



# Eastern Massachusetts Healthcare Initiative

## Clinical Data Exchange Policy Framework DRAFT

*June 10, 2009*

CSC Health Services Sector  
266 SECOND AVENUE  
WALTHAM, MA 02451

PHONE: 781.890.7446



<b>1.0 Overview</b>	<b>1</b>
1.1 Background	1
1.2 Purpose of the Framework	1
1.3 Guiding Principles	1
1.4 Applicability and Scope	2
1.4.1 Organizations and Locations	2
1.4.2 Data	3
1.4.3 Business Processes	3
1.4.4 Applications and Technologies	3
1.5 Effective Date	3
1.6 Responsibilities	3
1.6.1 NEHEN	3
1.6.2 Participants	4
1.6.3 External Trading Partners	4
<b>2.0 Clinical Data Exchange Policies</b>	<b>5</b>
2.1 Federal, State, and Local Laws	5
2.2 Data Sharing Agreements	6
2.3 Suspension and Termination of Participation	7
2.4 Release/Disclosure of Patient Information	8
2.4.1 Disclosure of Patient Information Not Requiring Written Authorization	8
2.4.2 Disclosure of Patient Information for Secondary Use	9
2.4.3 Disclosure of Sensitive Health Information	10
2.5 Auditing Access to Patient Information	12
2.6 Reporting Disclosures	14
2.7 Breach of Disclosure Policy	15
2.8 Access to Data Exchange Policies	16
2.9 Authentication and Authorization of System Users	17
2.10 Use of Data Exchange Standards	19
2.11 Security	21
2.12 Service Levels	22
<b>3.0 Clinical Data Exchange Requirements and Best Practices</b>	<b>23</b>
3.1 Registering Participants and Users	23
3.2 Sending Clinical Data	24
3.3 Receiving Clinical Data	25



## TABLE OF CONTENTS continued

<b>4.0 Definitions</b>	<b>26</b>
<b>Appendix A: EMHI Participants in 2009</b>	<b>29</b>

## 1.0 Overview

### 1.1 Background

The Eastern Massachusetts Healthcare Initiative (EMHI) is a collaborative formed in 2006 to improve the performance of the region's health care system. In 2009, EMHI participants included three universities, four commercial health plan insurers, and nine healthcare provider organizations (including an alliance of multi-specialty group physician group practices, a community hospital, specialty hospitals, academic medical centers and an integrated delivery network). See Appendix A for a list of EMHI participants in 2009.

In 2009, the New England Healthcare Exchange Network, Inc. (NEHEN) was formed by the merger of two existing healthcare exchanges: (1) the New England Healthcare EDI Network (NEHEN, LLC), which operated a broad-based exchange of administrative and financial healthcare data among payer organizations, provider organizations, and vendor organizations operating in Massachusetts and Rhode Island, and (2) Massachusetts Simplifying Healthcare Among Regional Entities (MA-SHARE, LLC), which operated a more limited exchange of clinical healthcare data among payer organizations, provider organizations, and vendor organizations operating in Massachusetts.

One of EMHI's healthcare improvement objectives was to improve healthcare IT interoperability, and to that end, EMHI funded initial development of this policy framework for community clinical data exchange. EMHI's intent was that NEHEN would adopt the framework, and as such, the framework would provide the policy foundation for data sharing among organizations participating in clinical data exchange via NEHEN, including both EMHI organizations and other NEHEN member organizations.

Except as otherwise stated, references to "NEHEN" in this document refer to NEHEN in its role as operator and facilitator of clinical data exchange for the region.

### 1.2 Purpose of the Framework

This framework defines the policies for clinical data exchange via NEHEN. The policies establish operating rules for NEHEN, as the provider of health information exchange (HIE) services, and for NEHEN Participants, as users of the HIE. The policies also provide the foundation for development of Implementation Guides which will define the specific requirements for exchanging clinical data via NEHEN.

### 1.3 Guiding Principles

The following principles guide the development of all policies for community clinical data exchange.

- *Decisions Based on Guiding Principles.* Decisions are arrived at collaboratively based on adherence to underlying principles.
- *Openness and Transparency.* Policies are available for review by all stakeholders—payers, providers, Patients, employers, and vendors. Decisions and activities are communicated openly in public and electronic forums. All stakeholders are welcome to comment on and propose changes to policies, procedures, and technologies.
- *Patients' Rights.* Patients are provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their health information. Patients have a simple and timely means to view who has access to their health data and what data is accessed.
- *Patient Access and Participation.* Patients may request and receive information about access to their own data, to the extent possible with available technologies. Patients may dispute the accuracy or integrity of their health information, have erroneous information corrected, or have a note made of the disputed data, if correction is not feasible.

- *Data Collection and Use Limitation.* Health data are collected, exchanged, and used only for the agreed upon and stated purpose. The purpose itself is narrowly suited to the need.
- *Privacy and Security Policy Compliance.* Policies comply with Federal laws and regulations, including HIPAA, and with other applicable laws governing electronic healthcare data exchange.
- *Coordinated Decentralization.* Policies are designed to allow local control and management by Participants to the extent practical, in order to allow flexibility and minimize centralized resources and costs.
- *Broad Adoptability.* Policies are designed for ease of use by Participants and for cost effectiveness, in order to facilitate broad adoption and to facilitate participation by organizations with varying access to resources. To the extent practical, policies are designed to permit reasonable adoption time frames by Participants.
- *Anticipation of Change.* To the extent practical, policies are designed to anticipate and prepare for potential changes in federal and state requirements and standards.

The following principles guide the adoption and use of technology policies.

- *Open Standards.* All policies adhere to accepted national and industry standards where available, are based on open standards, are not dependent on proprietary technologies, and are vendor-neutral to facilitate widespread adoption. Connectivity among Participants' systems is based on the public Internet.
- *Federated Data Architecture.* Policies are designed to promote "informational sovereignty" and are biased toward local control of data and local accessibility.
- *Flexibility and Agility.* Following architectural best practices, policies for application software design are biased toward loosely coupled and coarse grained services and reusability without compromising performance.
- *No Rip and Replace.* Policies are designed to protect current technology investments of Participants to the extent possible through adoption of open standards.
- *Multiple Implementation Models.* Policies are designed to support multiple network architectures, varying from Participant and vendor-hosted connectivity, to centrally hosted services.

## **1.4 Applicability and Scope**

The policies in this document apply to the exchange of clinical data and the organizations, business processes, computer applications, and technology involved in the exchange of clinical data via NEHEN. Clinical data is understood to include data directly related to care provided to individuals and data used to manage the exchange of this data.

The policies in this document apply to the internal business processes, computer applications, or technology solutions of the Participants only as they are directly used in the electronic exchange of clinical data via NEHEN.

The policies in this document do not apply to the exchange of financial and administrative data between Participants or to NEHEN in its role as operator and facilitator of administrative and financial healthcare data exchange.

The following are more specific definitions of scope and applicability.

### **1.4.1 Organizations and Locations**

The organizations to which the policies apply are:

- NEHEN. NEHEN is located in Massachusetts. Compliance by employees, agents, contractors, and other persons affiliated with NEHEN is the responsibility of NEHEN.
- NEHEN Participants. Participants include all organizations actively exchanging clinical data via NEHEN. These organizations may include payer, provider, quality, government, and other organizations. Participants are located mainly in New England. Participants may be located outside of New England with approval of the NEHEN Board of Directors. Compliance by employees, agents, contractors, and other persons affiliated with a Participant is the responsibility of the Participant.

#### **1.4.2 Data**

Data to which the policies apply are:

- All clinical data transmitted in electronic form from one Participant to another using NEHEN services.
- All clinical data stored by NEHEN in support of the transmission of data from one Participant to another.

#### **1.4.3 Business Processes**

Business processes to which the policies apply are:

- All business processes used by a Participant to send or receive data via NEHEN.
- All business processes used by NEHEN to provide clinical data exchange services and infrastructure.

#### **1.4.4 Applications and Technologies**

The computer applications and technology solutions to which the policies apply are:

- All applications and technology solutions owned or operated by a Participant or on behalf of a Participant which are used to send or receive data via NEHEN.
- All applications and technology solutions owned or operated by NEHEN or on behalf of NEHEN which are used to provide clinical data exchange services.

### **1.5 Effective Date**

The policies outlined in this document are effective upon approval by EMHI and upon acceptance by NEHEN.

### **1.6 Responsibilities**

The following are the policy-related responsibilities of Participants in the community clinical data exchange.

#### **1.6.1 NEHEN**

The NEHEN Board of Directors is accountable for the execution of NEHEN's responsibilities, which may be carried out by the Board itself and by NEHEN's employees, agents, vendors, and subcontractors.

NEHEN's responsibilities are to:

- Work with the Participants to develop and gain consensus on policies, service levels, requirements, and best practices required to operate the exchange.
- Maintain this policy framework.
- Make this policy framework available to requestors upon request.
- Manage development of Data Sharing Agreements and related changes with Participants and other trading partners as needed to align the agreements with current policies.

- Manage development of Data Sharing Agreements with other trading partners and related changes as needed to align them with current policies.
- Provide consultative assistance to Participants in interpreting and implementing policies.
- Participate in an annual review with each Participant of policies, service levels, requirements, and best practices.
- Adjudicate issues affecting a Participant’s “good standing” with NEHEN. This adjudication is the responsibility of the NEHEN Board of Directors.
- Inform Participants of non-compliance, and administer agreed-upon disciplines, up to and including termination or suspension of participation.

### **1.6.2 Participants**

Each Participant is accountable for the execution of its responsibilities, which may be carried out by the Participant organization itself and by its employees, agents, vendors, subcontractors, and affiliates.

Participant responsibilities are to:

- Work with NEHEN to develop and gain consensus on policies, requirements, and best practices required to operate the exchange.
- Participate in an annual review with NEHEN of policies, service levels, requirements, and best practices.
- Comply with Data Sharing Agreements, policies, and service levels.
- Make best efforts to comply with best practices.
- Annually execute a “statement of compliance” with agreements, policies, service levels, requirements, and best practices.
- Remedy situations of non-compliance.

### **1.6.3 External Trading Partners**

Each external trading partner is accountable for the execution of its responsibilities, which may be carried out by the partner organization itself and by its employees, agents, vendors, subcontractor, and affiliates. External trading partner responsibilities are to comply with the provisions of Data Sharing Agreements executed with NEHEN.

## 2.0 Clinical Data Exchange Policies

### 2.1 Federal, State, and Local Laws

NEHEN clinical Data Sharing Agreements are structured to comply with federal laws and with the laws of the Commonwealth of Massachusetts. Participants subject to the laws of other states are responsible for compliance with the laws of those states.

NEHEN	Participant
<ul style="list-style-type: none"><li>• NEHEN shall comply with all federal, state, and local laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as they pertain to healthcare data exchanged via NEHEN.</li><li>• NEHEN shall maintain internal policies and procedures for compliance with legal requirements.</li></ul>	<ul style="list-style-type: none"><li>• Participant shall comply with all federal, state, and local laws, including HIPAA, as they pertain to healthcare data exchanged via NEHEN.</li><li>• Participant shall maintain internal policies and procedures for compliance with legal requirements.</li></ul>

## 2.2 Data Sharing Agreements

NEHEN	Participant
<ul style="list-style-type: none"> <li>• NEHEN shall execute a Data Sharing Agreement with each Participant and External Trading Partner prior to beginning live exchange of data. Such a Data Sharing Agreement shall establish the mutual responsibilities of NEHEN and the Participant or External Trading Partner for compliance with the policies in this document and shall be amended as needed.</li> <li>• NEHEN shall comply with all provisions of the Data Sharing Agreement.</li> <li>• Any Data Sharing Agreement that contains provisions that are not consistent with the policies in this document shall require approval by the NEHEN Board of Directors.</li> <li>• NEHEN shall participate annually in a review with each Participant of the Data Sharing Agreement and related policies, service levels, requirements, and best practices.</li> <li>• NEHEN shall administer disciplines for non-compliance with Data Sharing Agreements up to and including termination or suspension of a Participant’s participation in NEHEN.</li> </ul>	<ul style="list-style-type: none"> <li>• Participant shall execute a Data Sharing Agreement with NEHEN prior to beginning live exchange of data. Such a Data Sharing Agreement shall establish the mutual responsibilities of NEHEN and the Participant for compliance with the policies in this document and shall be amended as needed.</li> <li>• Participant shall comply with all provisions of the Data Sharing Agreement.</li> <li>• Participant shall participate annually in a review with NEHEN of the Data Sharing Agreement and related policies, service levels, requirements, and best practices.</li> <li>• Participant shall make best efforts to comply with best practices agreed upon by NEHEN and Participants.</li> <li>• Participant shall execute annually a “Statement of Compliance” with the Data Sharing Agreement, policies, service levels, requirements, and best practices.</li> </ul>

## 2.3 Suspension and Termination of Participation

NEHEN	Participant
<ul style="list-style-type: none"> <li>• NEHEN shall terminate or suspend a Participant’s participation in NEHEN only as directed by the Participant or for cause.</li> <li>• NEHEN shall promptly inform Participant of any incident or report of non-compliance with a Data Sharing Agreement by a Participant and shall promptly conduct a preliminary investigation. If NEHEN determines that there is a reasonable likelihood that a Participant’s acts or omissions would cause harm to another Participant, or to a Patient whose data is exchanged through the network, NEHEN shall suspend the Participant’s participation in NEHEN and shall provide to the Participant a written summary of the reasons for the suspension.</li> <li>• NEHEN shall provide prompt notice of a Participant’s suspension to all other Participants.</li> <li>• If desired by the Participant and if approved by the NEHEN Board of Directors, NEHEN shall work with the Participant to correct the situation that caused the suspension. Upon resolution of the situation, NEHEN shall reinstate participation and shall notify other Participants of the reinstatement. If the situation is not corrected to the satisfaction of the NEHEN Board of Directors, NEHEN shall terminate the Participant’s participation in NEHEN.</li> </ul>	<ul style="list-style-type: none"> <li>• A Participant may terminate participation in NEHEN, with or without cause, by giving NEHEN written notice. NEHEN shall execute such instructions by terminating the Participant’s ability to access NEHEN services without any further action by the Participant, and NEHEN shall provide notice of such termination to the remaining Participants.</li> </ul>

## 2.4 Release/Disclosure of Patient Information

Release and disclosure of Patient Information, also referred to as Protected Health Information (PHI), are governed by federal and state laws as well as by internal policies and practices of NEHEN Participants. Factors affecting release and disclosure of information include but are not limited to:

- HIPAA, which provides for use and disclosure of PHI for treatment, payment, operations, and certain secondary uses, without written authorization by the Patient.
- State laws, such as the Massachusetts laws restricting transmission and use of certain types of Sensitive Health Information and requiring certain types of Patient authorization for transmission and use.
- Internal Participant policies that require redaction of certain types of Sensitive Health Information in outgoing electronic and/or paper-based transmissions.

NEHEN’s role is only to serve as intermediary among NEHEN Participants for exchange of clinical data, and as such, NEHEN is not authorized to release PHI for any reason unless authorized to do so by written agreement with a Participant.

### 2.4.1 Disclosure of Patient Information Not Requiring Written Authorization

NEHEN	Participant
<ul style="list-style-type: none"> <li>• NEHEN shall not release or disclose any PHI except as required by law or as defined in a Data Sharing Agreement or in a separate agreement between NEHEN and a Participant or between NEHEN and an External Trading Partner.</li> </ul>	<ul style="list-style-type: none"> <li>• Participant shall maintain and follow internal policies which shall govern release and disclosure of PHI.</li> <li>• Participant may delegate responsibility for release or disclosure of PHI to NEHEN, in which case mutual responsibilities of NEHEN and Participant shall be defined in a written agreement.</li> </ul>

### 2.4.2 Disclosure of Patient Information for Secondary Use

NEHEN	Participant
<ul style="list-style-type: none"><li>• NEHEN shall not release or disclose any PHI except as required by law or as defined in a Data Sharing Agreement or in a separate agreement between NEHEN and a Participant or between NEHEN and an External Trading Partner.</li></ul>	<ul style="list-style-type: none"><li>• Participant shall maintain and follow internal policies which shall govern release and disclosure of PHI.</li><li>• Participant may delegate responsibility for release or disclosure of PHI to NEHEN, in which case mutual responsibilities of NEHEN and Participant shall be defined in a written agreement.</li></ul>

### 2.4.3 Disclosure of Sensitive Health Information

Some federal, state, and local laws may impose requirements and restrictions on disclosure of certain types of health information and may require certain types of Patient consent for such disclosures. For example, Massachusetts law imposes restrictions on sharing Patient Information held by certain health plans related to treatment for HIV, mental health, and substance abuse.

Review of such laws has revealed that the laws may be difficult to interpret and may be difficult to implement in business operations and electronic systems given the current state of these systems. Additionally, research has shown that interpretation of the laws may vary significantly among healthcare organizations wishing to collaborate in the exchange of healthcare data. (*Reference the MA-HISPC Report.*) NEHEN Data Sharing Agreements shall be designed to apply more stringent restrictions where variations of interpretation or implementation are recognized.

Responsibility for restricting the transmission of Sensitive Health Information will reside with either the Sending Participant or NEHEN. If NEHEN assumes responsibility for restricting transmission of Sensitive Health Information, the NEHEN Board of Directors will approve the restriction methods.

NEHEN	Participant
<p>If Sensitive Health Information is not restricted by the Sending Participant, one of the following conditions shall apply:</p> <ul style="list-style-type: none"> <li>NEHEN shall remove Sensitive Health Information from transmissions as agreed with the Sending Participant. In this case, NEHEN and the Sending Participant shall execute a written agreement detailing the conditions and methods under which NEHEN shall remove the data. <b>Example:</b> A Payer Organization delegates to NEHEN the responsibility for removing restricted drug information from a list of paid claims for Patient medications. NEHEN removes the Sensitive Health Information from a Patient list before transmitting the list to a requesting Provider Organization.</li> <li>If NEHEN has not executed an agreement with the Sending Participant for removal of Sensitive Health Information and NEHEN has developed a method of removing Sensitive Health Information that is approved by the NEHEN Board of Directors, NEHEN shall employ such method to remove Sensitive Health Information from transmissions. <b>Example:</b> NEHEN removes restricted drug information from a list of paid claims for Patient medications obtained from a Payer Organization who has not executed an agreement for removal of Sensitive Health Information.</li> <li>If NEHEN has not executed an agreement with the Sending</li> </ul>	<p>If Sensitive Health Information is restricted by the Sending Participant, one of the following conditions shall apply:</p> <ul style="list-style-type: none"> <li>The Sending Participant shall obtain appropriate Patient consent, if required, prior to transmitting Sensitive Health Information and shall transmit such information only if such consent has been obtained. In this case, responsibility for restricting information on a Patient-by-Patient basis resides with the Sending Participant, and the Sending Participant shall inform NEHEN in writing that it appropriately restricts transmission of Sensitive Health Information. <b>Example:</b> A Payer Organization employs procedures for obtaining Patient consent according to its interpretation of law and restricts transmission of Sensitive Health Information based on whether such consent has been obtained.</li> <li>The Sending Participant shall remove Sensitive Health Information from a transmission or shall engage another party to remove such information. In this case, the Sending Participant shall inform NEHEN in writing that such data is removed from transmissions. <b>Example:</b> A Payer Organization contracts with its Pharmacy Benefit Manager to remove Sensitive Health Information from lists of paid claims for Patient medications prior to transmitting such lists.</li> </ul>

NEHEN	Participant
Participant for removal of Sensitive Health Information and NEHEN has not developed an approved method of removing Sensitive Health Information, NEHEN shall not accept transmissions from the Sending Participant.	If one of the above conditions applies, NEHEN shall not apply any further restriction.

## 2.5 Auditing Access to Patient Information

As Patient data are shared across NEHEN, the ability to monitor and audit how Users access information is essential to ensure that all Participants involved in data exchange are complying with access control policies. In addition, publicly announced audit and logging practices foster trust among stakeholders that Patient data are used only in appropriate ways by NEHEN and Participants.

NEHEN	Participant
<ul style="list-style-type: none"> <li>• NEHEN shall publish Implementation Guides that shall specify requirements for logging of messages pertaining to Patient data transmitted via NEHEN. NEHEN Implementation Guides shall contain general requirements for logging all messages and specific requirements for logging in the context of a use case implementation. Requirements shall include:               <ol style="list-style-type: none"> <li>a) Logs shall be immutable, meaning either that log information cannot be altered by anyone regardless of access privilege or that any alterations are tamper evident.</li> <li>b) Log records shall support reporting to Patients and other stakeholders of all disclosures of Patient data via NEHEN. Future enhancements may include alerts, alarms, and analysis.</li> <li>c) Log records shall contain, at a minimum, the following information:                   <ul style="list-style-type: none"> <li>▪ The identity of the Patient whose information was accessed</li> <li>▪ The identity of the User accessing the Patient data</li> <li>▪ The identity of the Participant with which the User is affiliated, and through whose systems NEHEN services were accessed</li> <li>▪ The type of Patient data or record accessed (e.g., pharmacy data, laboratory data, etc.) with 'sensitive' data specifically identified</li> <li>▪ The date and time of access</li> <li>▪ The source of the Patient data (i.e., the Participant from whose system the accessed</li> </ul> </li> </ol> </li> </ul>	<ul style="list-style-type: none"> <li>• Participant shall maintain logs of all messages transmitted using NEHEN services, in conformance with specifications published by NEHEN.</li> <li>• Participant shall consider logs to be PHI and shall secure them accordingly.</li> <li>• Participant shall support efficient access to these logs by NEHEN, including remote access by authorized NEHEN support personnel. Such secure access capabilities may be built into the NEHEN services that are deployed at Participant sites and networks.</li> <li>• Participant shall fully cooperate with any monitoring or auditing activities by providing information requested by NEHEN or other Participants regarding data exchanged or the secure and reliable operation of the network.</li> <li>• Participant shall retain logs for a period specified by law or regulation. If not specified by law or regulation, retention shall be not less than three years from the date of access to Patient data.</li> </ul>

NEHEN	Participant
<p data-bbox="451 253 764 280">Patient data were derived)</p> <ul data-bbox="207 302 1014 438" style="list-style-type: none"><li data-bbox="207 302 1014 362">• NEHEN shall maintain logs of all messages that pass through its systems.</li><li data-bbox="207 378 1014 438">• NEHEN shall consider logs to be PHI and secure them accordingly.</li></ul>	

## 2.6 Reporting Disclosures

Participants will be responsible for responding to Patient requests for reporting of disclosures of their PHI. NEHEN will support this requirement by making available the content of logs maintained by NEHEN for use in the Participants’ disclosure reporting processes.

NEHEN will only be able to make available data that pertains to a transmission that took place via NEHEN. Participants will be responsible for logging data related to other transmissions as required by their internal policies.

NEHEN	Participant
<ul style="list-style-type: none"> <li>• NEHEN shall make available to Participants who are parties to a clinical data transmission all log data maintained by NEHEN that pertains to the transmission.</li> <li>• NEHEN shall publish, as part of Data Exchange Standards, specifications for accessing of log information by authorized Participant staff.</li> </ul>	<ul style="list-style-type: none"> <li>• Participant shall maintain internal policies for reporting to Patients regarding PHI disclosures.</li> <li>• Participant shall be responsible for responding to Patient requests for disclosure and may use data in NEHEN logs to respond to such requests.</li> <li>• Participant shall have the ability report to Patients all disclosures represented in internal and NEHEN logs for not less than three years from the date of access to Patient data.</li> </ul>

## 2.7 Breach of Disclosure Policy

Both NEHEN and the Participants will work to ensure that Patient Information remains safe and protected. However, in the event that Patient Information is misused or the privacy and security of the information is compromised, the following policies outline the responsibilities of NEHEN and the Participants.

NEHEN	Participant
<p>In the event that NEHEN becomes aware of any actual or suspected breach, either through notification by a Participant or otherwise, NEHEN shall:</p> <ul style="list-style-type: none"> <li>• Notify any Participants whose data is affected by the breach.</li> <li>• Investigate (or require the applicable Participant to investigate) expediently and without unreasonable delay the scope and magnitude of such actual or suspected breach, and identify the root cause of the breach.</li> <li>• Mitigate (or require the applicable Participant to mitigate) to the extent practicable, any harmful effect of such breach that is known to NEHEN or the Participant. NEHEN's mitigation efforts shall correspond with and be dependent upon its internal risk analyses.</li> <li>• Notify (or require the applicable Participant to notify) the Patient and any applicable regulatory agencies as required by federal, state and local laws and regulations, except if a law enforcement agency determines that such notification impedes a criminal investigation.</li> </ul>	<ul style="list-style-type: none"> <li>• Participant shall maintain and uphold individual policies for the notice of misuse or breach of policies.</li> <li>• Participant shall appropriately train its personnel and inform them of sanctions and other action that will result from any breach of confidentiality.</li> <li>• Participant shall report any breaches and/or security incidents to the particular Participant or External Trading Partner whose data was improperly used. Notification shall be made in writing and in the most expedient time possible and without unreasonable delay.</li> <li>• Participant shall report to NEHEN any actual or suspected breach of confidentiality. Notification shall be made in writing in the most expedient time possible and without unreasonable delay.</li> <li>• Participant shall notify the Patient whose health information was disclosed in breach of policy.</li> </ul>

## 2.8 Access to Data Exchange Policies

NEHEN	Participant
<ul style="list-style-type: none"><li>• NEHEN shall provide access to its data exchange policies upon request.</li></ul>	<ul style="list-style-type: none"><li>• Participant shall provide access to its data exchange policies upon request.</li></ul>

## 2.9 Authentication and Authorization of System Users

Access to Patient data must be carefully controlled, given its sensitive and private nature. Data in electronic form are vulnerable to copying, tampering, and other misuse. NEHEN and its Participants will ensure that only system users who have been authenticated as being persons authorized to access a Patient’s health information for a specific permitted purpose are allowed access to that information.

NEHEN network security is based on the principle of ‘transitive trust’. That is, each node in a network data exchange must trust the immediate preceding node, and so on. Therefore, clear definition of the affiliation of individual User to a Participant organization is critical. A User who accesses data via NEHEN is assumed to have been registered as an authorized User by a Participant Organization.

For example, if a specialty hospital in Boston needs to exchange clinical data with a physician in California, the hospital may register the physician as a User who may exchange data via the hospital’s NEHEN connection. The physician may then send and/or receive clinical data via the methods offered by the hospital and supported by the physician’s local capabilities. For example, the hospital might use NEHEN services to fax information to the physician or might offer the physician access to messages via the hospital’s secure email. Alternatively, if such capability exists, the physician may be directed to register with another Participant who provides access to NEHEN services via a portal.

In conducting clinical data exchange via NEHEN, Participant organizations are the primary network destinations for addressing messages. Messages to and from individual Users will be routed via the Participant organization with which the User is affiliated. This policy is consistent with the need for individual Users to be invariably authenticated by a Participant system before access to Patient Information is granted.

NEHEN	Participant
<ul style="list-style-type: none"> <li>NEHEN shall establish ‘Roles’ for all Users, which define categories of Users of NEHEN services. These categories are based on the types of Patient data that these users need to access to perform their job functions, and the permitted purposes for such access. The permitted purposes are based on each User’s job function and relationship with the Patient. NEHEN Roles are used as community standard classifications, to enable Sending and Receiving Participants to establish access control rules that are meaningful to each other.</li> </ul> <p><b>Example:</b> Industry standards for healthcare stakeholder Roles are evolving. Initial data exchange programs have adopted simple structures, such as classifying users into two categories</p>	<ul style="list-style-type: none"> <li>Participant shall authenticate all system Users before the User is given access to any NEHEN resource containing Patient data. Such authentication shall be implemented using an authentication methodology that meets the minimum technical requirements for Authentication Assurance Level 2 set forth in National Institute of Standards and Technology Special Publication 800-63<sup>1</sup>.</li> <li>Participant shall assign each system User with access to NEHEN services to a specific Role as defined by NEHEN.</li> <li>Participants shall mutually communicate and authenticate credentials. In any data exchange, the Sending Participant shall communicate its credentials, and the Receiving Participant shall</li> </ul>

<sup>1</sup> Level 2 requires, among other technical specifications, Participants to authenticate system user’s identity using only single-factor authentication, which queries users for something they know (e.g., a password). Participants will be free to use only a password, and need not use it in combination with any other tokens, provided it protects against online guessing and replay attacks. Participants are required to implement initial identity-proofing procedures (either remote or in-person) that require Authorized Users to provide identifying materials and information upon application for access to information through NEHEN.

NEHEN	Participant
<p>(Roles): <i>clinical</i> and <i>administrative</i>. NEHEN will initially favor simple, broad Role definitions to facilitate adoption by Participants and will refine these definitions over time.</p>	<p>use such credentials to authenticate that the Sending Participant is a NEHEN Participant in good standing.</p> <ul style="list-style-type: none"> <li>Participant shall include in each request for Patient data a non-repudiable assertion as to the identity and Role of the system User who will receive the data.</li> <li>Participant shall verify that the user accessing received Patient Information has a Role that is permitted to access the type of data being requested from the Sending Participant.</li> </ul> <p><b>Example:</b> One User may be affiliated with multiple Participant organizations. Access privileges are governed by the Role of the User in the Participant organization to which the clinical message is addressed. A User may be the Primary Care Physician of a Patient in one clinic, authorized to view the full longitudinal health record in a message addressed to that clinic. The same User may play a specialist Role in another Participant organization, where messages are filtered to display only data needed for permitted purpose.</p> <ul style="list-style-type: none"> <li>Participant shall maintain policies and procedures that govern Users' ability to access information on or through the Participant's system and through NEHEN services ('Participant Access Policy').</li> <li>Participant shall impose appropriate sanctions for work force members who violate security policies or make improper use of Patient Information, including revocation of a User's authorization to access the network as may be appropriate under the circumstances.</li> <li>Participant shall provide its Participant Access Policies to any other Participant upon reasonable request.</li> </ul>

## 2.10 Use of Data Exchange Standards

Achieving data interoperability across Participants' systems requires the implementation of common data exchange standards by the systems involved. Traditionally, the healthcare sector has focused on data interface standards to support integration across clinical systems within a provider enterprise. Extension of these standards to inter-enterprise data movement requires the specification of coherent standards across the network from low level transport to common clinical terminology and reference codes.

Concurrent with the NEHEN policy development and implementation of clinical data exchange, Federal initiatives are under way to specify standards for secure and reliable healthcare data exchange between disparate healthcare entities over the Internet. The policies outlined below will evolve to conform to national and regional standards as they are institutionalized.

NEHEN	Participant
<ul style="list-style-type: none"> <li>• NEHEN shall adopt data element, message and network protocol standards (referred to as 'data exchange standards') that shall be used by NEHEN and Participants to securely and reliably exchange health information. Data exchange standards shall conform to open industry standards and be technology neutral so as to pose the lowest practical barrier to entry for Participants without sacrificing data security and privacy. Data exchange standards shall conform with standards and interoperability specifications as put forth by HITSP and related Federal HHS initiatives.</li> <li>• NEHEN shall develop, maintain, and publish Implementation Guides that set forth the data exchange standards. NEHEN Implementation Guides: <ul style="list-style-type: none"> <li>○ Shall be developed through a community process into which all interested Participants shall have input and shall have the right to propose alternatives.</li> <li>○ Shall be adapted and revised as needed to accommodate new use cases for community data exchange and to accommodate industry developments and changes.</li> <li>○ Shall be designed to allow Participants to progressively adapt to new and changed data exchange standards. For example, an "earlier" version of a standard shall be supported for an agreed-upon time period to allow Participants to adapt to a current version.</li> <li>○ Shall be designed to support the incremental growth of data granularity across the exchange. For example, a</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Participant shall comply with NEHEN Implementation Guides rigorously to support efficient interoperability across the network. Compliance shall include filling all mandatory data elements, making best efforts to fill optional data elements, and avoiding unconventional interpretations of data exchange standards not supported by the Implementation Guide.</li> <li>• Participant shall support the growth of semantic interoperability across Participants' systems by making best efforts to progress from unstructured data exchange to structured data exchange.</li> <li>• Participant shall make best efforts to adopt revised standards expeditiously so as to enable the community to keep up with technological development and industry best practices.</li> <li>• Participant shall maintain internal data and messaging formats and ensure that internal system changes do not adversely impact compliance with NEHEN data exchange standards.</li> </ul>

NEHEN	Participant
Participant may initially participate in NEHEN using primarily unstructured, text-based data and evolve to using more structured data.	

## 2.11 Security

Besides security mechanisms, supported through data exchange standards, used to ensure than only authorized Users access NEHEN resources, the community must consistently implement additional safeguards to protect the confidentiality and integrity of the its information assets.

NEHEN security policies are designed to meet minimum legal requirements and may be augmented by Participants based on best practices agreed to by the community.

NEHEN	Participant
<ul style="list-style-type: none"> <li>NEHEN shall maintain a secure environment for all its systems that handle Patient data and any centralized data repositories containing Patient or Participant data, including implementing and enforcing appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data.</li> <li>NEHEN shall ensure that in the operation of directories and registries such as Patient registries and Provider registries no incidental disclosure of data occurs during the process of searching for Patient or provider matches in the directories. Such controls shall be appropriate to the type of data searched. <b>Example:</b> A Provider directory is used to route clinical messages, and should enable the discovery of provider locations and affiliations to Participant institutions. A Patient registry (or RLS) shall not support wild-card queries for Patient names, which can lead to disclosure of information that the system User has no authority to access.</li> <li>NEHEN shall avoid the use of proprietary encryption algorithms, unless reviewed by qualified experts outside of the vendor in question and approved by Federal guidelines. Asymmetric crypto-system keys shall be of a length that yields equivalent strength. NEHEN’s key length requirements will be reviewed annually and upgraded as technology allows.</li> </ul>	<ul style="list-style-type: none"> <li>Participant shall maintain a secure environment for NEHEN-related infrastructure, services, and data to support the secure and reliable operation and continued development of NEHEN, including implementing and enforcing appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data accessed through NEHEN services.</li> <li>Participant shall employ security controls that meet applicable industry or federal standards so that the information and data being transmitted shall not introduce any viruses, worms, unauthorized cookies, trojans, malicious software, or “malware”. In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.</li> <li>Participant shall collaborate with NEHEN to develop security policies and to amend, repeal, or replace provisions as necessary to support the secure operation and continued development of the network.</li> <li>Participant shall conduct periodic reviews, not less than once in a calendar year, of Participant’s internal security controls, for example, logs, access reports, and incident tracking, and make results of the review available to NEHEN.</li> </ul>

## 2.12 Service Levels

System service levels and procedural controls are essential to support the reliable exchange of clinical data, and the incorporation of data sharing into critical clinical and operational workflows at Participant organizations.

NEHEN	Participant
<ul style="list-style-type: none"> <li>• NEHEN shall work with the Participants to develop ‘service levels’ for support of operational processes and problems that may arise during exchange of health data between Participants. These service levels shall include obligations on the part of NEHEN as well as expectations of the Participants involved in the exchange, to maintain a minimum level of network performance and continuity of operation.</li> <li>• For each business purpose, NEHEN shall identify network or operational risks that could affect Patient safety or quality of care, and define ground rules for each Participant involved to mitigate each risk. These rules shall govern the Participants’ and NEHEN’s responsibilities during the course of normal operations and in the event of problems.</li> <li>• NEHEN shall size and configure systems integral to the operation of the network to enable agreed-upon levels of performance. The performance level shall be determined based on what is essential for the efficient and effective implementation of the use case across the Participant organizations.</li> </ul> <p><b>Example:</b> NEHEN may host a Provider directory which is essential for locating the network address of specific providers to whom messages may be routed. To ensure that Users can unambiguously identify the Provider to which they can send a clinical message, it is essential that the Provider directory be available and responsive. Poor system performance can adversely affect the perception of this NEHEN service, and lead to reduced usage.</p>	<ul style="list-style-type: none"> <li>• Participant shall comply with service levels established for the exchange in order to support the efficient and effective clinical data exchange across the network, including assigning appropriate internal priority to maintaining compliance with service levels.</li> <li>• Participant shall size and configure internal systems integral to the operation of the network to enable agreed-upon levels of performance.</li> </ul>

### 3.0 Clinical Data Exchange Requirements and Best Practices

NEHEN will work with Participants to develop requirements and best practices for interoperability that will be incorporated into Implementation Guides. Participants will be required to comply with all mandatory requirements and will be required to make best efforts to comply with best practices.

#### 3.1 Registering Participants and Users

Requirement	Best Practice
<ul style="list-style-type: none"> <li>• Each Participant organization shall formally register its participation in NEHEN and shall provide identifying information required by NEHEN. Such information shall include but not be limited to:                             <ul style="list-style-type: none"> <li>○ Participant name</li> <li>○ Participant ID</li> <li>○ Participant address</li> <li>○ Participant affiliation (i.e., parent organization name and ID)</li> <li>○ Participant NEHEN gateway IDs</li> </ul> </li> <li>• All individuals who are direct addressees to receive clinical information via NEHEN services shall be licensed care providers and shall be associated with and registered by a Participant responsible for authenticating and authorizing the individual’s use of clinical information obtained via NEHEN. Such individuals are referred to as “Users.”</li> <li>• Each Participant organization shall provide to NEHEN message addressing information required by NEHEN for all Providers registered by the Participant. Such information shall include but not be limited to:                             <ul style="list-style-type: none"> <li>○ User name</li> <li>○ User ID (e.g., NPI for providers)</li> <li>○ User affiliation (i.e., Participant registering the User)</li> <li>○ User message addressing information (e.g., User NEHEN gateway ID)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Participant should make best efforts to register all eligible Users for participation in NEHEN.</li> <li>• Participant policies should not require Participant to obtain consent from individual Providers for registration to participate in NEHEN.</li> </ul>

### 3.2 Sending Clinical Data

Receiving Users have a reasonable expectation that their preferences for clinical data transmissions to them will be honored by Sending Participants and Sending Users.

Requirement	Best Practice
<ul style="list-style-type: none"> <li>Participant shall address a transmission of clinical data only to a Participant or User who is registered with NEHEN.</li> <li>Participant shall address a transmission of clinical data to only a single destination for a User.</li> </ul>	<ul style="list-style-type: none"> <li>Participant should maintain internal policies for whether clinical data contained in transmissions may contain data received from external sources.</li> <li>Participant should maintain internal policies for the timeliness with which clinical information should be sent.</li> <li>Participant should maintain internal policies for whether a Sending Participant or Sending User may specify preferences for how and when messages are to be delivered (e.g., specify urgency.)</li> <li>Participant should disambiguate User addressing information to the extent possible in systems used to address messages.                     <p><b>Example:</b> A Provider to whom a message is to be addressed practices in multiple locations and has multiple associated affiliations and destinations. Participant should make best efforts to identify the most appropriate destination based on information obtained from the Patient (e.g., at registration or during treatment.). If such information is not available, or internal systems are not capable of such addressing, Participant should address the message to the Provider’s preferred destination.</p> </li> <li>If a Sending Participant receives notification that a clinical data transmission is not accepted by the intended Receiving Participant or cannot be delivered to an intended Receiving User, the Sending Participant should investigate the cause of the problem, attempt to correct the problem, and attempt to re-deliver the transmission by the original method or an alternate method.</li> </ul>

### 3.3 Receiving Clinical Data

Sending Participants and Sending Users have a reasonable expectation that their clinical data transmissions will be delivered to the addressees identified on the transmission. Receiving Participants will be required to meet certain requirements to meet these expectations and ensure effective use of clinical data exchange services.

Requirement	Best Practice
<ul style="list-style-type: none"> <li>Participant shall accept all properly formed and addressed clinical data transmissions from Sending Participants and Sending Users and shall acknowledge receipt of such transmissions. Responsibility for receipt and acknowledgment may be shared between the Participant and the NEHEN Gateway.</li> <li>Participant shall reject clinical data transmissions that are not properly formed or not properly addressed and shall notify the Sending Participant of the rejection and reason. Responsibility for rejection and notification may be shared between the Participant and the NEHEN Gateway.</li> <li>Participant shall deliver accepted clinical data transmissions to the Participant’s Receiving User(s) within a reasonable period of time.</li> <li>If Participant designates a “general address” for receipt of external messages, Participant shall maintain internal policies and procedures for controlling access to such information and for distributing such information to other Users within the Participant organization.</li> </ul> <p><b>Example:</b> If a Receiving Participant (e.g., a Community Health Center, a Clinic, or a Payer Organization) specifies a “general inbox” to which external messages should be addressed, the Receiving Participant shall rigorously control access to the information received.</p>	<ul style="list-style-type: none"> <li>Participant should maintain internal policies for whether access to clinical data received from external sources may be extended to individuals other than the intended Receiving User (e.g., allow Receiving User to specify others, such as another licensed provider or assistant, to receive or view an incoming message.)</li> <li>Participant should maintain internal policies for whether Receiving User(s) are required to view clinical data received from external sources. Participant may allow Receiving User(s) to “turn off” receipt of some or all messages addressed to the Receiving User; however, Participant should encourage Receiving User(s) to view all messages.</li> <li>Participant should maintain internal policies for whether Receiving User(s) may specify preferences for how and when they receive messages from external sources (e.g., “as soon as available”, “bundled at end of day”); however, Participant should encourage Receiving User(s) to honor preferences specified by the Sending Participant or Sending User (e.g., “urgent delivery”).</li> <li>Participant should maintain internal policies for whether Receiving User(s) are required to retain clinical data received from external sources. Participant may allow Receiving User(s) to discard messages; however, received information that is generally considered to be an integral part of the Patient medical record should be imported into the medical record.</li> <li>Participant should notify the Sending Participant whether a clinical data transmission was delivered to the Receiving User(s) or failed to be delivered to the Receiving User(s).</li> </ul> <p><b>Example:</b> A clinical data transmission is accepted by the Receiving Participant but cannot be delivered to the intended Receiving User. The Receiving Participant should notify the Sending Participant that the transmission was not delivered to the intended individual addressee.</p>

## 4.0 Definitions

- **Affiliated Practitioner:** An affiliated practitioner refers to:
  - a) A Practitioner employed by or under contract to a Provider Organization to render health care services to the Provider Organization's Patients.
  - b) A Practitioner on a Provider Organization's formal medical staff.
  - c) A Practitioner providing services to a Provider Organization's Patients pursuant to a cross-coverage or on-call arrangement.
- **Audit Log:** An electronic record of the access of information via NEHEN, such as, for example, queries made by Authorized Users, type of information accessed, information flows between NEHEN and Participants, and date and time markers for those activities.
- **Authorized User:** An individual who has been authorized by a Participant or by NEHEN to access Patient Information in accordance with NEHEN policies and procedures.
- **Breach:** Any unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of Protected Health Information or Demographic Information. An Incidental Disclosure by NEHEN or a Participant is not a Breach.
- **Business Associate Agreement:** A written, signed agreement meeting the requirements of 45 CFR § 164.504(e).
- **Clinical Data:** Healthcare data directly related to care provided to individuals and data used to manage the exchange of clinical data.
- **Data Sharing Agreement:** A written, signed agreement between NEHEN and a Participant or between NEHEN and an External Trading Partner which sets forth the terms and conditions governing the operation of NEHEN and the rights and responsibilities of NEHEN and the Participant or External Trading Partner with respect to clinical data exchange.
- **De-Identified Data:** Data that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Data may be considered de-identified if it satisfies the requirements of 45 C.F.R. § 164.514(b).
- **Demographic Information:** A Patient's name, gender, address, date of birth, social security number, and other personally identifiable information, not including any information regarding a Patient's health or medical treatment or the names of any organizations that maintain medical records about such Patient.
- **External Trading Partner:** An organization that is not a NEHEN Participant but engages in clinical data exchange with NEHEN, provides clinical data services to NEHEN, or receives clinical data services from NEHEN. Examples may include local, regional and federal public health authorities and remote provider organizations that exchange Patient referrals and clinical summaries with NEHEN Participants via NEHEN.
- **Failed Access Attempt:** An instance in which an Authorized User or other individual attempting to access the HIE is denied access due to use of an inaccurate log-in, password, or other security token.
- **Health Information Exchange (HIE):** An organization or group of organizations which develops and manages a set of contractual conventions and terms, arranges for the means of electronic exchange of information, and develops and maintains HIE standards.

- **Implementation Guide:** A document intended for use by technical persons which defines standards, guidelines, and other rules for transmission of clinical data via NEHEN.
- **NEHEN Board of Directors:** The governing body of NEHEN, consisting of representatives of payer organizations, provider organizations, government organizations, and other organizations.
- **New England Healthcare Exchange Network, Inc. (NEHEN):** A consortium of payer organizations, provider organizations, government organizations, vendor organizations, and other organizations operating a healthcare data exchange in New England to facilitate the exchange of electronic healthcare data, including administrative, financial, and clinical data. *Note that this policy framework applies only to clinical data exchange.*
- **One-to-One Exchange:** A disclosure of Protected Health Information by one of the Patient's providers to one or more other providers treating the Patient with the Patient's knowledge and implicit or explicit consent where no records other than those of the Participants jointly providing health care services to the Patient are exchanged. A One-to-One Exchange is an electronic transfer of information that is understood and predictable to a Patient, because it mirrors a paper-based exchange, such as a referral to a specialist, a discharge summary sent to where the Patient is transferred, or lab results sent to the Practitioner who ordered them.
- **Participant:** A Provider Organization, Payer Organization, or Other Organization that has directly entered into a Data Sharing Agreement with NEHEN, accesses Protected Health Information via NEHEN, and actively participates in the exchange of electronic healthcare data via NEHEN.
- **Patient:** Any person who receives or may receive healthcare.
- **Patient Information:** Any information, individually identifiable or not, about a Patient.
- **Payer Organization:** An insurance company, health maintenance organization, employee health benefit plan established under ERISA, or any other entity that is legally authorized to provide health insurance coverage.
- **Pharmacy Benefit Manager:** A third-party administrator of prescription drug programs who may be responsible for processing and paying prescription drug claims, developing and maintaining a formulary, contracting with pharmacies, and negotiating discounts and rebates with drug manufacturers.
- **Policy:** A formal statement or plan that defines an organization's general beliefs, goals, and acceptable procedures for a specified subject area.
- **Policy Framework:** A set of policies that form the basis for making rules and guidelines and give overall direction for planning and development.
- **Practitioner:** A health care professional or a resident or student acting under the supervision of such a professional.
- **Protected Health Information (PHI):** Individually identifiable health information (e.g., any oral or recorded information relating to the past, present, or future physical or mental health of an individual; the provision of health care to the individual; or the payment for health care) of the type that is protected under the HIPAA Privacy Rule.
- **Provider Organization:** An entity such as a hospital, nursing home, home health agency or professional corporation legally authorized to provide health care services.
- **Receiving Participant:** A Participant engaged in receiving clinical data from another Participant via NEHEN.

- **Receiving User:** A person who is associated with a NEHEN Participant and receives clinical data via that association.
- **Sending Participant:** A Participant engaged in sending clinical data to another Participant via NEHEN.
- **Sending User:** A person who is associated with a NEHEN Participant and sends clinical data via that association.
- **Sensitive Health Information:** Any information subject to special privacy protection under state or federal law, including but not limited to, HIV/AIDS, mental health, alcohol and substance abuse, reproductive health, sexually-transmitted disease, and genetic testing information.
- **Vendor Organization:** A commercial organization providing clinical data or related services to NEHEN or a Participant.

## Appendix A: EMHI Participants in 2009

### Hospitals and Medical Groups:

- Atrius Health, *Physician Group Practice Alliance*
  - Dedham Medical Associates
  - Granite Medical
  - Harvard Vanguard Medical Associates
  - South Shore Medical Center
  - Southboro Medical Group
- Beth Israel Deaconess Medical Center, *Academic Medical Center*
- Children’s Hospital Boston, *Academic Medical Center*
- Dana-Farber Cancer Institute, *Specialty Hospital*
- Lahey Clinic, *Academic Medical Center*
- Massachusetts Eye and Ear Infirmary, *Specialty Hospital*
- Partners HealthCare System, Inc., *Integrated Delivery Network*
  - Brigham and Women’s Hospital
  - Massachusetts General Hospital
  - Partners Community Healthcare, Inc. (PCHI)
- Tufts Medical Center, *Academic Medical Center*
- Winchester Hospital, *Community Hospital*

### Health Plans:

- Blue Cross Blue Shield of Massachusetts
- Harvard Pilgrim Health Care
- Neighborhood Health Plan
- Tufts Health Plan

### Universities:

- Harvard University
- Brandeis University
- Tufts University