NeHII, Inc.
PRIVACY POLICIES

NeHII, Inc. wishes to express its gratitude to Connecting for Health and the Markel Foundation for their work in developing the Common Foundation: Resources for Implementing Private and Secure Health Information Exchange. This work incorporates some of the concepts set forth in those resources.

Table of Contents

NeHII Privacy Policies

INTRODUCTION

The following policies apply to the access, use and disclosure of protected health information by Participants through the NeHII Record Locator Service ("RLS") and other data exchange services being made available to Participants in NeHII (the RLS and other services are collectively referred to as the "System"). These are initial policies designed for use during the Pilot Phase when NeHII and certain Participants will be testing with live data. It is anticipated these policies will be reviewed and revised as needed based on the experience of NeHII and Participants during the Pilot Phase.

These NeHII Privacy Policies ("Privacy Policies") are rooted in nine privacy principles discussed in the **Connecting for Health** "Architecture for Privacy in a Networked Health Information Environment" and a tenth added by NeHII that, taken together with privacy policies and procedures already deployed by Participants as covered entities under HIPAA, form a comprehensive array of administrative safeguards addressing privacy of protected health information. NeHII has modeled its Privacy Policies on the **Connecting For Health** "Model Privacy Policies and Procedures for Health Information Exchange," with a number of differences based on state law, physical and technical safeguards available through NeHII, and NeHII's unique operating environment.

These core privacy principles and the policies that flow from them promote balance between consumer control of and access to health information and the operational need of covered entities to ensure that information uses and disclosures are not overly restricted, such that consumers would be denied many of the benefits and improvements that information technology can bring to the health care system. The policies are intended to reflect a carefully balanced view of all of the principles and avoid emphasizing some over others in any way that would weaken the overall approach. The guiding NeHII privacy principles are as follows:

Openness and Transparency. Openness about procedures, policies, developments, and technology concerning the handling of protected health information is vital to protecting privacy. Individuals should be able to understand what information exists about them, how the protected health information is used, and how they can control use of that information. Openness and transparency helps promote privacy practices and gives individuals confidence with regard to privacy of protected health information, which in turn can help increase consumer participation in health information networks.

Purpose Specification and Minimization. Access to and use of patient health information must be limited to the type and amount necessary to accomplish specified permitted purposes. Minimizing the use of patient health information will help decrease the amount of privacy violations, which may occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

Disclosure Limitation. Protected health information should be made available through the NeHII System to NeHII and Participants only by lawful means, and, if applicable, with the knowledge and permission of the individual. It is important that individuals are aware of how information concerning them is being collected in an electronic networked environment. Individuals should be educated about the potential health and treatment benefits as well as risks to their protected health information that are associated with participation in the System. Individuals deciding not to participate should have the opportunity to know the System-wide effect of such decision and the potential disadvantages.

Access and Use Limitation. Protected health information should be accessed by one Participant from another Participant only pursuant to mutual agreement that the information will be used by the second Participant: (i) for the treatment, payment, or health care operations purposes of the Participant who disclosed it, (ii) the treatment, payment or health care operations purposes of the Participant who accessed it, or (iii) as specifically permitted by §164.512 of the Privacy Rule (Uses and Disclosures For Which Consent, an Authorization, or Opportunity to Agree or Object is Not Required), permitted under these Policies and approved by the Privacy and Security Committee. Information recipients may use and disclose protected health information obtained through the System only for purposes and uses consistent with their permitted access and consistent with their obligations as covered entities under HIPAA. Certain exceptions, such as for law enforcement or public health, may warrant reuse of information for other purposes. However, when information obtained by a Participant through the System is used for purposes other than those for which the information was originally obtained, the Participant so using or disclosing the information should first apply the rules applicable to it as a covered entity under HIPAA and as a contracting Participant.

Individual Participation and Control. Consistent with the scope of individual rights in HIPAA, individuals should have the right to request and receive in a timely and intelligible manner information regarding various parties that may have that individual's specific protected health information; to know any reason for a denial of such request; to request to amend any protected health information that the individual believes is inaccurate; and to request not to have his or her information made available through the System. Individuals have a vital stake in personal protected health information, such rights enable individuals to make informed decisions about participation and provide another means to monitor for inappropriate access, use and disclosure of protected health information. Individual participation promotes information quality, privacy, and confidence in privacy practices.

Data Integrity and Quality. Health information should be detailed, complete, appropriate, and current to guarantee its value to the various parties. The effective delivery of quality health care depends on complete health information. In addition, individuals can be negatively affected by inaccurate health information in other contexts, such as insurance and employment. Therefore, the System must maintain the integrity of protected health information and individuals must be allowed to view information

about them and request to amend such health information so that it is accurate and complete.

Security Safeguards and Controls. Security safeguards are essential to privacy protection, because they help prevent information loss, corruption, unauthorized use, modification, and disclosure. With increasing levels of cyber-crime, networked environments may be particularly susceptible without adequate security controls. Privacy and security safeguards should work together and be well coordinated for the protection of patient health information.

Accountability and Oversight. Privacy protections have less value to an individual if privacy violators are not held accountable for failing to follow procedures relating to such privacy protections. Potential Participants, such as those who will provide data to the System, are unlikely to fully trust the System and fully participate, if they believe other Participants are not applying the same rules and being held to the same standard of accountability. User and workforce training, privacy audits, and other oversight tools can help to identify and address privacy violations and security breaches by conditioning participation and access authority on compliance with these and the individual Participant's privacy policies, by excluding from participation those who violate privacy requirements, and by identifying and correcting weaknesses in privacy and security safeguards.

Remedies. To ensure privacy protection there must be legal and financial remedies that hold violators accountable for failing to comply with System policies. Such remedies will give individuals confidence in the organization's commitment to keeping protected health information private, and mitigate any harm that privacy violations may cause individuals. As a condition of continued participation, All Participants in the System must have a common duty to participate in investigation, mitigation and remediation steps for the integrity of the System.

Reliance on Covered Entity Policies and Enforcement. While NeHII should have a number of core policies and procedures for the benefit and confidence of all Participants, NeHII should not try to replace policies, procedures and methods already adopted by Participants as covered entities under HIPAA. NeHII should identify, disseminate and enforce only those policies and procedures necessary for coordination of privacy response, but should recognize that existing Participant policies govern in all other areas.

These ten principles underlie the NeHII privacy policies. Given the advanced level of technology available to most organizations, a majority of the policies should be relatively manageable to implement. In some cases, however, organizational and technical barriers may restrict an organization's ability to implement the policies. For example, the System does not currently allow a patient to access the System and see an audit trail of those parties that have requested information about the patient. Patients could potentially benefit from such information, and such options should be implemented to promote the principles of openness and transparency, security

safeguards and controls, purpose specification and minimization, disclosure limitation, collection limitation, and accountability.

The creation of a networked electronic health information environment will provide for more efficient and effective delivery of patient care. However, the creation of an electronic network that includes a massive volume of protected health information that can be easily collected and disseminated must have adequate privacy and security measures. NeHII policies incorporate principles outlines in the ten principles as well as basic requirements set forth in HIPAA. The NeHII policies seek to achieve a balance between maintaining the confidentiality of protected health information and maximizing the benefits of such information.

STATUS OF NEHII AND PARTICIPANTS

Participants – those which provide data to the System and those which obtain and use data from the System – are either health care providers, health plans, or health care clearinghouses. All Participants are covered entities under HIPAA or agree to be contractually bound to follow all HIPAA rules and regulations as though they were a covered entity.

NeHII is a business associate ("BA") of the Participants. NeHII accepts and agrees to follow terms applicable to the privacy of protected health information by virtue of its business associate agreement with each Participant and these privacy policies.

EFFECT OF LEGISLATION AND RULE CHANGES

NeHII and Participants need to remain flexible in approach in order to adapt to the uncertainty of state and federal legislation and regulations that will affect design, safeguards, rights and responsibilities over time. This shall include monitoring and implementing design components and safeguards mandated in the Health Information Technology for Economic and Clinical Health Act or “HITECH” as enacted in P.L 111-5 and regulations to be issued thereunder.

SAFEGUARDS IN AN ELECTRONIC NETWORKED ENVIRONMENT

HIPAA permits covered entities that hold protected health information to disclose such information to third parties for the *disclosing entity's* own treatment, payment and health care operations[1]. Using payment as an example, a provider Participant can send a bill (a health care claim or equivalent encounter transaction) to a health plan for the provider's own payment purposes, along with the protected health information needed to support the claim.

When the health plan is also a NeHII Participant, the parties can avoid requiring the provider having to actually send the supporting information or respond to requests for additional information, because the NeHII System lets the receiving health plan directly access the provider's records and obtain the needed information electronically.

[1] 45 C.F.R. § 164.506(c)(1).

The disclosure by the provider in this example is for *its* payment purpose ("obtain reimbursement") and the access and use by the health plan in this example is for *its* payment purpose ("provide reimbursement").

HIPAA also permits covered entities that hold protected health information to disclose such information to other covered entities (or providers in the case of treatment) *for the receiving party's* treatment, payment or health care operations.[2] For example, subject to safeguards and conditions:

- A provider can furnish insurance and demographic information to the office of the on-call physician who attended the patient the previous night to permit the physician to submit a bill for professional services. This is a disclosure for the recipient's payment purposes.

- A provider can furnish data to a covered health plan at the request of the health plan to enable the health plan to measure effectiveness of a disease management system implemented by the health plan and deployed at the provider. This is a disclosure for the health plan's health care operations. A provider can furnish protected health information specific to a covered plan's covered lives.

In a non-electronic networked environment, the disclosing Participants in the examples above would have the opportunity to examine third party access or requests for information beforehand and make an individual determination whether a requested access or disclosure is a permitted disclosure for the treatment, payment, or qualifying health care operations purposes of the disclosing or requesting Participant or for those purposes specifically permitted by §164.512(b) of the Privacy Rule and permitted under these policies.

In an electronic networked environment, such as NeHII, the disclosing Participant will not receive or "process" a request for disclosure. The other Participant that needs the information, using the RLS, can simply locate the Participant's records and access them as needed. The human element of analyzing individual requests is absent.

Accordingly, to permit Participants that disclose information or whose information is accessed to meet their obligation under HIPAA, and to address the need for safeguards, NeHII and Participants have placed the burden on the *requesting* Participant to access information from the record of the *disclosing* Participant only:

- When necessary and requested for the treatment, payment or health care operations of the *disclosing* Participant (for example, to pay a claim submitted by the disclosing Participant or to render a consult requested by the disclosing Participant); or

[2] 45 C.F.R. § 164.506(c)(2), (3) and (4).

- When necessary for the treatment, payment or "qualifying"[3] health care operations of the *receiving* Participant (for example, to obtain information needed to submit a claim or to obtain information needed to assess provider performance); or

- When the disclosure by the *disclosing* Participant is specifically permitted by §164.512(b) of the Privacy Rule and these Policies; and

- In all cases, subject to the conditions and safeguards described in these Policies. In connection with disclosure for any payment or health care operations purposes, regardless of whether they are the payment or health care operations of the disclosing or receiving Participant, these conditions and safeguards include meeting the minimum necessary standard.

- As an additional safeguard, all Participants must be covered entities under HIPAA and therefore individually subject to regulation and penalties.

- Participants may access PHI of others only for permitted purposes.

Special rules and conditions apply when a disclosure is for the health care operations of the receiving Participant, and these are discussed in Policy 400.

[3] Only a narrow subset of health care operations supporst disclosure for the health care operations uses of the recipient. This is discussed in detail in the next Section "Special Rules for Disclosure For The Health Care Operations Of the Recipient".

NeHII Privacy
Policy 100: Compliance with Law and Policy

Scope and Applicability: This Policy applies to NeHII and all Participants.

Policy:

1. Laws. Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of protected health information and establishing certain individual privacy rights. Each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure compliance.[2]

2. NeHII Policies. Each Participant shall, at all times, comply with these NeHII Policies ("NeHII Policies"). These NeHII Policies may be changed and updated from time to time upon reasonable written notice to Participants. Amendment shall be effective when adopted by the NeHII Board of Directors, ordinarily following input by the NeHII Privacy and Security Committee. NeHII shall notify Participants of all policy changes. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these NeHII Policies.

3. Participant Policies. Each Participant is responsible for ensuring that it has the appropriate and necessary internal policies for compliance with applicable laws and these NeHII Policies.

4. Participant Criteria. Each Participant shall itself be a HIPAA "covered entity" and thus subject to both its individual legal duty as a regulated covered entity under HIPAA and its contractually assumed obligations under its Participation Agreement. Each Participant must agree to be a data provider in order to become a data user.

5. User Criteria. Authorized users are individuals who have been granted access authority. Each authorized user derives his or her permission to access and use the System from a Participant. Therefore each authorized user must maintain a current relationship to a Participant in order to use the System. Authorized users must therefore be: (i) Participants (for example, an individual physician) or workforce of a Participant, (ii) an individual BA or workforce of such BA, or (iii) an individual contractor or subcontractor of a BA or workforce of such contractor or subcontractor. Additionally, a Participant that is a covered health plan may also be an authorized user in its role as a third party administrator and BA for self-funded group health plans that are covered entities under HIPAA but are not themselves Participants.

[2] The Participants acknowledge the need to revise Policies and certain other technical and administrative features to conform to HITECH and regulations to be promulgated thereunder. These changes will be made in due course.

6. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

NeHII Privacy
Policy 200: Notice of Privacy Practices

Scope and Applicability: This Policy applies to all Participants.

Policy:

Each Participant shall develop and maintain a notice of privacy practices (the "Notice"). The Notice must describe the uses and disclosures of protected health information contemplated through the Participant's participation in the System.

1. Content. The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule[3] and comply with applicable laws and regulations. Participants shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through the System. NeHII provides the following sample language for Participants who elect to amend their Notice:

"We may make your protected health information available electronically through an electronic health information exchange to other health care providers that request your information for their treatment, payment or health care operations purposes and to participating health plans that request your information for their payment and health care operations. In all cases the requesting provider or health plan must have or have had a relationship with you. Participation in an electronic health information exchange also lets us see their information about you for our treatment, payment and health care operations purposes."

2. Dissemination and Individual Awareness. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgment of receipt by the individual, [4] which policies and procedures shall comply with applicable laws and regulations.

3. Participant Choice. Participants may choose a more proactive Notice distribution or patient awareness process than provided herein and may include more detail in their Notice, so long as any expanded detail does not misstate the safeguards supporting the System.

[3] 45 C.F.R. § 164.520(b).
[4] See 45 C.F.R. § 164.520(c)(2)(ii).

NeHII Privacy
Policy 300: Individual Control of Information Available Through the System

Scope and Applicability: This Policy applies to NeHII and all Participants.

Policy:

1. Choice Whether to Have Information Included in the System. All individuals will have the opportunity to opt out of participating in NeHII. A request to opt out will be treated as a request for restrictions on use and disclosure of protected health information. Participants agree to approve such requests, subject to qualifications and limitations as described in the informational brochure referred to below or in these policies. That is, a request shall not be accepted to the extent it agrees to restrictions that exceed the then current physical, technical and administrative capabilities of the System.

1.1. Individuals shall be afforded the opportunity to exercise this choice at the time of any service at a Participant that is a health care provider or thereafter through a uniform "opt-out" process.

1.2. NeHII will, from time to time, furnish Participants that are health care providers with an informational brochure about the System for distribution to individuals and for use in explaining the meaning and effect of participation or opting out. Participants may customize the informational brochure as they deem appropriate to fit their circumstances. The brochure will also contain a link to the NeHII website where NeHII will provide an explanation of the meaning and effect of participation or opting out and a tool for opting out or revoking a prior opt-out election.

1.3. The brochure shall explain the System-wide scope of an opt-out decision, the risks to the individual's data privacy and security if the individual participates, the effect and benefits of participation, and the effect and disadvantages of opting out. The brochure will explain that a Participant's policies continue to govern access, use and disclosure in all other contexts.

1.4. The brochure shall state that the Participant (and other Participants) will not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her included in the System.

1.5. Participants should furnish the brochure to individuals at the initiation of an episode of care and note for individuals the opportunity to opt-out or ask questions. Each Participant will have one or more persons designated to answer questions about the System or about opting out or revoking a prior opt-out election.

1.6. Participants may also direct individuals to the NeHII website and to a help line at NeHII where the individual can ask additional questions and obtain additional information about participation in NeHII and opt-out. NeHII as a business associate of the Participants is authorized to provide information and answer individual questions about NeHII and the opt-out alternative on behalf of Participants.

1.7. Participants that are health plans provide only limited enrollment and eligibility information through the System and have limited or no face-to-face contact with individuals. Participants that are health plans shall provide a description of the System, an explanation of the right to opt out, a link to the NeHII website and a phone number individuals can use to obtain additional information about the System, insurer access, and the right to opt out in their annual Notice and otherwise as they determine necessary.

1.8. An individual's election to opt out of participation in the System shall be communicated to NeHII in the manner provided by NeHII and be of System-wide effect once so communicated and processed.

2. Change to Prior Election. An individual may opt out or revoke a prior election to opt out at a later date. The brochure and information on the NeHII website should inform the individual that withdrawing a prior opt-out election will result in information that was previously unavailable through the System becoming available to all Participants using the System.

3. Effect of Choice. An individual who opts out of the System opts out as to all of his or her records made available through the System, not just with respect to a particular Participant or episode of care. The effect is System-wide. An individual's election to opt out, whether made at the time of service or subsequently, will have prospective effect only and will not impact access, use and disclosure occurring before the decision is received and communicated through the System.

4. Limited Effect of Opt-Out. A decision to opt out only affects the availability of the individual's protected health information through the System. Each Participant's policies continue to govern access, use and disclosure in all other contexts and via all other media.

5. Documentation. Each Participant shall document and maintain documentation that information about the System and about the ability to opt out of the System has been provided to the Participant.

6. Participant's Choice. Participants shall establish reasonable and appropriate processes to enable the exercise of the individual's choice not to have information about him or her included in the System. The uniform processes described in this Policy are not exclusive, and Participants may adopt additional, not inconsistent, mechanisms.

7. Change in Law. In the event Neb. Rev. Stat. § 71-8403 is amended to remove the twelve month limit on duration of patient authorization to disclose medical record information, Participants may switch to a "consent" or "authorization" mechanism for participation, or NeHII may adopt a uniform policy thereon.

8. Provision of Coverage or Care. A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice to opt out.

9. Reliance. Participants will be entitled to assume that an individual has not opted-out if the individual's protected health information is available through the System.

10. Incompetence or Incapacity. Unless NeHII has been specifically notified of an individual's incompetence or incapacity, NeHII may presume that an individual is competent to exercise his or her rights under this Policy (unless such individual is a minor).

NeHII Privacy
Policy 400: Access to and Use and Disclosure of Information

Scope and Applicability: This Policy applies to NeHII and all Participants.

Policy:

1. Compliance with Law. Participants shall access, use and disclose protected health information through NeHII only in a manner consistent with all applicable federal, state, and local laws and regulations and not for any unlawful or discriminatory purpose.

2. Documentation and Reliance. If applicable law requires that certain documentation exist or that other conditions be met prior to disclosing protected health information for a particular purpose, the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions. Each access and use of protected health information by a Participant is a representation to every other Participant whose protected health information is being accessed and used that all prerequisites under state and federal law for such disclosure by the disclosing Participant have been met.[5]

3. Purposes. A Participant may request and use protected health information from other Participants through the System only: (i) to participate in treatment (in the case of providers), payment or health care operations of the disclosing Participant; (ii) to conduct treatment (in the case of providers), payment and qualifying health care operations purposes of the requesting Participant; or (iii) for those purposes specifically permitted by §164.512(b) of the Privacy Rule and approved by the Privacy and Security Committee, and then only to the extent necessary and permitted by applicable federal, state, and local laws and regulations and these Policies, including any conditions required imposed by the Committee.[6] A Participant may request and use protected health information through the System only if the Participant has or has had or is about to have the requisite relationship to the individual whose protected health information is being accessed and used.

4. Prohibitions. Information may not be requested for fundraising, marketing or purposes related to fundraising or marketing without specific patient authorization. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request or access information through the System.

5. Participant Policies. Participant uses and disclosures of, and requests for, protected health information through the System shall comply with NeHII's policies on Minimum Necessary and Information Subject to Special Protection.[7]

---

[5] See 45 C.F.R. § 164.530(j).
[6] 45 C.F.R. § 164.502(a), (b).
[7] 45 C.F.R. § 164.502(b).

6. Participant Policies. Each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of protected health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.

7. Subsequent Use and Disclosure. A Participant that has accessed information through the System and merged the information into its own record shall treat the merged information as part of its own record and thereafter use and disclose the merged information only in a manner consistent with its own information privacy policies and laws and regulations applicable to its own record. A Participant shall not access protected health information through the System for the purpose of disclosing that information to third parties, other than for the Participant's treatment, payment or qualifying health care operations purposes.

8. Disclosures to Law Enforcement. As permitted by § 164.512(f), if a law enforcement official requests PHI from NeHII via a court order, subpoena, warrant, summons, or other similar document, NeHII may provide the requested PHI as required by and in accordance with city, state, and federal law without first obtaining specific patient authorization:

a. to assist in the identification or location of a suspect, fugitive, material witness, or missing person;

b. regarding a patient who is or is suspected to be a victim of a crime;

c. to alert law enforcement of the death of the individual;

d. if NeHII believes the PHI requested constitutes evidence of criminal conduct that occurred on the premises of NeHII;

e. in emergency situations, to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime;

and, only if:

a. the PHI sought is relevant and material to the law enforcement inquiry;

b. the request is specific and limited in scope to the extent reasonably practicable;

c. de-identified PHI could not be used; and

d. the court order, subpoena, warrant, summons, or other similar document complies with Nebraska law which in some cases requires patient authorization to release.

If a NeHII employee is presented with a court order, subpoena, warrant, summons, or other similar document, the employee should immediately notify the Privacy Officer of the document who will evaluate the document and determine whether and how the disclosure will be made. No PHI should be disclosed in response to a court order, subpoena, warrant, summons, or other similar document prior to discussing the document with the Privacy Officer.

The person providing PHI in response to a court order, subpoena, warrant, summons, or other similar document is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided, the agency name and address (if known), the date the PHI was provided, and a brief summary of the PHI provided for each patient whose PHI is reported or released.

Documentation of releases and disclosures that are made in response to a court order, subpoena, warrant, summons, or other similar document may be maintained by the NeHII Privacy Officer. All documentation relating to requests for a patient's PHI shall be maintained for a minimum of six (6) years.

9. Responding to Inquiries from National Security, Intelligence, and Protective Services Officials.

As permitted by§ 164.512(k), if a federal official requests PHI from NeHII for intelligence, counter-intelligence, and other national security activities, NeHII may provide the requested PHI as required by and in accordance with city, state, and federal law without first obtaining specific patient authorization. The NeHII employee receiving such request should immediately contact the NeHII Privacy Officer.

The person providing PHI to authorized federal officials for national security and intelligence activities and protective services is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided, the agency name and address, the date the PHI was provided, and a brief summary of the PHI provided for each patient whose PHI is reported or released.

Documentation of releases and disclosures that are made to authorized federal officials for national security and intelligence activities and protective services shall be maintained by the Privacy Officer. All documentation relating to requests for a patient's PHI will be maintained for a minimum of six (6) years.

10. Accounting of Disclosures. Each Participant shall be responsible to account only for its own disclosures. NeHII shall provide a means by which each Participant requesting information will indicate the purpose and use for such request so that Participants that disclose information may document the purposes for which they have made disclosures for use in an accounting or as otherwise requested by the

Participant.[8] Unless a Participant requesting information notes otherwise: (i) each request by a Participant that is a provider is deemed to be for such Participant's treatment, payment or qualifying health care operations purposes or to conduct a requested treatment, payment or health care operations function of the disclosing Participant, (ii) each request by a Participant that is a health plan is deemed to be for such Participant's payment or qualifying health care operations purposes or to conduct a requested payment or health care operations function of the disclosing Participant, and (iii) each request by a Participant that is acting as a plan administrator of one or more other health plans covered by HIPAA is deemed to be for the payment or qualifying health care operations purposes of such other health plans. Each Participant requesting information shall provide information required for the disclosing Participant to meet its obligations under the HIPAA Privacy Rule's accounting for disclosures requirement.

11. Audit Logs. Participants and NeHII shall develop an audit log capability to document which Participants posted and accessed the information about an individual through the System and when such information was posted and accessed.[9] Upon request of a Participant, NeHII shall provide such periodic and/or one-time reports as are necessary to determine and/or document user access including what information was accessed by a given user and when such information was accessed.

12. Authentication. NeHII shall follow a uniform authentication requirement for verifying and authenticating the identity and authority of each authorized user and Participant.[10] [11] Participants shall be entitled to rely on NeHII's user access and authorization safeguards and may assume an authorized user making a request for protected health information on behalf of a Participant is authorized to do so. This process is described in greater detail in the NeHII Security Policies.

13. Access. Each Participant should have a formal process through which it permits individuals to view information about them that has been posted by the Participant to the System.[12] Participants and NeHII shall consider and work towards providing patients direct access to the information about them contained in the System.[13] This capability will not be available at the NeHII launch date.

14. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

15. Special Rules for Disclosures for the Health Care Operations of the Recipient

---

[8] 45 C.F.R. § 164.528. For HIPAA Covered Entities, this is currently required by law.

[9] See 45 C.F.R. §§ 164.316, 164.308(a)(1)(i).

[10] See 45 C.F.R. §§ 164.514(h), 164.312(d).

[11] See **Connecting for Health**, "Authentication of System Users."

[12] See 45 C.F.R. § 164.524.

[13] See **Connecting for Health**, "Patients' Access to Their Own Health Information."

The authority for a covered entity to disclose protected health information to another covered entity *for the other covered entity's health care operations* is subject to the following 5 conditions:

a. The recipient must be a covered entity.

b. Only health care operations activities described in subsections (1) and (2) of the regulatory definition of health care operations will support the disclosure by the disclosing Participant or access by the receiving Participant. These activities represent a narrow subset of the full list of health care operations. To draw attention to the limited nature of these health care operations, these Policies refer to them as "qualifying" health care operations. Per the Privacy Rule, they consist only of the following activities:

> *"(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;*
>
> *(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities."*

No other health care operations activities of a requesting Participant will support acess or disclosure. This although a Participant could access or disclose protected health information of its own patients for a much broader array of *its own* health care operations activities, it may only access information from another Participant for "qualifying" health care operations..

c. The recipient must have or have had a relationship with the individual who is the subject of the information being disclosed. For example, if a health plan Participant requests PHI for the Plan's health care operations, access would be limited to individuals who then were or who had been covered enrollees of the health plan.

d. The information accessed or disclosed must pertain to the relationship. For example, if a health plan Participant requests PHI for the plan's health care operations, access would be limited to the period of the individual's enrollment in the health plan's plan.

e. The disclosure, and therefore the access, is subject to the minimum necessary rule.

In addition, a Participant desiring to utilize the protected health information of other Participants for its health care operations must first obtain approval of the Privacy and Security Committee as set forth below:

a. The Participant must first submit a "Use Case" to the Privacy and Security Committee for review, discussion and approval. An approved Use Case will include the conditions and safeguards the Committee determines are necessary and reasonable to permit the proposed acquisition and use for qualifying health care operations. The approval will be by function, not requesting Participant, and other Participants may act on the authority of an approved Use Case.

b. A Participant that does not submit a Use Case for approval, but rather relies on one already approved by the Committee, must notify the Committee of its intent to access protected health information for its own qualifying health care operations and agree to meet the conditions of the approved Use Case. The Committee will provide a form for this purpose.

c. All participants acting in reliance on an approved Use Case must conform to all conditions in the approved Use Case.

NeHII will retain documentation of all Use Cases submitted for approval including any conditions and safeguards the Committee determines are necessary and reasonable to permit the proposed acquisition and use for qualifying health care operations.

NeHII Privacy
Policy 500: Information Subject to Special Protection

Scope and Applicability: This Policy applies to NeHII and all Participants.

Policy:

1. Special Protection. The System and these policies are geared to the HIPAA level of privacy. Some health information may be subject to special protection under federal, state, and/or local laws and regulations. Other health information may be deemed so sensitive that a Participant has made special provision to safeguard the information, even if not legally required to do so. Each Participant shall be responsible to identify what information is legally subject to special protection under applicable law and what information (if any) is subject to special protection under that Participant's policies, prior to disclosing any information through NeHII. Participants should not make protected health information requiring special protection available to the System. Each Participant is responsible for complying with laws and regulations and its own policies in regard to identifying and providing special treatment for information needing special protection.

2. Information Not Furnished. For System data to be useful, the Participant using it must know if it is complete or whether certain information would be withheld due to more stringent state and federal law or Participant policies.

1.1. Accordingly, Participants accessing and using another Participant's information obtained through the System should assume that the information made available would not include any of the following:

(a) Alcohol and substance abuse treatment program records;

(b) Records of emergency protective custody proceedings;

(c) Records of predictive genetic testing performed for genetic counseling purposes;

(d) HIV testing information;

(e) Certain records of minors if under state law only the minor's consent to treatment is needed, the minor has consented to the care, but the minor is not the party electing not to opt out. In Nebraska, this may include the following records:

- Records of STD testing and treatment (including HIV testing);[14]

[14] Neb. Rev. Stat. § 71-504 and 71-531 *et seq.*

- Diagnosis and treatment of suspected abuse by a parent, guardian or personal representative; and

(f) (In Iowa) records of mental health treatment centers.

1.2. This list is suggestive only. Other records may be added to the list. Data recipients are not entitled to rely on records being inclusive of the above listed records.

1.3. Any Participant unable to block such information shall specifically request from NeHII to block the information and shall agree to hold NeHII harmless from any inadvertent disclosure of such information.

3. Application to Business Associates and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

NeHII Privacy
Policy 600: Minimum Necessary

Scope and Applicability: This Policy applies to NeHII, all Participants and their BAs and contractors.

Policy:

1. Requests. When requesting or accessing protected health information of other Participants for payment or qualifying health care operations purposes, each Participant shall request only the minimum amount of health information through the System as is necessary for the intended purpose of the request.

2. Disclosures. A Participant is entitled to rely on the scope of a requesting Participant's request for information as being consistent with the requesting Participant's minimum necessary policy and needs.

3. Workforce, BAs and Contractors. Each Participant shall adopt and apply policies to limit access to the System to members of its workforce who qualify as authorized users and only to the extent needed by such authorized users to perform their job functions or duties for the Participant.

4. Entire Medical Record. A Participant shall not use, disclose, or request an individual's entire medical record unless necessary and justified to accomplish the specific purpose of the use, disclosure, or request.

5. Application to Health Plans. A Participant that is a health plan shall access and use PHI of another Participant only: (i) for "payment" purposes of the health plan or disclosing Participant as described in 42 C.F.R. § 164.501, or (ii) for qualifying "health care operations" purposes as described under Policy 400 - Special Rules for Disclosure for the Health Care operations of the Recipient.

Participants that are health plans shall initiate a search through the System for payment purposes only: (i) to obtain premiums or to determine or fulfill their responsibility for coverage and provision of benefits under the health plan; (ii) to obtain or provide reimbursement for the provision of health care; (iii) to determine eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (iv) to risk adjust amounts due based on enrollee health status and demographic characteristics; (v) for billing, claims management, collection activities, obtaining payment under a contract for reinsurance, including stop-loss insurance and excess of loss insurance, and related health care data processing; (vi) to review health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and (vii) for utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services.

All Participants shall access and use only the minimum information necessary when accessing and using information for payment or qualifying health care operations

purposes. A Participant that is a health plan shall not access protected health information related to a specific encounter and/or treatment of a patient if the patient has paid the health care provider directly out of pocket in full for such encounter and/or treatment.

6. Application to Providers and Treatment Purposes. While this minimum necessary policy is not required by HIPAA for providers accessing, using and disclosing protected health information for treatment purposes, they are encouraged to follow it when consistent with treatment needs.

7. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

NeHII Privacy
Policy 700: Workforce, Agents, and Contractors

Scope and Applicability: This Policy applies to NeHII and all Participants and their BAs and contractors.

Policy:

1. NeHII Responsibility. NeHII is responsible to establish and enforce policies designed to comply with its responsibilities as a Business Associate under HIPAA and to train and supervise its workforce to the extent applicable to their job responsibilities.

2. Participant Responsibility. Each Participant is responsible to establish and enforce policies designed to comply with its responsibilities as a covered entity under HIPAA and a Participant in the System, and to train and supervise its authorized users to the extent applicable to their job responsibilities.

3. Authorized Users. All authorized users, whether members of a Participant's workforce or member of the workforce of a BA or contractor, shall execute an individual user agreement and acknowledge familiarity with and acceptance of the terms and conditions on which their access authority is granted. This shall include familiarity with applicable privacy and security policies of the Participant, BA, or contractor, as applicable. Participants shall determine to what extent members of their workforce or the workforce of BAs and contractor require additional training on account of the Participant's obligations under their participation agreement and these policies, and arrange for and document such training. NeHII shall reserve authority in the Participation Agreement to suspend, limit or revoke access authority for any authorized user or Participant for violation of Participant and/or NeHII privacy and security policies.

4. 3. Access to System. Each Participant shall allow access to the System only by those authorized users who have a legitimate and appropriate need to use the System and/or release or obtain information through the System. No workforce member, agent, or contractor shall have access to the System except as an authorized user on behalf of a Participant and subject to the Participant's privacy and security policies and procedures and the terms of the individual's user agreement.

5. Discipline for Non-Compliance. Each Participant shall implement procedures to discipline and hold authorized users, BAs and contractors accountable for following the Participant's policies and procedures and for ensuring that they do not use, disclose, or request protected health information except as permitted by these Policies.[15] Such discipline measures may include, but not be limited to, verbal and written warnings, demotion, and termination and may provide for retraining where appropriate.

6. 5. Reporting of Non-Compliance. Each Participant shall have a procedure, and shall encourage all workforce members, BAs and contractors to report any non-compliance with the Participant's policies or the policies applicable to authorized

[15] 45 C.R.F. § 164.530(e).

users.[16] Each Participant also shall establish a mechanism for individuals whose health information is included in the System to report any non-compliance with these Policies or concerns about improper disclosures of protected health information.

7. **Enforcing BAAs and Contractor Agreements**. Each Participant shall require in any relationship with a BAs, contractor, or other third party (which may include staff physicians) that will result in such third party becoming an authorized user on behalf of the Participant, or that will result in members of the workforce of such third party becoming an authorized user on behalf of the Participant, that: (i) such third party and any member of its workforce shall be subject to these Policies when accessing, using or disclosing information through the System; (ii) that such third parties and/or authorized users on its workforce may have their access suspended or terminated for violation of these Policies or other terms and conditions of the authorized user agreement; and (iii) that such third party may have its contract with the Participant terminated for violation of these Policies or for failure to enforce these policies among its workforce.

[16] See 45 C.F.R. § 164.530(a), (d).

NeHII Privacy
Policy 800: Amendment Of Data

Scope and Applicability: This Policy applies to NeHII and all Participants.

Policy:

1. Accepting Amendments. Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information.[17] If an individual requests, and the Participant accepts, an amendment to the health information about the individual, the Participant, assisted by NeHII, shall make reasonable efforts to inform other Participants that accessed or received such information through NeHII, within a reasonable time. Only the Participant responsible for the record being amended may accept an amendment. If one Participant believes there is an error in the record of another Participant, it shall contact the responsible Participant.

2. Informing Other Participants. A Participant shall notify NeHII using a method established by NeHII for such purpose when it has amended an individual's protected health information via a mechanism developed by NeHII. NeHII shall cooperate in identifying other Participants who have accessed the information in its pre-amendment form. NeHII shall then be responsible to notify such other Participants of the amendment.

3. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

[17] 45 C.F.R. § 164.526.

NeHII Privacy
Policy 900: Requests For Restrictions

Scope and Applicability: This Policy applies to all Participants.

Policy:

1. Recipient Responsibility. A Participant when accessing data as a data recipient shall not be expected to know of or comply with a restriction on use or disclosure agreed to by a Participant that provides data.

2. Data Provider Responsibility. If a Participant agrees to an individual's request for restrictions,[18] as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions. This shall include not making the individual's information available to the System, including opting the individual out of the System, if required by the restriction. Participants should advise individuals that opting out only affects access, use and disclosure of their protected health information through the System. When evaluating a request for a restriction, the Participant shall consider the implications that agreeing to the restriction would have on the accuracy, integrity and availability of information through the System.

[18] Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 45 C.F.R. § 164.522. For example, an individual could request that information not be used or disclosed for a particular purpose or that certain information not be disclosed to a particular individual. Covered entities are not required to agree to such requests under HIPAA.

NeHII Privacy
Policy 1000: Mitigation

Scope and Applicability: This Policy applies to NeHII, all Participants and their BAs and contractors.

Policy:

1. **Duty to Mitigate**. Each Participant shall implement a process to mitigate, and shall mitigate to the extent practicable, the harmful effects that are known to the Participant of an access, use or disclosure of protected health information through the System that is in violation of applicable laws and/or regulations and/or these Policies and that is caused or contributed to by the Participant or its workforce members, agents, and contractors. Steps to mitigate could include, but are not limited to, Participant notification to the individual or Participant request to the party who improperly received such information to return and/or destroy impermissibly disclosed information.

2. **Duty to Cooperate**. A Participant that has caused or contributed to a privacy breach or that could assist with mitigation of the effects of such breach shall cooperate with NeHII and with another Participant that has the primary obligation to mitigate a breach in order to help mitigate the harmful effects of the breach. This obligation exists whether the Participant is directly responsible or whether the breach was caused or contributed to by members of the Participant's workforce or by its BAs or contractor or their workforce.

3. **Notification to NeHII**. A Participant primarily responsible to mitigate shall notify NeHII of all events requiring mitigation and of all actions taken to mitigate. NeHII may facilitate the mitigation process if asked. NeHII shall attempt to use examples of breaches and mitigation steps for education and for policy and other safeguard development.

4. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

NeHII Privacy
Policy 1100: Investigations; Incident Response System

Scope and Applicability: This Policy applies to NeHII, all Participants and their BAs and contractors.

Policy:

1. **Individual Complaints**. Any individual may submit a complaint about a use or disclosure of PHI by NeHII to either NeHII or to the Secretary of the Department of Health and Human Services (HHS) in Washington, DC. If the individual wants to file a formal complaint with NeHII, he or she should de directed to the NeHII Privacy Officer. If the individual wants to file his/her complaint with the Secretary of HHS, he/she should be directed to the Office for Civil Rights website (www.hhs.gov/ocr/hipaa). The NeHII Privacy Officer will document each privacy complaint received including in the documentation a brief description of and/or the basis for the complaint.

The Privacy Officer will supplement the initial documentation to include documentation of the investigation and any actions taken in response to the complaint. All documentation relating to the individual's complaint will be maintained for a minimum of six (6) years.

2. **Duty to Investigate**. Each Participant shall promptly investigate reported or suspected privacy breaches implicating privacy or security safeguards deployed by NeHII (or its contractors) according to its own policies. Upon learning of a reported or suspected breach, the Participant shall notify NeHII and any other Participant whom the notifying Participant has reason to believe is affected or may have been the subject of unauthorized access, use or disclosure. NeHII shall have the right to participate in the investigation and to know the results and remedial action, if any, taken, except that NeHII need not be notified of specific workforce disciplinary actions. Each investigation shall be documented. At the conclusion of an investigation, a Participant shall document its findings and any action taken in response to an investigation. A summary of the findings shall be sent to NeHII. NeHII shall attempt to use examples of breaches for education and for policy and other safeguard development.

3. **Incident Response.** NeHII shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by Participants or discovered by NeHII. The

incident response system shall include the following features, each applicable as determined by the circumstances:

3.1 Cooperation in any investigation conducted by the Participant or direct investigation by NeHII;

3.2 Notification of other Participants or authorized users as needed to prevent further harm or to enlist cooperation in the investigation and/or mitigation of the breach;

3.3 Cooperation in any mitigation steps initiated by the Participant;

3.4 Furnishing audit logs and other information helpful in the investigation;

3.5 Developing and disseminating remediation plans to strengthen safeguards or hold Participants or authorized users accountable;

3.6 Any other steps mutually agreed to as appropriate under the circumstances; and

3.7 Any other step required under the incident reporting and investigation system contained in the NeHII Security Policies.

4. **NeHII Cooperation**. NeHII shall cooperate with a Participant in any investigation of the Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by the Participant, when the investigation implicates NeHII conduct, or the conduct of another Participant or authorized user, or the adequacy or integrity of System safeguards.

5. **Participant Cooperation**. Each Participant shall cooperate with NeHII in any investigation of NeHII or of another Participant into NeHII's or such other Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by NeHII or the other Participant, when the investigation implicates such Participant's compliance with NeHII policies or the adequacy or integrity of System safeguards.

6. **Application to BAs and Contractors.** Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

If the NeHII privacy Officer determines that PHI that was wrongfully used or disclosed is created or maintained by a business associate of NeHII, the HIPAA Privacy Officer will notify the business associate of the results of the investigation and any required action on the part of the business associate. If the results of the investigation are that the NeHII business associate misused or improperly disclosed an individual's PHI, the NeHII Privacy Officer will prepare a recommendation for the NeHII Board as to whether the business associate relationship between the business associate and NeHII should continue.

7. **Mitigation by NeHII.** If an investigation of a privacy breach indicates that PHI was misused or improperly disclosed , the NeHII Privacy Officer shall determine:

i. What, if any, privacy practices at NeHII require modification;

i. Whether a new policy, procedure, or form should be developed or whether an existing policy, procedure, or form should be revised;

ii. Whether additional training is required to avoid a repeat violation;

iii. Whether additional training is required to avoid a repeat violation; and

iv. What sanctions, if any, will be imposed against the individual who committed the violation.

8. **Non-retaliation for filing a complaint.** NeHII will not intimidate, threaten, coerce, discriminate, penalize, or take other retaliatory action against an individual who exercises his/her rights under HIPAA or against any individual who participates in a process governed by the Privacy Regulations. This prohibition also applies to:

a. Individual and/or individual complaints filed with the Secretary of HHS;

b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing arising under the HIPAA Privacy Regulations; or

c. Opposing any act or practice of NeHII, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not disclose PHI in violation of the HIPAA Privacy Regulations.

9. **No waiver.** No individual will be asked to waive his/her HIPAA rights, including the right to file a complaint about the use or disclosure of his/her PHI.

NeHII Privacy
Policy 1200: Authorized User Controls

Scope and Applicability: This Policy applies to NeHII, all Participants and their BAs and contractors. This Policy is to be read and applied in conjunction with the NeHII Security Policy.

Policy:

1. **Participant Responsibilities.** Each Participant is responsible to:

3.1. Designate its responsible contact person who shall be initially responsible on behalf of the Participant for compliance with these policies and to receive notice on behalf of the Participant. For Participants that have their own system administrator, this shall ordinarily be the system administrator.

3.2. Designate its own authorized users from among its workforce, and designate BAs and contractors authorized to act as (or designate from among their workforce) authorized users on its behalf.

3.3. Train and supervise its authorized users and require any BA or contractor to train and supervise its authorized users consistent with the Participant's and NeHII's privacy policies and with the terms of the Participant's privacy policies and the BA Agreement as applicable.

3.4. In the case of Participants with a System Administrator, immediately suspend, limit or revoke access authority upon a change in job responsibilities or employment status of an authorized user. Revocation shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant.

3.5. For Participants without their own System Administrator, immediately notify NeHII of the change so that NeHII may revoke access authority. Notification shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant.

3.6. Hold their authorized users accountable for compliance with NeHII and the Participant's policies and, as applicable, the terms of any BA Agreement.

4. NeHII Responsibilities. NeHII is responsible to:

4.1. Grant access authority to individuals designated by a Participant, subject to reserved authority to suspend, limit, or revoke such access authority as described later.

4.2. Train and supervise its own authorized users on these policies and the standard terms required by its BA Agreement with Participants.

4.3. Suspend, limit or revoke access authority for its own authorized users or any authorized user who is a member of the workforce of any subcontractor of NeHII as required by these policies or the terms of its BA Agreement in the event of breach or non-compliance.

4.4. Immediately revoke access authority upon a change in job responsibilities or employment status of its own authorized users or the authorized user of its contractor.

4.5. Suspend, limit, or revoke the access authority of an authorized user on its own initiative upon a determination that the authorized user has not complied with the Participant's privacy policies, NeHII policies or the terms of the user agreement, if NeHII determines that doing so is necessary for the privacy of individuals or the security of the System.

5. User Audits

- Approximately January 1 of each year, NeHII will run a report of all Users by Participant. The report will be sent out to each Participant.
- Within thirty (30) days, Participant will review and determine which Users are no longer actively employed or should have had their access terminated for another reason and return such results to NeHII.
- If results are not returned, NeHII will terminate any User who has not accessed the system for 2 months and follow-up with Participant.
- After 90 days, Privacy Officer will report to Board which Participant's have not responded.
- If error rate is greater than 10% in physician practice or 5% in provider/payor, the Participant must provide an action plan within 30 days re how they will notify NeHII of User terminations in future.
- Appropriate follow-up audits will be performed within 90-120 days to ensure action plan is implemented and effective.

6. Access Audits

- Approximately July 1 of each year, NeHII will run an access report for the prior month for each Participant.
  The report will be by facility and include: User name – Patient Name accessed – Patient DOB – Date of access
- Report will be distributed to each Participant with a request to review/audit access of use and return summary report within 60 days.
- Each Participant will be responsible to review the report to determine any inappropriate access of patient information by that Participant's Users.
- If issues found, the Participant must provide NeHII with an summary report within thirty (30) days re how issues will/were addressed.
- Appropriate follow-up audits will be performed within 90-120 days to ensure action plan is implemented and effective.

5. NeHII Security Policy. The details of how to grant and revoke access authority are contained in the NeHII Security policy.

6. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

NeHII Privacy
Policy 1300: COMPLAINTS ABOUT USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Scope and Applicability: This Policy applies to NeHII and all Participants.

Policy:

In accordance with HIPAA, individuals may complain about how NeHII uses and disclose their Protected Health Information (PHI). All complaints regarding NeHII's conduct will be submitted to the NeHII Privacy Officer for investigation and resolution.

PROCEDURES:

1. **Submission of complaints**. An individual may submit a complaint about a use or disclosure of PHI by NeHII to either NeHII or to the Secretary of the Department of Health and Human Services (HHS) in Washington, DC.

    a. If the individual wants to file a formal complaint with NeHII, he/she should contact the NeHII Privacy Officer.

    b. If the individual wants to file his/her complaint with the Secretary of HHS, he/she should be directed to and follow the steps provided on the Office for Civil Rights website (www.hhs.gov/ocr/hipaa).

    c. Complaints regarding the use or disclosure of an individual's PHI by a NEHII Participant will be referred to the Participant for investigation and resolution.

2. **Responsibilities of the HIPAA Privacy Officer upon receipt of an individual complaint.**

    4. Documentation. The Privacy Officer will document each privacy complaint received including in the documentation a brief description of and/or the basis for the complaint.

    5. Investigation. With the assistance of NeHII support staff, The Privacy Officer will conduct an investigation to determine:

        1. What, if any PHI was misused or improperly disclosed;

        ii. If PHI was misused or improperly disclosed, whether such misuse or improper disclosure violates NeHII 's policies and procedures;

        iii. What, if any, privacy practices at NeHII require modification;

iv. Whether a new policy, procedure, or form should be developed or whether an existing policy, procedure, or form should be revised; and

v. Whether additional training is required to avoid a repeat violation.

f. Resolution.

i. If the Privacy Officer determines a violation has occurred, he/she will consult with NeHII staff and/or the Privacy Officer of the Participant whose staff inappropriately used or accessed PHI to determine what sanctions, if any, will be imposed against the individual who committed the violation.

ii. The Privacy Officer will supplement the initial documentation to include documentation of the investigation and any actions taken in response to the complaint.

iii. All documentation relating to the individual's complaint will be maintained for a minimum of six (6) years.

iv. If the PHI that was wrongfully used or disclosed is created or maintained by a business associate of NeHII, the HIPAA Privacy Officer will:

1. Notify the business associate of the results of the investigation and any required action on the part of the business associate.

2. If the results of the investigation are that the business associate misused or improperly disclosed an individual's PHI, prepare a recommendation for the NeHII Board as to whether the business associate relationship between the business associate and NeHII should continue.

2. **Non-retaliation for filing a complaint.** NeHII will not intimidate, threaten, coerce, discriminate, penalize, or take other retaliatory action against an individual who exercises his/her rights under HIPAA or against any individual who participates in a process governed by the Privacy Regulations. This prohibition also applies to:

d. Individual and/or individual complaints filed with the Secretary of HHS;

e. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing arising under the HIPAA Privacy Regulations; or

f. Opposing any act or practice of NeHII, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not disclose PHI in violation of the HIPAA Privacy Regulations.

b. **No waiver.** No individual will be asked to waive his/her HIPAA rights, including the right to file a complaint about the use or disclosure of his/her PHI.

c. **Questions.** Questions about filing a complaint with NeHII or the Secretary of HHA should be directed to the Privacy Officer.

NeHII Privacy
Policy 1400: BREACH NOTIFICATION

Scope and Applicability: This Policy applies to NeHII and all Participants.

Policy:

In the event of a breach of unsecured protected health information through the NeHII system, NeHII will fully cooperate with the Participant(s) who is the owner/creator of the disclosed information and any Participant(s) who may be involved in the incident to provide proper breach notification in compliance with the Breach Notification Requirements of §13402 of Title XIII of the ARRA of 2009 (HITECH) and any other applicable federal or state notification law.

Definitions:

Under HITECH and the HHS Rule, notice to an individual of a "breach" is required if the PHI is "unsecured".

For purposes of this policy, a "breach" occurs when there is an impermissible use or disclosure of unsecured PHI that violates the HIPAA Privacy or Security Rules and that creates a significant risk of financial, reputational, or other harm to the individual.

A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to NeHII, or, by exercising reasonable diligence would have been known to NeHII or one of its Business Associates.

PHI in any form is ''unsecured" if it is not secured through the use of a technology or methodology specified in HHS guidance.

Procedure:

Any NeHII Participant, employee, contractor or agent who discovers or suspects that a breach of patient information has occurred through the NeHII system will immediately notify the NeHII Privacy Officer. Notification may be made by e-mail, telephone, or by entry into the NeHII tracking system.

The NeHII Privacy Officer will log the breach and, in conjunction with the NeHII Security Officer, take any necessary action to promptly mitigate the situation and/or reduce the likelihood of any further breach.

In addition, the NeHII Privacy Officer will:

- promptly notify the Participant who is the owner/creator of the disclosed information and any Participant(s) who may be involved in the incident;

- identify the individuals whose unsecured PHI has been, or is reasonably believed to have been breached;

- in cooperation with the Participant(s), promptly investigate the circumstances and nature of the breach;

- in cooperation with the Participant(s), conduct a risk assessment to determine whether the disclosure poses a significant risk of financial, reputational or other harm to the individual and whether any exception to the breach rules apply; and

- based on the results of the risk assessment, fully cooperate with Participants in providing any notice required under HITECH and the HHS rule.

Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is otherwise permissible and occurs despite reasonable safeguards and proper minimum necessary procedures would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification, a risk assessment must be performed to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. This risk assessment shall be documented as part of the overall investigation. The attached Risk Assessment Analysis tool or the Participant's tool may be used to complete and document the analysis.

The risk assessment and the supporting documentation shall be fact specific and consider to whom the information was impermissibly disclosed, the type and amount of PHI involved, and the potential for significant risk of financial, reputational, or other harm. In completing the risk assessment, NeHII shall cooperate with any Participant whose patient and/or information is affected.

Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by NeHII or the business associate involved. Any required notification will be made jointly by NeHII and the Participant(s) whose patient and/or information is affected

Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states that a notification would impede a criminal investigation or cause damage to national security, notifications shall be delayed upon receipt of a written statement specifying the time for which a delay us required. If the statement is made orally, document the statement, and delay the notification no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

Content of the Notice: The notice shall be written in plain language and must contain the following information:

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

date of the discovery of the breach, if known.

2. A description of the types of unsecured protected health information that were involved in the breach.

3. Any steps the individual should take to protect themselves from potential harm resulting from the breach.

4. A brief description of what NeHII is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, web site, or postal address.

Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:

1. Notice to Individual(s): Notice shall be provided promptly and in the following form:

   a. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. If the individual is deceased, notice shall be made to the personal representative of the patient.

   b. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided.

      i. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

      ii. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of NeHII's website, or a conspicuous notice in a major print or broadcast media in NeHII's geographic areas where the individuals affected by the breach likely reside.

   c. If NeHII determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by

telephone or other means, as appropriate in addition to the methods noted above.

2. Notice to Media: Notice in the form of a press release shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients.

3. Notice to Secretary of HHS:

   a. NeHII shall provide Notice to the Secretary of HHS when the breach of **unsecured** PHI of more than 500 patients from a single state is accessed, acquired, used, or disclosed.

   b. For breaches involving less than 500 individuals from a single state, a log of the breaches shall be maintained and annually submitted to the Secretary off HHS.

Retention of Records: NeHII shall retain all documentation related to the breach investigation, including the risk assessment, for a minimum of six years.

APPENDIX A – COMPLAINT FORM

You have the right to make a written complaint concerning the Nebraska Health Information Exchange's (NeHII) compliance with its privacy policies and procedures or the requirements regarding medical information. If you wish to make a complaint, please complete this form and send it to the above address.

Person Making Complaint: _____

Relationship to Patient: _____

Address: _____

_____

_____

Telephone: _____

Patient Date of Birth: _____

Describe briefly what happened. How and why do you believe your (or someone else's) health information privacy rights were violated, or the HIPAA Privacy rule otherwise was violated? Please be as specific as possible:

_____

_____

_____

_____

_____

_____

Who (or what provider or health plan) do you believe violated your (or someone else's) health information privacy rights or committed another violation of the HIPPA Privacy Rule?

_____

_____

When do you believe that the violation of health information privacy rights occurred?

_____

Signature of Person Making Complaint: _____

Date: _____

Received by (Signature): _____ Date: _____

Title: _____

APPENDIX B – BREACH NOTIFICATION RISK ASSESSMENT

Risk Assessment Analysis – Name / Date

Q #	Question	Yes - Next Steps	No – Next Steps
	Unsecured PHI		
1.	Was the impressible use/disclosure unsecured PHI[4] (e.g., not rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary)?	Continue to next question.	Notification not required. Document decision.
Answer	→		
	Minimum Necessary		
2.	Was more than the minimum necessary for the purpose accessed, used or disclosed?	Continue to next question.	May determine low risk and not provide notifications. Document decision.
Answer	→		

[4] **Unsecured Protected Health Information**: Protected health information (PHI) that **is not rendered** unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology.

	Was there a significant risk of harm to the individual as a result of the impermissible use or disclosure?		
3.	Was it received and/or used by another entity governed by HIPAA Privacy & Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 & FISA of 2002?	May determine low risk and not provide notifications. Document decision.	Continue to next question
Answer	→	→	
4.	Were immediate steps taken to mitigate an impermissible use/disclosure (ex. Obtain the recipient' assurance the information will not be further used/disclosed or will be destroyed)?	May determine low risk and not provide notifications. Document decision .	Continue to the next question.
Answer	→		
5.	Was the PHI returned prior to being accessed for an improper purpose (e.g., A laptap is lost/stolen, then recovered & forensic analysis shows the PHI was not accessed, altered, transferred, or otherwise compromised)?	May determine low risk and not provide notifications. Document decision. Note: Don't delay notification based on a hope it will be recovered.	Continue to the next question.

Answer	→		
	What type and amount of PHI was involved in the impermissible use or disclosure?		
6.	Does it pose a significant risk of financial, reputational, or other harm?	Higher risk – should report.	May determine low risk and not provide notifications. Document decision.
Answer	→		
7.	Did the improper use/disclosure only include the name and the fact that services were received?	May determine low risk and not provide notifications. Document decision.	Continue to the next question.
Answer	→	→	
8.	Did the improper use/disclosure include the name and type of services received, services were from a specialized facility (such as a substance abuse facility), ***or*** the information increase the risk of ID Theft (such as SS#, account#, mother's maiden name).	High risk- should provide notifications.	Continue to the next question.

Answer	→		
9.	Did the improper use/disclosure ***not*** include the 16 limited data set identifiers in 164.514(e)(2) ***nor*** the zip codes or dates of birth? Note: Take into consideration the risk of re-identification (the higher the risk, the more likely notifications should be made).	High risk- should provide notifications.	May determine low risk and not provide notification. Document decision.
Answer	→		
10.	Is the risk of re-identification so small that the improper use/disclosure poses no significant harm to any individuals (ex. Limited data set included zip codes that based on population features doesn't create a significant risk an individual can be identified.	May determine low risk and not provide notification. Document decision.	Continue to the next question.
Answer	→		
	Specific Breach Definition Exclusion		

11.	Was it an unintentional access/use/disclosure by a workforce member acting under the organization's authority, made in good faith, with his/her scope of authority (workforce member was acting on the organization behalf at the time), and didn't result in further use/disclosure (ex. Billing employee receives an email containing PHI about a patient mistakenly sent by a nurse (co-worker). The billing employee alerts the nurse of the misdirected email & deletes it)?	May determine low risk and not provide notification. Document decision.	Continue to the next question.
Answer	→	→	
12.	Was access unrelated to the workforce member's duties (ex. Did a receptionist look through a patient's records to learn of their treatment)?	High risk- should provide notifications.	Continue to the next question.
Answer	→		

13.	Was it an inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same organization, or its OHCA, ***and*** the authority to use/disclose PHI in that organization/OHCA and the PHI is not further used/disclosed?	May determine low risk and not provide notification. Document decision	Continue to the next question.
Answer	→		
14.	Was a disclosure of PHI made, but there is a good faith belief that the unauthorized recipient would not have reasonably been able to retain it. (Ex. EOBs were mistakenly sent to wrong individuals and were returned by the post office, unopened, as undeliverable)?	May determine low risk and not provide notification. Document decision.	Document findings.
Answer	→		

Conclusion: