Mass HIway

Massachusetts Health Information Highway

Statewide Health Information Exchange

Policies and Procedures

Version 2

December 1, 2014

The Mass HIway is operated by the Commonwealth of Massachusetts' Executive Office of Health and Human Services (EOHHS). For more information visit www.masshiway.net.

Record of Changes

Version Number	Date	Description of Change	Author/Editor
1	October 28, 2012	Original release	Mass HIway
2	December 1, 2014	Significant update to the Mass HIway Policies and Procedures. Alignment of policies with *Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information* framework Codification of various Mass HIway policies, procedures and practices based on Mass HIway operational experience.	Mass HIway

Table of Contents

1. Introduction

The Mass HIway Policies and Procedures provide the Mass HIway, the statewide health information exchange operated by the Commonwealth of Massachusetts' Executive Office of Health and Human Services (EOHHS), and its Participants a common set of rules to guide exchange of personal health information (PHI) in a way that adheres to federal and state law and protects the privacy and security of Patient information.

1.1 Structure of Policies and Procedures

The Policies and Procedures follow the principles recommended by the Department of Health and Human Services Office of the National Coordinator (ONC) in the "Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information" published on December 15, 2008. Additional policy sections have been added that are specific to Massachusetts and its deployment of a statewide health information exchange.

The Policies and Procedures are organized around Mass HIway functionality. Currently, the Mass HIway offers two types of functionality:

- **Direct Messaging** allows encrypted "push" transactions between Participants.
- **Query & Retrieve** enables the listing of Participant-Patient relationships on the secure, web-based Mass HIway Relationship Listing Service (RLS) and makes this information available to other Participants. This service involves collection and storage of limited patient demographic data by the Mass HIway.

The Policies and Procedures are also organized to address variations in the way each Participant connects to the Mass HIway, whether through a Direct compliant electronic health record (EHR) system, through a LAND appliance, or through Webmail.

For each policy area, general policies are listed first followed by policies that apply specifically to the type of functionality. Mass HIway Participants, Integrators, and Authorized Personnel (see section 1.4 Defining Mass HIway Users) are accountable for adhering to the general policies and to the specific policies for the type(s) of functionality or connectivity option they use.

The Mass HIway may amend these Policies and Procedures from time to time. The Mass HIway will provide notice of changes by email to the Participant's designated Access Administrator and by posting changes to the Mass HIway website (www.masshiway.net) and EOHHS website (www.mass.gov/eohhs/gov/commissions-and-initiatives/masshiway/) in a manner and form that makes the changes apparent and readily available for review. The Mass HIway will post any such amendments on the Mass HIway websites at least thirty days before implementation of the amendment. However, the Mass HIway reserves the right to provide less notice, including no prior notice. It is the responsibility of the Participant to check the Mass HIway websites periodically for such updates. Participant's continued use of the Mass HIway constitutes acceptance of the changes.

1.2 Direct Messaging Services

Mass HIway provides technical services to enable private and secure transport of health information from one User to another. Sub-services include:

1.2.1 Technical Assessment & Connectivity Recommendation

Mass HIway helps Participants assess their current technology and to determine the best option for connecting to the Mass HIway for Direct Messaging.

1.2.2 Participant Authentication

Mass HIway verifies that Participants are who they claim to be. This is the one of the pre-requisites for trusted exchange and allows the Mass HIway to accurately represent a Participant to others.

1.2.3 Certificate Authority

Mass HIway issues and updates security certificates and encryption keys. These are the specific tools that:

- Encrypt and decrypt messages for private and secure transport of messages
- Attest to the authenticated identity of an organization
- Detect message tampering and ensure message integrity
- Prove message origin to for nonrepudiation

1.2.4 Connection to Direct Messaging Services

Mass HIway installs, sets up, tests, activates, and maintains connection to Mass HIway Services in coordination with a Participant's technology vendors. Connectivity options include:

EHR connection

Where a customer's health information system(s) is capable of a web services connection, customer may choose to connect directly to the Mass HIway.

Local Access for Network Distribution (LAND) connection

Where a customer's health information system(s) is not capable of a Direct connection, customer may choose to connect to the Mass HIway through a LAND appliance.

Webmail connection

Where a customer's health information system(s) are not capable of a Direct connection, customer may also choose to connect to the Mass HIway through a web based secure mail application.

1.2.5 Connection to Other Health Exchanges

Mass HIway connects to other trusted health information exchanges and Trusted HISPs and their users on behalf of Mass HIway Participants.

1.2.6 Direct Address Authority

Mass HIway issues and updates Direct addresses to Participants and their Authorized Personnel.

1.2.7 Provider Directory

Mass HIway publishes and maintains a statewide electronic Provider Directory of Mass HIway Participants and their Authorized Personnel.

1.2.8 Message Transformation

Where message sender and receivers utilize different message formats (e.g., S/MIME, XDR) Mass HIway transforms messages to the format of the data recipient. The Mass HIway does not perform Message Transformation on messages received from Non-Participant Users or Participants connecting through a trusted HISP at this time.

1.2.9 User Training and Documentation

Mass HIway will provide train-the-trainer and self-directed training tools and documentation as needed to educate Participants and Authorized Personnel on how to use the Mass HIway in compliance with the Policies & Procedures.

1.2.10 User Support

Mass HIway provides production, maintenance, and educational support to Participants. Note that Participants provide the first line of user support to their Authorized Personnel and may escalate issues and questions to the Mass HIway support team.

1.2.11 Reports

Mass HIway provides transaction log reports upon request to support Users' Accounting of Disclosure requests and breach investigations.

1.3 Query & Retrieve Services

In addition to the Direct Messaging services, Mass HIway provides services for statewide location of Patient information and secure medical record request. Sub-services include:

1.3.1 Technical Assessment & Connectivity Recommendation

Mass HIway helps Participants assess their current technology and to determine the best option for connecting to the Mass HIway for Query & Retrieve.

1.3.2 Connection to Query & Retrieve Services

Mass HIway sets up, tests, activates, and maintains connection to Mass HIway Services in coordination with a Participant's technology vendors. Connectivity options include:

EHR connection

Where a customer's health information system(s) is capable of a Direct connection, customer may choose to connect directly to the Mass HIway.

Provider Portal

Where a Participant's health information system(s) is not capable of integrating the Mass HIway Query & Retrieve web service, Participant may choose to connect through a web-based Provider Portal.

1.3.3 User Credentialing

Mass HIway issues and updates user names and passwords for Authorized Personnel that use the Provider Portal.

1.3.4 Relationship Listing Service or RLS

The Relationship Listing Service (RLS) is a searchable database that displays a list of Participants that have published a relationship with a Patient. The RLS is populated by Participants who transmit Patient demographic information with Patient consent.

1.3.5 Medical Record Request Service

The Medical Record Request Service facilitates the request of Patient records from another Participant. A record request may be initiated from the RLS, or manually by inputting Patient demographic data into the Medical Record Request Service.

1.3.6 Cross Entity Viewer

The Cross Entity Viewer is a variation of the Medical Record Request Service which facilitates Participant response to a Medical Record Request with the launch of a Medical Record Viewer. Note that the viewer is not a Mass HIway service – Mass HIway only makes the request for its launch.

1.3.7 Notification Service

Mass HIway provides notifications to Participants based upon trigger events. Currently notifications include the following:

"Break the Privacy Seal" Notification

Mass HIway sends a notification to a Participant's Access Administrator(s) each time one of the Participant's Authorized Personnel uses the "Break the Privacy Seal" feature to access a Patient's relationships on the RLS. (See Section 5.3.3 Relationship Listing Service "Break the Privacy Seal" Access).

1.4 Defining Mass HIway Users

The following definitions are used throughout the Policies and Procedures to differentiate the different types of organizations and individuals that use Mass HIway services:

1.4.1 Mass HIway User ("User")

An Organization that uses Mass HIway services is a *User*. *User* is the most general term and includes two (2) more specific terms based upon User's contractual relationship with the Mass HIway: Participant and Non-Participant**.**

1.4.2 Participant User ("Participant")

An organization that signs a Participation Agreement and uses Mass HIway services is a *Participant*. Participants may be single-legal entity organizations (e.g., Physician Practice, Hospital, Health Plan) or multi-entity organizations (e.g., Physician Hospital Organization (PHO), Independent Physician Association (IPA), Accountable Care Organization (ACO).

- A Participant must be an organization type that is permitted to use the Mass HIway services (See sections 4.1.2 *Permitted Users – General*, 4.2.2 *Permitted Users – Direct Messaging*, and 4.3.2 *Permitted Users – Query & Retrieve.*).
- A Participant connects to the Mass HIway directly or connects to the Mass HIway indirectly via a Trusted Health Information Service Provider (HISP).
- A Participant may connect to the Mass HIway with the help of an Integrator.
- A Participant is issued a domain and Direct addresses by Mass HIway or by a Trusted HISP.
- A Participant and its Authorized Personnel may be listed in the Mass HIway statewide Provider Directory.

1.4.3 Non-Participant User ("Non-Participant User")

An organization that does not sign a Mass HIway Access Agreement but that is granted access to the Mass HIway through a Trusted HISP is a *Non-Participant User*.

- A Non-Participant User signs an agreement and/or Business Associate Agreement with a Trusted HISP
- A Non-Participant User is issued a domain and Direct addresses by the Trusted HISP
- A Non-Participant User is able to send messages to and receive messages from Mass HIway Participants via the Trusted HISP and the Mass HIway
- The Mass HIway does not perform Message Transformation on messages received from Non-Participant Users at this time.
- Non-Participant Users are unable to access the RLS.

1.4.4 Mass HIway Integrator ("Integrator")

An Organization that connects Mass HIway Participants to the Mass HIway is an *Integrator*. Integrators are Business Associates of Participants and may include electronic health record (EHR) vendors, technical integrators, and regional health information organizations (RHIOs). Integrators use Mass HIway for HISP services.

1.4.5 Trusted Health Information Service Provider ("Trusted HISP")

A separate entity, not under the authority of the Mass HIway, providing health information exchange services to Users is a *Trusted HISP*.

- A Trusted HISP signs a HISP agreement with the Mass HIway
- A Trusted HISP sets and enforces its own policies and procedures with its users
- A Trusted HISP authenticates its users
- A Trusted HISP issues and maintains Direct addresses and security certificates for its users
- A Trusted HISP facilitates Direct Messaging for its users

1.4.6 Access Administrator ("Access Administrator")

Staff person(s) appointed by the Participant, with specific authority delegated by the Mass HIway to grant and administer access to Mass HIway services to the Participant's Authorized Personnel is an *Access Administrator*. Access Administrators have a number of obligations as further described throughout the Policies and Procedures document.

1.4.7 Authorized Personnel ("Authorized Personnel")

Staff persons of a User who have been granted access to Mass HIway services are *Authorized Personnel*. Authorized Personnel are granted access to Mass HIway services by an Access Administrator or by a comparable role with authority delegated by a Trusted HISP.

1.5 Defining Agreement Types

1.5.1 Participation Agreement ("Participation Agreement")

A legal agreement that defines the terms of access to Mass HIway services is a *Participation Agreement*. Participants, as defined above, sign Participant Agreements.

1.5.2 Business Associate Agreement ("Business Associate Agreement")

This definition has the meaning assigned to it in the Health Insurance Portability and Accountability (HIPAA) regulations.

1.5.3 HISP Agreement ("HISP Agreement")

A legal agreement that defines the terms of access to Mass HIway services for a Trusted HISP and its Users is a *HISP Agreement*. Trusted HISPs, as defined above, sign HISP Agreements.

1.5.4 Integrator Agreement ("Integrator Agreement")

A legal agreement that defines the terms of access to Mass HIway services for an Integrator is an *Integrator Agreement*. Integrators, as defined above, sign Integrator Agreements.

1.6 Defining Other Terms Used In Policies and Procedures

1.6.1 HIPAA Privacy and Security Rules ("HIPAA Privacy and Security Rules")

Standards of Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information, both at 45 CFR Parts 160 and 164, comprise the *HIPAA Privacy and Security Rules*.

1.6.2 HIway Provider Directory or Provider Directory or PD

A statewide listing of Direct Addresses for Participants and their Authorized Personnel that is accessed for selection of message destination is the *HIway Provider Directory*, also known as the *Provider Directory (PD)*.

1.6.3 Medical Record Number

A unique identifier assigned to a Patient by a healthcare provider for purposes of medical record keeping is a *Medical Record Number*.

1.6.4 Patient

An individual that receives healthcare services from a healthcare provider is a *Patient*.

1.6.5 Patient Demographic Data

Data about a Patient that identifies the Patient (such as name, address, and date of birth) and differentiates the Patient from other Patients that may have similar names is the *Patient Demographic Data*. See section 4.3.1 for demographic data collected by the Mass HIway for Query and Retrieve services.

1.6.6 Minimum Necessary Standard

For these Policies & Procedures, the definition of *Minimum Necessary Standard* shall be the same as its definition in the HIPAA Privacy and Security Rules.

2. Scope and Application

2.1 Scope and Application - General

The Policies and Procedures described in this document apply to all Participants and Integrators. The purpose of the Policies and Procedures are to provide clear direction so that Mass HIway Users understand the rules that govern use of the Mass HIway.

2.2 Acceptance of Terms

Use of the Mass HIway by Participants and Integrators constitutes acceptance of, and agreement to abide by all the requirements in these Policies and Procedures.

2.3 Incorporation by Reference

All the provisions of these Policies and Procedures are incorporated by reference into each Participation Agreement and Technical Integrator Agreement. All capitalized terms used in these Policies and Procedures shall have definitions provided herein.

2.4 Audits to Verify Proper Use of Mass HIway

The Mass HIway (or a third party engaged by the Mass HIway) may audit Participants and Integrators on a periodic basis. The purpose of these audits will be to confirm compliance with and proper use of the Mass HIway in accordance with the Participant Agreement, Integrator Agreement, and these Policies and Procedures.

Audits will take place during normal business hours and at mutually agreeable times and shall be limited to such records, personnel and other resources of the Participant as are necessary to determine proper use of the Mass HIway and compliance with the Access Agreement and these Policies and Procedures.

2.5 Merger, Acquisition, or Divestiture of Participant

Participant is responsible for notifying the Mass HIway of cases of merger, acquisition, or divestiture of a legal entity with another organization where such reorganization materially affects the Participant's use of the Mass HIway (e.g., Re-assignment of Access Administrator, Re-issuance of Direct addresses).

3. Openness and Transparency

The Mass HIway has been, and will continue to be, designed through an open and inclusive planning and decision-making process. MGL CH 118I designated a multi-stakeholder Health Information Technology Council (HIT Council) which provides input and advice regarding the Mass HIway directly to the EOHHS Secretary. In addition, the HIT Council is informed by multi-stakeholder Advisory Groups that bring Consumer/Patient and Healthcare Provider perspectives to the planning process as well as technical and legal expertise.

Information about Mass HIway activities are publically posted on the Mass HIway or EOHHS websites including Policies & Procedures, Participant Agreements, Rates, and all public meeting presentations and notes.

Mass HIway Participants are responsible for informing their own Patients of the Participant's use of Mass HIway services. Materials for educating Patients may be found on the Mass HIway or EOHHS websites.

4. Data Collection, Use, and Disclosure Limitation

4.1 Data Collection, Use, and Disclosure Limitation – General

4.1.1 Data Collection, Use, and Disclosure Limitation – General

Mass HIway has been designed so that Users take primary responsibility for data use and disclosure. Mass HIway is not a clinical data repository and collects and stores only the bare minimum data set required to operate the statewide health information exchange services. As such, Users are responsible for adhering to applicable federal and state laws, including without limitation the HIPAA Privacy Rule with regards to use and disclosure of PHI through the Mass HIway.

4.1.2 Permitted Users – General

Mass HIway services may be used by Covered Entities (including both Health Care Providers and Health Plans), Business Associates, and authorized Government Agencies, that are involved in Patient treatment, payment, or operations (TPO) as defined by HIPAA. Some Mass HIway levels of functionality may be more restrictive regarding Permitted Users. (See sections 4.2.2 *Permitted Users – Direct Messaging* and 4.3.2 *Permitted Users – Query & Retrieve.*)

4.1.3 Permitted and Prohibited Uses – General

Permitted uses of Mass HIway data by a Participant and its Authorized Personnel are currently limited to treatment, payment, or healthcare operations as defined by the HIPAA Privacy Rule. The Mass HIway may allow additional uses if it determines that such actions are in the public interest.

Prohibited uses of Mass HIway data by a Participant and its Authorized Personnel include the following:

- For illegal purposes or to further illegal activities including, without limitation, any upload, download, posting, distribution or facilitating the distribution of any material that constitutes unauthorized use or reproduction of material protected by copyright, trademark, trade secret or other intellectual property right.
- For any purpose or activity that is, or may be perceived as, obscene, threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, or invasive of another's privacy.
- For any unauthorized access to or inappropriate use of data, systems, and networks including, but not limited to, any probe or attempted probe, scan or vulnerability testing without the express authorization of The Mass HIway.
- To interfere with the service of any user, host or network, including deliberate attempts to overload a server, network connected device, or network component;

- To propagate malformed data or network traffic resulting in damage to, or disruption of, a service or network connected device;
- To forge data with the intent to misrepresent the origination user or source;
- To send unsolicited, mass electronic mail messages to one or more recipients or systems, including, without limitation, commercial advertising and informational announcements; or
- To forge electronic mail headers (including any portion of the IP packet header and/or electronic mail address) or to use any other method to forge, disguise, or conceal the user's identity or IP address.
- Any use that is not a Permitted Use

4.1.4 Disclosing Participants and Participant Uses of Mass HIway

The Mass HIway may publically disclose a list of Participants (organizations) through its website, marketing materials, and HIT Council meeting presentations.

The Mass HIway may publically disclose overall transaction volume and transaction volume by Participant type (e.g., Provider, Payer, Public Health Agency).

The Mass HIway does not have the ability to access information sent from one User to another and will not be able to determine, nor report on, Users' precise uses of the Mass HIway or the subjects of the messages sent.

The Mass HIway will not publically disclose transaction volume by Participant.

The Mass HIway allows Users to search the Provider Directory and may provide extracts of the Provider Directory to Users for permitted uses.

4.2 Data Collection, Use, and Disclosure – Direct Messaging

4.2.1 Data Collection, Use, and Disclosure - Direct Messaging

Mass HIway Direct Messaging functionality facilitates private and secure directed exchange of health information among Users. By design, Mass HIway has no way of accessing information being sent using Mass HIway Direct Messaging functionality and does not know the content, including Patient identity, of transacted messages. For Direct Messaging the Mass HIway has no role in collecting, using, or disclosing protected health information – these responsibilities belong solely to Users.

As the Mass HIway cannot see the contents of messages sent over the Mass HIway, it is unable to provide information with regards to which Participants are able to receive any particular type of message or document. Participants are encouraged to use the Provider Directory to determine which of their current trading partners are connected to the Mass HIway, then reach out to those Participants to determine which types of messages that organization is ready to receive before sending a message or document over the Mass HIway.

4.2.2 Permitted Users – Direct Messaging

Permitted users for Direct Messaging include: Massachusetts-licensed healthcare providers and provider organizations, Massachusetts-licensed Health Insurers, Government Agencies, Business Associates, and Non-Participant Users accessing Mass HIway through a Trusted HISP.

The Mass HIway maintains sole discretion to allow, deny, or suspend participation or use for any organization or individual.

4.2.3 Participant Data Collection and Use for Provider Directory

Data Elements Collected for Provider Directory

Mass HIway collects and uses Participant and Authorized Personnel data elements for operation of the Mass HIway Provider Directory. Required data elements are the bare minimum needed to operate the Provider Directory and will be collected as required by the Mass HIway.

Optional data may be collected and disclosed to enhance discovery of Participant addresses. Optional fields are found in the Participant address collection spreadsheet. The optional data that a Participant provides for the Provider Directory is at the discretion of the Participant. All collected data will be available for display in the Provider Directory so no sensitive data should be supplied.

Participant may provide required data elements initially and optional data elements at a later date.

Mass HIway may make all collected data elements discoverable in the Provider Directory.

Participant and Authorized Personnel Addressing

A Mass HIway Direct address is made up of 3 parts: a domain, an optional sub-domain, and a local name e.g., <<local name>>@direct.<<sub-domain>>.<<domain>>.masshiway.net. Each domain must be aligned with only one legal entity identified in a Participation Agreement. A Participant may have multiple sub-domains and local names.

A Participant's Access Administrator requests the <<domain>> and <<sub-domain>> portions of the address and Mass HIway issues them with mutual goals of maintaining addresses that are transparent and obvious to Users, avoiding duplicates, and ensuring standardization. Participant addresses must conform to the DIRECT protocol. The Participant's Access Administrator will assign the <<local name>> portions of the addresses and has full discretion in name selection.

The following are Mass HIway addressing conventions: [1]

[1] Note: Sub-domain addressing requires an interim workaround given vendor limitations at time of P&P update.

- **Single Legal Entity Participant with no sub-domains:**
  medical.records@direct.ParticipantA.masshiway.net
- **Single Legal Entity Participant with sub-domains:**

  Dr.A@direct.HospitalA.ParticipantB.masshiway.net

  Dr.B@direct.HospitalB.ParticipantB.masshiway.net
- **Multiple Legal Entity Participant with sub-domains:**

  Dr.C@direct.PracticeA.IntegratorA.masshiway.net
  Dr.D@direct.PracticeB.IntegratorA.masshiway.net

Provider Directory Data Upload

The Participant's Access Administrator is responsible for submitting the Mass HIway addressees for the Provider Directory using the Mass HIway *Provider Directory Provider Upload File Format* spreadsheet.csv file for bulk upload until a self-service option is available for upload by the Participants' Access Administrator.

Provider Directory Data Currency and Update

The Participant's Access Administrator is responsible for keeping its address data current.

If Participant has the following changes in its Authorized Personnel, the Mass HIway must be notified immediately:

- Termination / Suspension
- Completion of assignment (e.g., Resident)
- Resignation
- Lost or suspended license

If Authorized Personnel have a role change, the Mass HIway should be notified as soon as reasonably practicable, but no later than quarterly.

For all other changes to Authorized Personnel, the Mass HIway may be notified quarterly.

The Mass HIway will revoke certificates, make all updates to the Provider Directory, and take action to synchronize any Provider Directory copies.

Mass HIway will keep a master Provider Directory up to date and will periodically make copies available to Participants.

Permitted Use of the Provider Directory

The Mass HIway Provider Directory may be used only for purposes of exchanging information among Users, Integrators, and Authorized Personnel. Users, Integrators, and Authorized Personnel shall not publicly make available, sell, or otherwise share the Mass HIway Provider Directory.

Participants shall use active Mass HIway addresses and verify that the intended recipient is ready to receive that message type over the Mass HIway. If the

Participant is made aware that the intended recipient is not ready to receive that message type over the Mass HIway, the user shall find an alternative means to send the information

4.2.4 Data Collection, Use, and Disclosure – Webmail

Mass HIway administers webmail accounts on behalf of some Participants. As a Business Associate, Mass HIway is governed by HIPAA in its role as administrator of Webmail accounts and only accesses information for purposes of providing technical support to the Participant, or as otherwise agreed to in the Business Associate Agreement.

4.3 Data Collection, Use, and Disclosure – Query & Retrieve

4.3.1 Data Collection, Use, and Disclosure – Query & Retrieve

Mass HIway collects, uses, and discloses the following demographic data about individual Patients for the Relationship Listing Service. This data is provided to the Mass HIway by Participants with Patient consent. Clinical information is not sent to or held by the RLS. Mass HIway collects the minimum data set required to precisely match Patient identities and to enable the Relationship Listing Service to link an individual Patient identity to a Participant.

Patient demographic data collected, used, and disclosed:

- Patient Identifier (e.g., Organization specific Medical Record Number),
- Patient Name
- Patient Gender
- Patient Date of Birth
- Patient Address
- Patient Email
- Patient Phone Number

Mass HIway also collects and stores the following information:

- Participant sending the information and the Participant's Direct address
- Date message received
- Consent attestation – The Mass HIway will accept and store patient demographic data only for messages received with a "Yes" consent attestation, or messages with a "No" consent that override a previous "Yes" consent. The Mass HIway will discard all other messages sent with a "No" consent.

Any other data received from a Participant as part of publishing to the Relationship Listing Service is disposed of and not stored.

4.3.2 Permitted Users – Query & Retrieve

Mass HIway permitted users for the initial Query & Retrieve include: Massachusetts-licensed healthcare providers and provider organizations. It is

expected that Health Plans and Business Associates may be permitted users in future releases.

The HIway maintains sole discretion to allow, deny, or suspend participation or use for any organization or individual.

4.3.3 Relationship Listing Service and Sensitive Conditions

Participants that predominantly serve Patients with sensitive conditions (e.g., Title 42 substance abuse treatment centers) must determine whether or not listing of the Participant in the RLS for a given Patient constitutes a disclosure of sensitive information and whether use of the Mass HIway is permitted by law.

4.3.4 Relationship Listing Service and Minors

Minors are to be included in the RLS. Parents and legal guardians are authorized to provide consent for a minor. For mature or emancipated minors it is a Participant's responsibility to comply with the law and its own policies regarding whether the minor or their parent/legal guardian may assert consent.

On the minor's 18th birthday, Mass HIway will automatically turn the Patient's "Yes" consent to "No" in the RLS.

4.3.5 Relationship Listing Service Data Disclosure

The *Mass HIway Data Governance Advisory Group* assists the Mass HIway team with understanding and resolving potential issues related to data disclosure through the RLS and provides procedural guidance to the Mass HIway team.

4.3.6 Medical Record Request Service – General

The Medical Record Request Service allows Participants to submit electronic requests to other Participants for a given Patient’s records. Response to the medical record request is solely at the discretion of the data-holding Participant receiving the request. The Medical Record Request Service may be accessed through the Provider Portal or through a web service.

4.3.7 Medical Record Request Service – Obligations of Data Requestor

The Participant that makes a Medical Record Request shall request only records for Patients with whom the Participant has a treatment, payment, or healthcare operations relationship as defined by HIPAA.

The data requestor shall comply with the Minimum Necessary standard, as the term is defined in HIPAA, when requesting or viewing a Patient’s records from another Participant.

4.3.8 Medical Record Request Service – Responding to a Medical Record Request

The Participant holding the data (“Data Holder”) that receives a medical record request has the sole right and responsibility to:

- Accept or reject the data requestor credentials that are passed by the Mass HIway
- Verify the identity of the Patient for whom the request is made
- Determine the response to be made to any request for data

Data Holder has the sole right to respond to a request for data in the manner that Participant determines is appropriate, including the ability to deny the request.

Data Holder shall acknowledge the receipt of the request.

Data Holder shall comply with all applicable federal and state laws and regulations related to the disclosure of Patient information, including but not limited to, laws related to the release of HIV test results, genetic test information, substance abuse information, self-pay, and Minimum Necessary.

4.3.9 Cross Entity Viewer – General

The Cross Entity Viewer is a technical variation of the Medical Record Request Service. The service passes the credentials of the data requestor along with Patient demographic information. Upon the data holder evaluation of the request (may be manual or automated) and where data holder deems the request to be valid, the data holder permits the launch of a Patient record viewer in a separate browser that is outside of the Mass HIway. Note that Patient records will not be accessed, viewed or stored by the Mass HIway.

To use this service, Participant pairs must establish legal agreements and technology capabilities to access and view one another's Patient information. Participants may request that the Mass HIway enable a Cross Entity Viewer and each must sign a *Cross Entity Viewer Request Form* prior to the service being enabled.

5. Access Control

5.1 Access Control – General

Access to Mass HIway services is controlled through two Access Control models:

5.1.1 Direct Access Control by Mass HIway

Mass HIway controls access of Participants (organizations) and Integrators. Mass HIway delegates control of access of Authorized Personnel (individuals) to Participants' Access Administrators.

5.1.2 Indirect Access Control by Trusted HISP

Mass HIway controls access of HISPs. Mass HIway relies upon the Trusted HISP to control access of Participants and Non-Participant Users (organizations) as well as control of access of Authorized Personnel (individuals).

At this time, indirect Access Control by a Trusted HISP is only available for access to the Direct Secure Messaging service.

5.2 Access Control – Direct Messaging

5.2.1 Direct Access Control by Mass HIway

Participant Access

Mass HIway grants access to Mass HIway services to Participants. To be granted access the Participant must be a permitted user of the Mass HIway (See section 4.2.2) and must sign a Mass HIway Participant Agreement.

The Mass HIway may at any time suspend access to the Mass HIway by the Participant, Access Administrator and/or any of its Authorized Personnel as required to prevent unauthorized use of the Mass HIway; to prevent, investigate, or remedy a breach or security incident; to protect the integrity of the information systems operated by the Mass HIway and its contractors; or for violation of any of the requirements of these Policies and Procedures. The Mass HIway will restore such access as determined by the Mass HIway in its sole discretion.

Mass HIway enforces access control through issuance, management, and revocation of Participant security certificates for the Direct Messaging services. In addition, Mass HIway enforces access control through issuance, management, and revocation of Authorized Personnel credentials for Webmail services.

Authorized Personnel Access – Authority Delegated to Participant

Mass HIway formally delegates responsibility for individual access administration to Participants. Given that Participants are accountable for the privacy, security, and legal disclosure of their Patient information as defined by HIPAA including the physical, technical, and administrative access controls for the systems that interface with the Mass HIway, this is the appropriate level for individual access administration. Mass HIway delegates responsibility to specific Participant personnel that take the role of Access Administrator for their organization.

Access Administrators must be duly authorized by their organization to act on behalf of the Participant regarding the delegated administration, including the creation of accounts, for the Mass HIway.

Access Administrators will be issued user credentials (username and password) for the purpose of accessing delegated administrative functions, including the creations of accounts for the Mass HIway on behalf of the Participant. Access Administrators must keep user credentials confidential and not knowingly share them with anyone else, including co-workers, to use for any reason. Access Administrator is responsible, on behalf of the Participant, for any access gained as a result of negligence in failing to safeguard Access Administrator credentials. Access Administrator must immediately report to the Mass HIway any information that would lead a reasonable person to believe that someone else other than the Access Administrator had obtained access to Access Administrator credentials.

Access Administrator Responsibilities

The Access Administrator shall have the following responsibilities:

A. Access Administrators are responsible for being familiar with the Mass HIway Policies & Procedures, and monitoring their organization's compliance with the current Mass HIway Policies & Procedures.

B. Access Administrator shall verify and credential Authorized Personnel as members of the Participant organization and assess their need for access to the Mass HIway prior to creating an account and granting access rights.

C. Access Administrators shall advise and require all Authorized Personnel to keep their user names and passwords private.

D. Access Administrator shall review the accounts of Participant's Authorized Personnel and update any account that needs to be updated, including with information related to the account's listing in the Provider Directory. This shall be done as often as necessary, but in no event less often than quarterly (See section 4.2.3 *Participant Data Collection and Use for Provider Directory*).

E. Access Administrator shall terminate access to the Mass HIway immediately for any Authorized Personnel who no longer requires access by reason of termination of employment.

F. Access Administrator shall terminate access to the Mass HIway as soon as reasonably practicable for any Authorized Personnel who no longer requires access by reason of change in employment function or other reason.

G. Access Administrator shall suspend access to the Mass HIway for any Authorized Personnel who have information that would lead a reasonable person to believe that their account may have been breached, and shall promptly notify the Mass HIway of the suspected breach.

H. Access Administrator shall train and educate Authorized Personnel on the appropriate uses of the Mass HIway as described in the Policies and Procedures and as otherwise directed by the Mass HIway.

I. Access Administrator shall implement means to inform the Participant's Patients of the Participant's use of Mass HIway services.

J. Access Administrator shall submit Provider Directory information to the Mass HIway and shall keep Provider Directory information current.

K. Access Administrator shall have access to a Direct address which will be used for monitoring messages from the Mass HIway for purposes of Break the Seal Notification.

Designation of Access Administrator

Each Participant shall designate an individual to serve as Access Administrator in connection with the creation, oversight, and termination of Participant's Authorized Personnel. Mass HIway recommends designating a backup Access Administrator.

If a Participant feels that two Access Administrators are not sufficient to manage its Authorized Personnel, Participant may separately request that the Mass HIway credential additional Access Administrators; such request should contain a detailed rationale for why additional Access Administrators are necessary. Allowing for additional Access Administrators will be at the sole discretion of the Mass HIway.

Termination of Access Administrator

Each Participant is responsible for promptly disabling the identified individual's access to the Mass HIway when such individual can no longer perform the role of designated Access Administrator by reason of termination of employment or change in employment function.

Replacement of Access Administrator

Each Participant is responsible for having at least one (1) Access Administrator at all times, and for designating replacement Access Administrators as necessary.

Identification of Authorized Personnel

Each Participant's Access Administrator must provide the Mass HIway with a list of the Participant's Authorized Personnel, and such other information about such Authorized Personnel as the Mass HIway may reasonably require. Each Participant's process for identifying Authorized Personnel must include verifying each individual's identity, the individual's affiliation with the Participant, the individual's functional role with the Participant, and whether it is appropriate for the individual to send or receive information using the Mass HIway.

Assignment of Usernames and Passwords

Participant shall provide Authorized Personnel with a user name and a password to access the Mass HIway. Authorized Personnel are prohibited from sharing their user names and/or passwords with others and from using the user names and/or passwords of others.

Authorized Personnel Training and Compliance with Policies & Procedures

Participant is responsible for training all of its Authorized Personnel and ensuring that they have read and understood the Mass HIway Policies and Procedures. Each Participant shall ensure that all of its Authorized Personnel comply with the Mass HIway Policies and Procedures and comply with Participant's own privacy and security policies and procedures.

Termination of Authorized Personnel

Each Participant shall terminate access to the Mass HIway immediately for any Authorized Personnel who no longer require access by reason of termination of employment, and as soon as reasonably practicable for Authorized Personnel who no longer require access by reason of change in function. Each Participant shall terminate access to the Mass HIway immediately for any Authorized Personnel that engages in conduct that could undermine the security and integrity of the Mass HIway. Each Participant shall notify the Mass HIway immediately upon termination of any Authorized Personnel accounts.

5.2.2 Indirect Access Control by Trusted HISP

Trusted HISP Access

Mass HIway grants access to Mass HIway services only to HISPs that are trusted and that mutually agree to:

- Perform basic HISP functions in accordance with the Direct protocols including authenticating users, issuing Direct addresses, managing security keys, and routing Direct messages
- Execute Business Associate Agreements and/or other appropriate agreement with all users for whom the HISP routes messages and protect privacy and security of PHI and PII in line with HIPAA
- Protect anchor certificates: The Mass HIway and Service provider will use a device or approach that is compliant with *Federal Information Processing Standards (FIPS) Publication 140-2 Security Requirements for Cryptographic Modules*.
- Assure no interference or delay in message transmission and no alteration of message content. (Note: Transformation of message protocol is allowed)

Trusted HISP access is granted and maintained/controlled through execution of a HISP Agreement and sharing of anchor certificates. Mass HIway will not charge other HISPs nor will Mass HIway work with HISPs that charge the Mass HIway. Mass HIway will not charge Participants that use another HISP as their sole connection to the Mass HIway. (Note: There may be Participants that connect multiple ways. Joining directly and through a HISP does not exempt a Participant from fees)

The Mass HIway may at any time suspend access to the Mass HIway by the HISP and its users as required to prevent unauthorized use of the Mass HIway; to prevent, investigate, or remedy a breach or security incident; to protect the integrity of the information systems operated by the Mass HIway and its contractors. The Mass HIway will restore such access as determined by the Mass HIway in its sole discretion.

Authorized Personnel Access

A Trusted HISP is a separate entity that is not under the authority of the Mass HIway. The Trusted HISP is responsible for granting access to its users and Authorized Personnel. The Trusted HISP executes its own legal agreements, sets and enforces its own policies and procedures, authenticates users and Authorized Personnel, issues and maintains Direct addresses and security certificates, and facilitates Direct Messaging.

The Trusted HISP enforces access control through issuance, management, and revocation of user security certificates for the Direct Messaging services pursuant to its own policies and procedures.

5.2.3 Provider Directory Access

Access to the Mass HIway Provider Directory is limited to Participants, Non Participant Users, Integrators, and Trusted HISPs.

Mass HIway Provider Directory may be accessed through the Provider Portal, as a secure web service, or may be distributed by a .csv or other industry standard file for local upload or manual entry into a Participant's, Integrator's, or Trusted HISP's systems. The Provider Directory may be used only to facilitate use of the Mass HIway for uses permitted by these Policies and Procedures.

5.3 Access Control – Query and Retrieve

5.3.1 Relationship Listing Service Access Based On Data Contribution

At this time, Mass HIway will only allow RLS access to Participants that contribute Patient data and therefore document a consented relationship with the Patient, with the exception of Break the Privacy Seal access (See section 5.3.3 *Relationship Listing Service "Break the Privacy Seal" Access*.). Mass HIway will continue to monitor RLS access requests for Participants that are not able to submit data but where it is in the public interest for them to be able to access the RLS.

5.3.2 Cross Entity Viewer Access

A Cross-entity viewer will be enabled between Participants that have entered into an agreement that allows for the use of a Cross Entity Viewer.

Mass HIway will pass user credentials when Participants use the cross-entity viewer. It is up to the Participant to evaluate credentials and determine Participant access and monitor use of the viewer.

5.3.3 Relationship Listing Service "Break the Privacy Seal" Access

Break the Privacy Seal access is intended to facilitate care in medical emergencies. This section describes the use of the feature and associated security controls.

In non-emergency situations, only those Participants that have published Relationships to the RLS for a given Patient are permitted to view relationships for that Patient on the RLS. This is enforced through a technical control that limits relationship list access.

Authorized Personnel shall only search, publish, or view the RLS for Patients with whom the Authorized Personnel have treatment, payment, or healthcare operations relationships as defined by HIPAA.

Authorized Personnel may use the "Break the Privacy Seal" function in cases where the Participant does not have a previously established relationship with a Patient recorded in the RLS and where there is clear medical necessity to access the RLS.

Access to the "Break the Privacy Seal" function is limited to clinical users who have a defined system role of "emergency care" by their Access Administrator.

Clinicians who are not assigned this "emergency care" role will be able to search for and find a Patient, but will not be able to access their Relationship List. In this case the RLS display area shows the following text "Some items are not shown due to privacy restrictions".

A User who uses the "Break the Privacy Seal" function will be prompted to provide a reason for each access instance; the reason, date, and time will be logged for follow up. (Note: The User will continue to have access to the Patient's RLS until they log out or close their session. If access is needed again at a future time, user will be required to repeat the "Break the Privacy Seal" process.)

Notification of "Break the Privacy Seal" access will be sent to the Participant's Access Administrator at each occurrence. It is the responsibility of the Access Administrator to determine whether access was warranted and to follow up accordingly.

It is the responsibility of the Participant User who used the Break the Privacy Seal function to follow the Participant's policies when determining if the Patient must be informed when "Break the Privacy Seal" has been used to access the Patient's listing in the RLS.

Mass HIway will create an exception reporting process to monitor overall use of the "Break the Privacy Seal" function and where necessary, may take steps to suspend access to the function and conduct a review of the Participant's use of the function.

6. Consent

6.1 Consent – General

6.1.1 Scope of Consent

Participant is responsible for obtaining Patient permission to share Patient information over the Mass HIway. This permission pertains solely to the use of the Mass HIway. Participant is responsible for obtaining any and all additional Patient consents and authorizations, including without limitation consent to release HIV test results, genetic test information, substance abuse information, and as otherwise required by law.

Transactions covered under separate statutory authority (e.g., Mandatory Public Health reporting) are not subject to the Patient consent policy.

HIPAA defined administrative transactions that directly support payment are not subject to the Patient consent policy.

Transactions sent over the Mass HIway between a Covered Entity and its Business Associate(s) for healthcare operations are not subject to the Patient consent policy.

6.1.2 Consent – Forms and Language

The Mass HIway does not prescribe specific consent forms or language and thus allows Participants flexibility in designing and implementing Mass HIway consent processes in accordance with their local processes and Patient needs. Optional templates and educational resources are available at www.masshiway.net to assist Participants with development of their policies, processes, and materials.

6.1.3 Consent – Duration

Mass HIway imposes no specified duration on Mass HIway consent. The following situations require new consent collection by a Participant:

Changes in HIway Functionality

New consent must be obtained if a Participant has consented Patients solely for Direct Messaging and later adds Query & Retrieve functionality. Should a Participant wish to implement the Mass HIway functionality in stages, but does not want to obtain new consent when adding Query & Retrieve, the Participant may do so by following Query & Retrieve consent requirements. While the Mass HIway does not anticipate any additional changes in Mass HIway functionality that would require new consent, the Mass HIway reserves the right to create new consent requirements if appropriate.

Change in status of adolescent Patients

Participants shall follow the law and their own internal policies when it comes to mature and emancipated minors. However, the system will automatically reset the consent to "No" upon the Patient's 18th birthday.

6.1.4 Consent – Changes to Patient Consent Preference

Participants are required to allow Patients to change their Mass HIway consent preferences.

6.2 Consent – Direct Messaging

6.2.1 Consent Requirements

If Participant is solely enabling Direct Messaging functionality:

- Participant must get Patient permission to use the Mass HIway to transmit Patient health information.
- Participant must identify the Mass HIway as a mode of exchange.

6.3 Consent – Query & Retrieve

6.3.1 Consent Requirements

If Participant is enabling Query &Retrieve functionality:

- Participant must get Patient permission to use the Mass HIway to transmit Patient health information.
- Participant must identify the Mass HIway as a mode of exchange.
- Participant must get Patient permission to transmit specified Patient demographic information (See Section 4.3.1 *Data Collection, Use, and Disclosure – Query & Retrieve*) to the Mass HIway RLS, which stores the Patient demographic information and discloses the Participant's relationship with the Patient to other authorized RLS users.

- As part of obtaining this permission, Participant must describe the Mass HIway Query & Retrieve functionality to the Patient.

6.3.2 Consent – Changes

Participants are required to allow Patients to change their Mass HIway consent preferences. Participants are responsible for updating consent preferences with the Mass HIway.

7. Patient Access

7.1 Patient Access – Direct Messaging

Patient may request a copy of his/her medical records directly from the healthcare provider that holds the record. Mass HIway has no way of accessing a Patient record.

7.2 Patient Access – Query & Retrieve

Participant shall provide a report of the relationships listed on the Relationship Listing Service to a Patient upon Patient request. Mass HIway will provide the reports to support the Patient request.

8. Patient Correction

8.1 Correction – Direct Messaging

Patient may request a correction to his/her medical records directly from the healthcare provider that holds the record. Mass HIway has no way of accessing a Patient record.

8.2 Correction – Query & Retrieve

Patient may request a correction to his/her information on the Mass HIway Relationship Listing Service by contacting the healthcare provider that provided the record to the Mass HIway. Participant will then submit corrected information to the Mass HIway Relationship Listing Service.

9. Transaction Logs

9.1 Transaction Logs – General

Transaction logs may be used for the following purposes:

- To support Participant audits, accounting of disclosure requests, and breach investigations
- To support operational reporting of Mass HIway usage volume

Transaction logs may be accessed directly only by Mass HIway personnel, including EOHHS and vendor staff.

Transaction logs may be transmitted to a Mass HIway Participant Access Administrator upon request. Requesting Participant will be given a log containing only the messages in which Participant is the sender or receiver. Requests for transaction logs where Participant is neither the sender nor the receiver require permission from each Participant in the requested report.

An individual Patient may contact a Participant directly for an accounting of disclosures for the Relationship Listing Service about themselves or an individual for whom he/she is the legal guardian. Participant may then request transaction log information from Mass HIway. Mass HIway will provide the transaction information to the Participant.

9.2 Transaction Logs – Direct Messaging

Mass HIway will keep a transaction log of Direct messages sent from and received by Participants for the purposes of audit, breach investigation, and responding to Patient accounting of disclosures requests.

Transaction log will contain the following data elements:

A. Sender Direct address

B. Receiver Direct address

C. Date and time of transaction

D. Optional message ID

The transaction log will not contain any Patient information. By design, the Mass HIway cannot access the message contents and has no way of identifying the Patient or anything about the Patient.

Patients will be directed to Participants for requests for accounting of disclosures. Participants may request Transaction logs from Mass HIway to support accounting of disclosures requests.

9.3 Transaction Logs – Query & Retrieve

Mass HIway will collect and maintain a log of the limited Patient information for which Mass HIway is the recipient. The following information is collected for purposes of audit, breach investigation, and responding to Patient accounting of disclosures requests. Notes are provided to explain information limitations.

9.3.1 Relationship Listing Service (RLS) Publish Log

Log of messages sent from Mass HIway Participants noting that the Participant has a consented relationship with a specific Patient and that this relationship may be published to the RLS -or- that this relationship with a specific Patient may no longer be published to the RLS.

9.3.2 RLS View Log

Log of individuals that have viewed the Patient's relationships on the RLS. (Note that an individual's organization must have an existing consented relationship with the Patient in order for the individual to be allowed access to view the RLS.)

9.3.3 Break the Privacy Seal Log

Log of individuals that have used the "Break the Privacy Seal" function to view the Patient's relationships on the RLS. ("Break the Privacy Seal" is used for individuals that require access to view the RLS for a specific Patient but where a previous consented relationship has not been established.)

9.3.4 Medical Record Request Log

Log of individuals that have initiated medical records requests (including cross entity viewer) from the RLS.

Mass HIway cannot track and audit messages initiated outside the Mass HIway RLS (e.g., Replies to Medical Record Requests, Cross Entity Viewer Displays.)

Transaction logs will contain the following data elements that apply:

- Patient demographic information (as limited by RLS data elements collected)
- Direct address and user credentials for individuals accessing Patient information.
- Date and time of each access.

Patients will be directed to Participants for requests for accounting of disclosures. Participants may request transaction logs from Mass HIway to support accounting of disclosures requests.

10. Data Quality and Integrity

Mass HIway supports data quality and integrity through its technical design. Participants maintain full control over their Patients' information. Where Mass HIway holds information it is a copy of data created by and updated by Participants. Mass HIway does not modify the data thus avoiding data discrepancies between Mass HIway and its Participants.

10.1 Data Quality and Integrity – Direct Messaging

Participants are responsible for ensuring accuracy, completion, and currency of Patient information sent via the Mass HIway. Mass HIway has no access to Patient records and takes no role in ensuring quality and integrity of Patient records.

Mass HIway delivers messages from one Participant to another Participant where Mass HIway is the HISP. This includes delivery to the Participant domain or to the Integrator designated by the Participant. Participants are responsible for intra-organizational routing, and routing between entities under an Integrator.

Where members of another HISP utilize Mass HIway, Mass HIway will deliver messages to the HISP. Delivery to the addressee under the HISP is the responsibility of the other HISP. The Mass HIway does not perform Message Transformation on messages received from Non-Participant Users or Participants connecting through a trusted HISP at this time.

Mass HIway employs public key infrastructure to verify integrity of messages sent over the Mass HIway. If Mass HIway is notified of a failed message delivery, that notification will be forwarded to the Participant.

10.2 Data Quality and Integrity – Query & Retrieve

Participants are responsible for ensuring the accuracy, completion, and currency of Patient demographic information submitted to the Relationship Listing Service.

Mass HIway is responsible for the accuracy of Patient matching, based on the data received from the Participants. Mass HIway staff will periodically review and adjust the RLS so that two or more messages regarding an individual are linked only when Mass HIway staff is reasonably certain that the identities in the messages are for the same person. Mass HIway staff will manually review and resolve situations where demographic information for two or more individuals is very similar. Mass HIway staff may contact Participants for additional information as part of the Patient identity matching process.

11. Safeguards

Given that Mass HIway and its Users, Integrators, and Trusted HISPs all steward personal health information, they are bound by the HIPAA Security rule. The rule provides comprehensive requirements for protection of personal health information. Rather than duplicating the HIPAA Security rule in these policies & procedures, the Mass HIway has chosen to keep the policies & procedures aligned with and reference HIPAA.

11.1 Safeguards – General

11.1.1 Compliance with HIPAA

The Mass HIway and its Users, Integrators, and Trusted HISPs all must comply with HIPAA provisions with regards to security safeguards including:

- § 164.308 Administrative safeguards
- § 164.312 Technical safeguards
- § 164.310 Physical safeguards

11.1.2 Participant Responsibilities

Participant is accountable for the following Patient privacy and security protections:

- Authorizing users
- Issuing user credentials
- Training users

11.1.3 Duty to Report

Participants should immediately report any weaknesses in or breach of system security and/or any incidents of possible misuse or violations of these Policies and Procedures to the Mass HIway.

11.1.4 Mass HIway Safeguards

Participants may not attempt to disable, modify, or circumvent any security safeguards adopted by the Mass HIway. Participant acknowledges and agrees that the Mass HIway can monitor, record, and Audit use of the Mass HIway in order to protect the security of the Mass HIway.

11.1.5 Non-disclosure of Security Information

Participant and its Authorized Personnel shall not divulge connectivity details, passwords, or other access control information that could be used by a third party to gain unauthorized access to the Mass HIway.

11.1.6 Physical Security

Participant and Authorized Personnel shall take reasonable precautions to secure their physical working environment to guard against unauthorized access including, but not limited to workstations, laptops or HIE issued software, certificates, private keys or network connected devices (e.g. LAND). In addition, the Participant and Authorized Personnel shall take security precautions in the workspace such as the use of password screen locks, session timeouts, logging out of workstations at the end of the working day and strong passwords.

11.1.7 Network Security

Participant must maintain a secure network through measures such as multiple firewalls configured for high availability and minimal vulnerability and the latest versions of OS and antivirus protection.

11.1 Safeguards – Direct Messaging

Mass HIway and its Users, Integrators, and Trusted HISPs shall safeguard personal health information that is sent via the Direct messaging service. Mass HIway has put the following safeguards in place:

- Mass HIway controls Access to the Mass HIway using legally binding agreements to clearly define rules for Access. (See section 5 *Access Control* for policies and procedures governing access.)
- Mass HIway delegates responsibility to its Participants for maintaining safeguards in compliance with HIPAA. (See section 5 *Access Control* for policies and procedures governing access.)
- Mass HIway authenticates and authorizes Participant organizations. Mass HIway delegates authority to Participants for user authentication and authorization. Mass HIway facilitates exchange with peer HISPs and relies upon these HISPs to authenticate and authorize their users.
- The Mass HIway follows the nationally recognized Direct standard for secure messaging of health information. The technology includes Public Key Infrastructure (PKI) and Certificate Authority (CA) which are used to achieve the following security objectives:
    - Confidentiality: Security keys encrypt and decrypt messages so they may be sent securely.

  - Authentication: Certificate Authority attests to the verified identity of a certificate holder.
  - Integrity: Recipient can identify tampering of a signed message and tampered messages fail.
  - Nonrepudiation: Message signed with private key proves the message origin
- Mass HIway uses security keys to limit access to authenticated and authorized Participants and their Authorized Personnel.
- Mass HIway permits Users that have been authenticated and authorized by a Trusted HISP to exchange Direct messages with Mass HIway Participants and their Authorized Personnel.
- Mass HIway uses a secure data center to facilitate the Direct messaging service. The data center uses appropriate administrative, technical, and physical safeguards in compliance with HIPAA.
- Mass HIway encrypts all data sent via the Direct messaging service so that it may not be intercepted and accessed in line with the Direct standards. Mass HIway works with Trusted HISPs to encrypt data coming from and going to the Trusted HISPs.

11.2 Safeguards – Query & Retrieve

Mass HIway and its Participants and Authorized Personnel shall safeguard personal health information that is accessed via the Query & Retrieve service. Mass HIway has put the following safeguards in place:

- Mass HIway protects data stored for the Query & Retrieve services by limiting access to Authorized Personnel. (See section 5.3 *Access Control – Query and Retrieve* for policies and procedures governing Query & Retrieve access.)

11.3 Safeguards – LAND

Mass HIway regularly monitors LAND devices for vulnerabilities and corrects such vulnerabilities when discovered. Mass HIway keeps LAND technology up to date with appropriate security patches.

11.4 Safeguards – Webmail

11.4.1 Access to Webmail

Participant shall use appropriate care to access Webmail only from computers and networks with adequate security and privacy for handling PHI.

11.4.2 Webmail – Security Procedures

Participant will implement safeguards that are reasonable and appropriate to ensure the security of the Mass HIway. Security of any Authorized Personnel's PCs, laptops, tablets or other devices that use Webmail is the responsibility of the Participant. Participant is also responsible for having processes in place to reduce vulnerabilities for data breach. Security of webmail content downloaded via the Mass HIway Webmail interface is the responsibility of the Participant.

11.4.3 Webmail Capacity

Each webmail account will be subject to a storage capacity limit of 10MB per message, including attachments, and 1GB for the mailbox itself. The Mass HIway will notify Authorized Personnel when their webmail account has reached its storage capacity limit, after which the webmail account will not be able to receive additional messages until messages have been removed to allow additional storage. The Mass HIway will not delete or archive messages in a webmail account, but will not deliver messages to an account when it is over its storage capacity limit.

EVERY PARTICIPANT AND AUTHORIZED PERSONNEL AGREES AND ACKNOWLEDGES THAT THEY WILL NOT BE ABLE TO RECEIVE MESSAGES SENT TO THEIR WEBMAIL ACCOUNT WHEN IT IS OVER ITS STORAGE LIMIT CAPACITY.

11.4.4 Webmail Supported Browsers

Webmail will be supported on PC/Mac browsers with a default or Medium security setting for versions as specified below:

- Internet Explorer 8+
- Firefox 5+
- Safari 5+

11.4.5 Webmail – Workforce and Permitted Users

Participant shall be responsible for training its own workforce regarding the fundamentals of operating the Mass HIway Web Portal. Participant shall comply with all Mass HIway polices relating to the use of the Portal, including without limitation Mass HIway privacy, information security, and acceptable use policies as further described in the Policies and Procedures.

11.4.6 Webmail – Suspension of Account

Mass HIway may at any time suspend Participant's access to the Mass HIway Web Portal or suspend any Authorized Personnel as required to prevent unauthorized use of the Mass HIway Web Portal, to prevent, investigate, or remedy a privacy breach or security incident, or to protect the integrity of the information systems operated by EOHHS and its contractors. The Mass HIway will restore such access as determined by the Mass HIway in its sole discretion.

11.4.7 Webmail – Mass HIway Safeguards

Participant will not attempt to disable, modify or circumvent any security safeguard adopted by Mass HIway. Participant acknowledges and agrees that Mass HIway may monitor, record and audit Participant's use of the Mass HIway Web Portal in order to protect Patient privacy, protect the security of information maintained in databases, and protect the security of EOHHS' information system.

11.4.8 Webmail - Participant Safeguards

Participant shall implement reasonable and appropriate safeguards to protect the confidentiality, integrity and availability of the information it maintains, stores and transmits using the Mass HIway Web Portal and all information made available to Participant, including but not limited to keeping information such as user names and passwords confidential.

12. Breach Response

12.1 Breach Investigation and Public Notification

Mass HIway and its Participants will follow existing laws in cases of a security breach. In line with current laws governing breach, the Covered Entity will take primary accountability for breach investigation and public notification. Where Mass HIway is directly involved in the breach, Mass HIway will provide full support for breach investigation and notification. Where Mass HIway is indirectly involved in the breach, Mass HIway will provide transaction logs to support breach investigation.

Authorized Personnel are obligated to report all breach events to their Access Administrator and organization's privacy and security officer(s) immediately after their discovery. The Access Administrator is shall advise the Mass HIway of the breach event. Other individuals who have information about breach events involving the Mass HIway are encouraged to file reports or complaints with the EOHHS privacy and security officer or his/her designee.

13. Local Access for Network Distribution (LAND)

13.1 LAND – General

If the Participant has elected to use LAND Appliance services ("LAND Services") additional provisions shall apply. "LAND Contractor" shall mean any Contractor(s) used by the Mass HIway to provide hardware, software, or services in connection with the LAND Appliance.

13.2 LAND – Provisioning

The Mass HIway or its LAND Contractor will ship or deliver an Appliance to Participant according to an agreed-to schedule following Participant's election to use the LAND Services. LAND Contractor shall ensure such Appliance is configured for remote management to allow for software upgrades installed automatically from a remote site and reinstallation of standard and specialized configuration parameters that will be retained electronically at a remote site to facilitate ready deployment of a replacement unit if necessary. The LAND Contractor shall provide Tier 2 and 3 technical support to Participant as part of the annual fee. If the LAND Contractor determines that an issue cannot be resolved remotely, the LAND Contractor will arrange to exchange the Appliance.

13.3 LAND – License Grant

Subject to the terms and conditions of the Participation Agreement and these Policies and Procedures, Participant is granted a non-exclusive, annual license, renewable upon payment of the annual fee, to use: (i) certain LAND Contractor proprietary computer software contained in the Appliance in binary executable form only (the "Software"), (ii) certain LAND Contractor supplied computer hardware (the "Hardware") and (iii) certain LAND Contractor proprietary documentation in the form generally made available by LAND Contractor to its customers for use with these deliverables, (the "Documentation"). The Software and Hardware are collectively referred to herein as the Appliance ("Appliance"). The Appliance and Documentation are collectively referred to herein as the "Product."

13.4 LAND – Intellectual Property Rights

For purposes of these Policies and Procedures, "LAND Intellectual Property Rights" means in connection with the Product, any and all rights existing from time to time under patent law, copyright law, semiconductor chip protection law, moral rights law, trade secret law, trademark law, unfair competition law, publicity rights law, privacy rights law, and any and all other proprietary rights, and any and all applications, renewals, extensions and restorations thereof, now or hereafter in force and effect worldwide. The LAND Contractor, its licensors, and EOHHS will retain all ownership rights, title, and LAND Intellectual Property Rights in and to the Product Participant acknowledges that its possession, installation or use of the Product will not transfer to it any title to such property.

13.5 LAND – Use of LAND Software, Documents, and Appliance

The Participant agrees not to, or to allow others to: (i) adapt, alter, modify, decompile, translate, disassemble, or reverse engineer the Product or any component thereof, including without limitation, the source code and any other underlying ideas or algorithms of the Software (except to the extent applicable laws specifically prohibit such restriction); (ii) alter the number of documents authorized for Participant's use; (iii) create separate license keys that enable the Software; (iv) copy the Software; (v) use the Product for high risk activities; (vi) transfer, sublicense, loan, sell, lease or use for timesharing or service bureau purposes the Product or any component thereof; or (vii) ship, divert, transship, transfer, export or re-export the Product or any component thereof into any country or use it in any manner prohibited by any export control laws, restrictions, or regulations administered by the U.S. Commerce Department's Bureau of Export Administration, the U.S. Department of Treasury's Office of Foreign Assets Control or any other applicable government agency. For the avoidance of doubt, nothing in the Participation Agreement or these Policies and Procedures grants to Participant any rights whatsoever in or relating to the source code of the Software. Any trade names, trademarks, service marks, logos, trade dress, and any other distinctive or proprietary symbols, labels, designs or designations ("Brand Features") as well as any copyright or other proprietary notices appearing on or in the Product shall be maintained and shall not be removed, modified or altered by Participant.

13.6 LAND – License Term and Termination

The term of the license provided hereunder commences upon shipment of the Appliance to Participant. EOHHS may terminate the length of the license in whole or in part, (i) if the Participant materially breaches this section of the policies and procedures and does not cure such material breach within thirty (30) calendar days after receipt of written notice of such

breach; (ii) immediately following the failure to resolve the suspension of business, insolvency, institution of bankruptcy, liquidation proceedings by or against the Participant, appointment of a trustee or receiver for Participant's property or business, or any assignment, reorganization or arrangement by Participant for the benefit of its creditors; (iii) immediately, in the event that the LAND Contractor determines that the Product may be infringing and that no commercially reasonable alternative product is available or, (iv) immediately if Participant is in (a) breach of the ownership, restricted use or confidential information sections herein or (b) the Participation Agreement is terminated. Upon expiration or termination of the Participation Agreement is, all licenses, and any other rights and services provided to Participant as set forth in this Agreement, shall cease immediately and Participant shall immediately return the Product, at Participant's sole cost, to the Mass HIway as directed by the Mass HIway.

13.7 LAND – Confidential Information

Participant acknowledges that the source and object code of the Software remains a confidential trade secret of LAND Contractor and/or its licensors and that Participant is not entitled to review either the object code or the source code of the Software for any reason at any time. Participant shall not disclose or cause to be disclosed any Confidential Information of the LAND Contractor.