may revoke a consent to disclose information relating to SUD care verbally or in writing at any time. NCH and its affiliated entities use one form for

authorization of release of medical records and SUD, in order to simplify the authorization process. The form has a special SUD release section.

NCH and its affiliated entities may ask for your written consent to disclose SUD treatment information in certain circumstances, including releasing treatment information to or obtaining information from your other medical providers, obtaining payment from insurance or other payors, or contacting your family either for treatment purposes or in the case of a medical or other emergency. NCH and its affiliated entities will not disclose your treatment information for these purposes without your consent.

In certain very limited situations, NCH and its affiliated entities may disclose treatment information without your written consent, as allowed under Part 2. For treatment purposes, NCH and its affiliated SUD entities only are permitted to use and disclose treatment information internally and to entities with which your SUD provider shares administrative control. NCH and its affiliated entities are permitted to share treatment information as necessary with qualified service organizations that agree to maintain the confidentiality of the information. NCH and its affiliated entities also may disclose treatment information to outside auditors, regulatory agencies and evaluators and for certain research purposes. NCH and its affiliated entities may disclose treatment information without your written consent when necessary in a life-threatening medical emergency and may disclose to report a crime on the premises or against NCH and/or affiliated entity staff. NCH and its affiliated entities also may disclose client information without consent where the State mandates child abuse and neglect reporting; when cause of death is being reported; or when required by a valid court order that contains specific required findings. NCH and its affiliated entities may contact you to share information about NCH and its affiliated entities' treatment services or to send you reminder notices of future appointments for your treatment.

Violations of SAMHSA's protections are not legal, and may be reported to:

Bureau of Drug and Alcohol Services
N.H. Department of Health and Human Services
105 Pleasant St.
Concord, NH 03301

PRIVACY OFFICER

Our Privacy Officer may be reached by mail, phone or email at:

Privacy Officer
8 Clover Lane
Whitefield, NH 03598
Phone:603-326-5608 | *Email*: privacy@northcountryhealth.org

COMPLAINTS

You may complain to us or to the Secretary of the U.S. Department of Health and Human Services if you believe your privacy rights have been violated by us. We will not retaliate against you for filing a complaint. You may contact our Privacy Officer at 603-326-5608 for further information about the complaint process.

EFFECTIVE DATE OF NOTICE

This Notice was published and becomes effective on October 30, 2024.

SERVICE LOCATIONS

This joint Notice applies to the three hospitals and home health and hospice agency comprising the North Country Healthcare ACE, and their OHCAs, at all of their service delivery sites. These include the following locations:

Androscoggin Valley Hospital 59 Page Hill Road Berlin, NH 03570	**North Country Home Health and Hospice Agency, Inc.** 536 Cottage Street Littleton, NH 03561
AVH Surgical Associates 59 Page Hill Road Berlin, NH 03570	NCH Home Medical Supplies 252 Meadow Street Littleton, NH 03561
AVH Surgical Associates 7 Page Hill Road Berlin, NH 03570	**Weeks Medical Center** 173 Middle Street Lancaster, NH 03584
AVH Outreach Laboratory Coos County Family Health Services 133 Pleasant Street Berlin, NH 03570	Lancaster Patient Care Center 173 Middle Street Lancaster, NH 03584
AVH Outreach Laboratory Coos County Family Health Services 2 Broadway Street Gorham, NH 03581	Whitefield Patient Care Center 8 Clover Lane Whitefield, NH 03598
NCH Patient Care Center 167 Main Street Gorham, NH 03581	Groveton Patient Care Center 47 Church Street Groveton, NH 03582
NCH Patient Care Center 1976 White Mountain Highway, Suite 110B North Conway, NH 03860	Littleton Patient Care Center 536 Cottage Street Littleton, NH 03561
AVH Surgical Associates Outreach Clinics Weeks Medical Center 173 Main Street Lancaster, NH 03584	Stewartstown Patient Care Center 6 Duranleau Street West Stewartstown, NH 03597
AVH Surgical Associates Outreach Clinics Upper Connecticut Valley Hospital 181 Corliss Lane Colebrook, NH 03576	Colebrook Patient Care Center 141 Corliss Lane Colebrook, NH 03576
Upper Connecticut Valley Hospital 181 Corliss Lane Colebrook, NH 03576	Weeks Medical Center and The Doorway 7 Page Hill Road Berlin, NH 03570

Attachment G

Request for Amendment of Medical or Billing Records

Patient Name:_____ Date of Birth:_____

Medical Record Number (if known):_____ Phone Number:_____

Address:_____ City:_____ State:_____ Zip Code:_____

Facility where the records are located:

☐ Androscoggin Valley Hospital (AVH) ☐ North Country Home Health and Hospice Agency (NCHHHA)
☐ Upper Connecticut Valley Hospital (UCVH) ☐ Weeks Medical Center (WMC)

Describe the information that you would like to be amended (e.g. physician notes, lab test results):_____

On what date(s) was the care that is described in the record provided?_____

What is incorrect about the record? What would you like to change/add to the record?_____

To your knowledge, has anyone received or relied on this information (i.e., your doctor, another healthcare provider, an insurance company)? If yes, please provide the name(s) and address(es) of those individuals or organizations so that we may inform them of any amendments._____

Signature:_____ Date:_____

If you are not the patient, please fill in the following:

Name:_____ Relationship to Patient:_____

Address:_____ City:_____ State:_____ Zip Code:_____

Phone Number:_____

Signature:_____ Date:_____

Attachment H

Request for Restrictions on the Use and Disclosure of Protected Health Information

Patient Name:_____ Date of Birth:_____

I understand that:

1. There are legal restrictions on the manner in which NCH may use or disclose health information about me.

2. Under certain circumstances, I have the right to request additional restrictions on the way in which NCH uses or discloses my health information, in addition to the restrictions already imposed by law.

3. NCH is not required to grant my request for additional restrictions, unless: (a) the request relates to disclosures to a health plan; (b) the disclosure is for purposes of carrying out payment or health care operations; (c) the disclosure is not otherwise required by law; and (d) the health information pertains solely to a health care item or service for which I, or someone on my behalf other than the health plan, have paid the hospital in full.

4. If NCH does grant my request for restrictions, the restricted information will not be used or disclosed except to provide treatment to me in an emergency.

5. NCH and I can terminate our agreement to a restriction at any time by notifying the other party. If NCH terminates its agreement to a restriction, it will notify me, and will continue to comply with the restriction for any information that was created prior to the date of termination.

6. I request the following restrictions with respect to my protected health information:

_____

_____

_____

_____

_____

_____ _____
Patient Signature (or Patient Representative) Date

_____ _____
Privacy Officer Signature (or Patient Representative) Date

Attachment I

Privacy Compliant Form

Patient Name:_____ Date of Birth:_____

Medical Record Number (if known):_____ Phone Number:_____

Address:_____ City:_____ State:_____ Zip Code:_____

Please describe the nature of your concerns (be as specific as possible including, dates, times, and individuals or dates of care involved):

_____

_____

_____

_____

_____

_____

What response do you desire, if any?

_____

_____

_____

_____

_____

Do you know of anyone who may have received protected health information? ☐ Yes ☐ No

If yes, who?_____

Signature:_____ Date:_____

If you are not the patient, please fill in the following:

Name:_____ Relationship to Patient:_____

Address:_____ City:_____ State:_____ Zip Code:_____

Phone Number:_____

Signature:_____ Date:_____

Attachment J

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made as of this _____ day of _____, 20____, by and between North Country Healthcare, Inc. ("Covered Entity"), and _____ ("Business Associate").

WHEREAS, the Covered Entity has engaged the Business Associate to perform services for the Covered Entity and/or one of its affiliates (Androscoggin Valley Hospital, North Country Home Health and Hospice Agency, Upper Connecticut Valley Hospital, and Weeks Medical Center) as described in the underlying agreement between them (the "Services Agreement"); and

WHEREAS, pursuant to the Services Agreement, the Covered Entity may disclose Protected Health Information to the Business Associate and the Business Associate may receive, use, disclose, transmit, store and/or maintain such Protected Health Information in its performance of services for the Covered Entity; and;

WHEREAS, the Covered Entity and the Business Associate intend to comply with all applicable federal and state laws governing the privacy of Protected Health Information, including but not limited to: (1) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); (2) the HIPAA Privacy Regulations set forth at 45 C.F.R. Part 160 and Part 164, Subparts A and E; (2) the HIPAA Security Regulations set forth at 45 C.F.R. Part 160 and Part 164, Subparts A and C; (3) the Transactions and Code Set Standards set forth at 45 C.F.R. Part 162; (4) the Health Information Technology for Economic and Clinical Health Act; and (5) the New Hampshire Right to Privacy Law, codified at RSA Chapter 359-C:19-21;

NOW THEREFORE, in consideration of the mutual covenants contained in this Agreement and intending to be legally bound, the parties agree as follows:

Section 1. Definitions

(a) "Protected Health Information" shall have the same meaning as set forth in the HIPAA Privacy Regulations, and is recognized by the parties to include both (1) Electronic Protected Health Information; and (2) Personal Information as that term is defined in the New Hampshire Right to Privacy Law.

(b) Capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Privacy Regulations and HIPAA Security Regulations.

Section 2. Obligations and Activities of Business Associate

Business Associate agrees to:

(a) not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law;

(b) use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement;

(c) mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement;

(d) immediately report to Covered Entity any use or disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware, with such reports including at least the following information:

(1) the identity of each individual whose information was accessed, acquired or disclosed during the improper use or disclosure;

(2) a brief description of what happened;

(3) the date of the improper use or disclosure and the date of its discovery;

(4) the nature of the Protected Health Information that was involved (e.g., social security numbers, date of birth, etc.);

(5) any steps individuals should take to protect themselves from potential harm resulting from the improper use or disclosure; and

(6) a brief description of what the Business Associate is doing to investigate the improper use or disclosure, to mitigate harm to individuals, and to protect against any further incidents;

(e) in accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree in writing to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

(f) make available to Covered Entity Protected Health Information in a Designated Record Set as necessary to allow Covered Entity to satisfy its obligations under 45 C.F.R. §164.524 to provide Individuals with access to their Protected Health Information;

(g) make available to Covered Entity Protected Health Information in a Designated Record Set for amendment and incorporate any amendments made by Covered Entity in accordance with 45 C.F.R. § 164.526;

(h) make available to Covered Entity the information required to allow Covered Entity to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528. This provision shall survive termination or expiration of this Agreement;

(i) make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the federal Department of Health and Human Services ("HHS") for purposes of HHS determining Covered Entity's compliance with the Privacy Regulations. Business Associate agrees to notify the Covered Entity promptly of communications with HHS regarding Protected Health Information covered by this Agreement and to provide Covered Entity with copies of any information Business Associate has made available to HHS under this provision;

(j) to the extent the Business Associate is to carry out one or more of Covered Entity's obligations under the HIPAA Privacy Regulations, comply with the requirements of the Privacy Regulations that apply to the Covered Entity in the performance of such obligations;

(k) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity, and otherwise comply with the HIPAA Security Regulations with respect to such electronic Protected Health Information, to prevent uses or disclosures of Protected Health Information other than as provided for by this Agreement (Business Associate recognizes that civil and criminal penalties for violation of the HIPAA Security Rule apply to a Business Associate in the same manner as they apply to a Covered Entity);

(l) immediately report to Covered Entity any Security Incident;

(m) refrain from storing, processing or otherwise handling or using Protected Health Information outside the United States and its territories (i.e., "offshore" activities), and refrain from engaging any subcontractor who conducts any such offshore activities, unless Covered Entity approves in writing a specific offshore activity. Notwithstanding any provision in the underlying Services Agreement or this Agreement, Business Associate will indemnify Covered Entity against any and all liability based on the improper use or disclosure of Protected Health Information resulting from the offshore activity; and

(n) cooperate with the Covered Entity in investigating and taking prompt corrective action to prevent or cure any violation of any federal or state law governing Protected Health Information.

Section 3. Permitted Uses and Disclosures by Business Associate

(a) General Use and Disclosure Provisions

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity pursuant to the underlying Services Agreement between the parties, provided that such use or disclosure would not violate the Privacy Regulations if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

(b) Specific Use and Disclosure Provisions

(1) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(2) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(3) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 C.F.R. § 164.504(e)(2)(i)(B).

(4) Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

Section 4. Obligations of Covered Entity

Covered Entity shall:

(a) notify Business Associate of any limitation(s) in its Notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information;

(b) notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or

disclosure of Protected Health Information;

(c) notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Section 5. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Regulations if done by Covered Entity.

Section 6. Term and Termination

(a) Term. The Term of this Agreement shall be effective as of the effective date of the underlying Services Agreement between the parties and shall terminate upon the earlier of:

(1) expiration or termination of the underlying Services Agreement; or

(2) termination of this Agreement for cause by the Covered Entity as authorized by subsection (b) below.

(b) Termination for Cause. Upon either party's knowledge of a material breach by the other party, the non-breaching party shall either:

(1) provide an opportunity for the breaching party to cure the breach or end the violation and terminate this Agreement if the breaching party does not cure the breach or end the violation within the time specified by non-breaching party; or

(2) immediately terminate this Agreement if the breaching party has breached a material term of this Agreement and cure is not possible.

(c) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) Business Associate shall complete such return or destruction as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, Business Associate shall provide a letter to Covered Entity certifying that all possible records have been returned to Covered Entity or destruction has been completed. If Business Associate destroys Protected Health Information, it shall be done using technology or a methodology that renders the Protected Health Information unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in HHS guidance.

(3) In the event that Business Associate determines that returning or destroying the Protected Health Information is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return, or destruction of Protected Health Information is not feasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further

uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Section 7. Miscellaneous

(a) Regulatory References. A reference in this Agreement to a section in the Privacy Regulations or Security Regulations means the section in effect, or as amended.

(b) Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of applicable law governing Protected Health Information.

(c) Interpretation. Any ambiguity in this Agreement shall be resolved to permit the parties to comply with applicable law governing Protected Health Information.

(d) Indemnification. Each party agrees to indemnify and hold harmless the other party and its affiliated organizations, and their Board members, officers, agents, and employees, from any and all claims of any kind, including costs, expenses and attorney fees, which arise as a result of the negligence or intentional misconduct of, or breach of this Business Associate Agreement by, the indemnifying party or its Board members, officers, agents or employees. This subsection will survive termination or expiration of this Agreement. Any limitation of liability provision set forth in the underlying Services Agreement shall not apply to the indemnification obligation described in this subsection.

(e) Qualified Service Organizations. If any Part 2 Program of the Covered Entity or its affiliates discloses Protected Health Information to Business Associate that is subject to the rules set forth in 42 C.F.R. Part 2 ("Confidentiality of Alcohol and Drug Abuse Patient Records") because it involves diagnosis, treatment or referral for treatment of alcohol abuse and/or drug abuse, Business Associate acknowledges that it will be a "qualified services organization" under 42 C.F.R. § 2.11. Accordingly, Business Associate will not re-disclose such information except as permitted by 42 C.F.R. Part 2, and will otherwise comply with such rules in receiving, storing, processing or otherwise dealing with any Protected Health Information covered by them. Further, if necessary, Business Associate will resist in judicial proceedings any effort to gain access to such patient records except as permitted by these rules.

(f) No Waiver of Privilege. Neither Covered Entity nor Business Associate is waiving any legal privilege, including but not limited to the attorney/client privilege, by virtue of any provision in this Agreement.

(g) Inconsistencies. To the extent of any inconsistencies between the Services Agreement and this Agreement, this Agreement shall be controlling.

The parties have caused this Agreement to be executed on the date first written above.

DATE:_____

NORTH COUNTRY HEALTHCARE, INC.

BY:_____

_____
Print Name

_____
Title

DATE:_____

[BUSINESS ASSOCIATE]

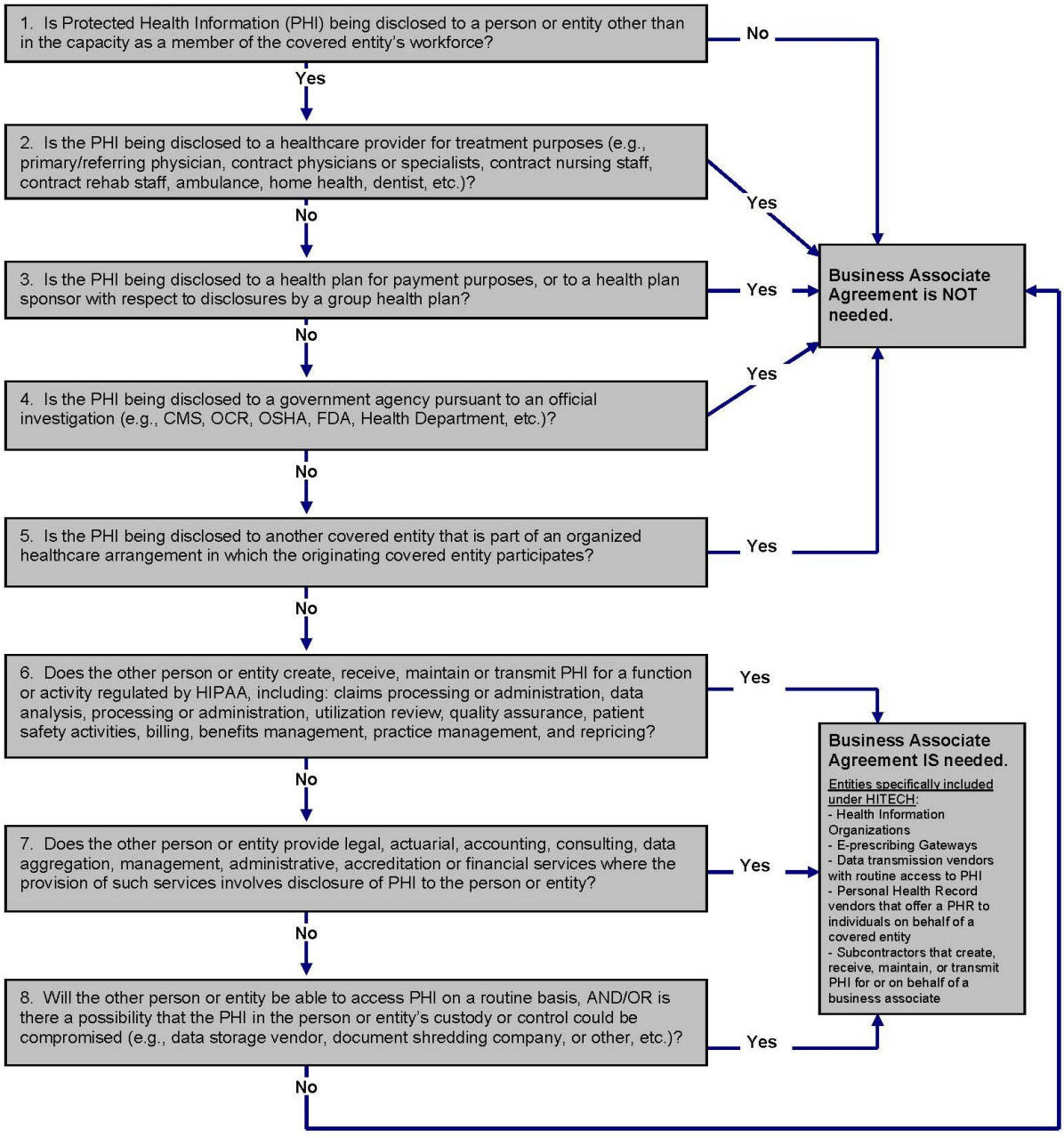
BY:_____

_____
Print Name

_____
Title

Attachment K

HIPAA/HITECH
Business Associate Decision Tree



Attachment L

Confidentiality Attestation

I have received a communication containing protected health information (PHI) that belonged to the medical record of another patient. I understand that North Country Healthcare and its affiliates have a legal duty to protect the privacy of patient information under a federal law known as HIPAA. Accordingly, I acknowledge the following:

1. *Confidentiality Requirement:* I understand that the information I have received is confidential and protected under the Health Insurance Portability and Accountability Act (HIPAA) and other applicable privacy laws. I agree to maintain the confidentiality of this information.

2. *Restriction on Use and Disclosure:* I agree not to use, disclose, or share any of the received information with anyone else. I will not discuss, display, or otherwise disseminate this information in any manner.

3. *Return of Information:* I have returned the information or attest that the information has been destroyed in a HIPAA compliant manner.

4. *Acknowledgment of Understanding:* By signing this attestation, I acknowledge that I have read and understood the confidentiality requirements associated with the information I have received and agree to comply with them.

_____ _____
Signature Date

_____
Printed Name