MHIN DIRECT HISP PRACTICES STATEMENT

Version 1.0
Effective Date: 6/28/2018

MICHIANA HEALTH INFORMATION NETWORK
220 W. Colfax Ave. Suite 300 South Bend, IN 46601

Table of Contents

1 Introduction

1.1 Overview

This MHIN HISP Policy (HP) describes the unified policy under which a the MHIN Health Information Services Provider (HISP) operates. The purpose of this policy is to define best practices and minimum administrative and technical requirements for HISP operation. Goals associated with the publication of this HP include maintenance of security and trust within the Direct community, and to facilitate interoperability with DirectTrust Accredited Trust Anchor Bundle members. This policy aims to ensure compliance to EHNAC DTAAP requirement and will assist in the accreditation and audit process. This HP will be updated to conform to technical advances, regulatory changes, or other relevant changes in the field.

This MHIN HP follows the general structure of the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure (PKI) Certificate Policy and Certification Practices Framework (RFC 3647). When required this policy may include additional technical requirements to address additional unique aspects of HISP operations and Direct messaging for the c transport of health information over the Internet.

The Direct Project is an initiative sponsored by the Office of the National Coordinator (ONC) for Health Information Technology to allow participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet. The Direct Project is based on S/MIME message signatures and message encryption for the purposes of achieving privacy, authentication, and message integrity.

In keeping with the IETF RFC 3647 framework, the MHIN HP is divided into nine parts that cover the security controls and practices and procedures for HISP-related Direct messaging services. To maintain the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation." Additional elements have also been added to reflect the unique aspects related to technical and operational aspects of HISPs.

1.1.1 Relationship between the MHIN HISP Practices Statement and the DirectTrust HP

In accordance with the DirectTrust HP, MHIN is publishing this HISP Practices Statement (HPS) to describe how it meets the requirements of the DirectTrust HP.

1.1.2 Relationship between the MHIN HISP Practices Statement and DirectTrust CP

The DirectTrust Certificate Policy (CP) describes policies relating to issuance and management of X.509 certificates for use in Direct messaging applications. The DirectTrust CP is maintained by the DirectTrust Certificate Policies and Practices Workgroup. The DirectTrust Board of Directors is responsible for managing the CP versioning lifecycle and for determining which versions of the DirectTrust CP are currently active, referred to in this document as the "Active Versions". The MHIN HISP conforms to the requirements of at least one of the Active Versions of the CP. If there is a conflict between the policies of the DirectTrust CP and this HISP Policy, the requirements of the DirectTrust CP will apply. All references to "the DirectTrust CP" in this document shall mean any of the Active Versions of the CP. Practice Note: As of 5/18/16, the Active Versions of the DirectTrust CP were version 1.1, 1.2 and 1.2.1. The most current list of Active Versions may be requested from DirectTrust.

1.1.3 Relationship between the MHIN HISP Practices Statement and the DirectTrust Accreditation program in partnership with EHNAC

DirectTrust operates an Accreditation program in partnership with the Electronic Healthcare Network Accreditation Commission (EHNAC) to certify the operations and policies of HISPs to the standards developed and maintained by DirectTrust. MHIN uses this HPS as a guide to conformance to the DirectTrust HP and to achieve accreditation with EHNAC. This HPS does not serve as a substitute to accreditation. This HP is intended to be fully consistent with the requirements of the Direct Trusted Agent Accreditation Program (DTAAP), an Accreditation program established by DirectTrust in partnership with EHNAC.

1.2 Document Name and Identification

This document is the MHIN HISP Practices Statement and was approved for publication on May 2018 by the MHIN Management Team. Future revisions will be tracked within this document. This MHIN HPS is assigned a unique object identifier (OID). The applicable MHIN OID pertaining to this HPS is 2.16.840.1.113883.3.1805.5.1.1 under the MHIN Root OID (2.16.840.1.113883.3.1805).

1.3 PKI Participants

PKI Participants are those entities involved in the registration, issuance, use of, or reliance upon MHIN HISP Certificates. The following are roles relevant to the administration and operation of the PKI within which the MHIN HISP operates to provide Direct messaging services.

1.3.1 Certification Authorities

A Certification Authority (CA) is an entity that issues Public Key X.509 Certificates and, through such issuance, attests to the binding between an identity and cryptographic Key Pair to a Subscriber. The MHIN HISP has a contract with DigiCert to act as CA. DigiCert is EHNAC DTAAP-CA accredited. CAs accredited

through EHNAC for DirectTrust issuance operate under a Certification Practices Statement (CPS) that is reviewed as part of the accreditation process to ensure conformance to the policies of this HPS.

1.3.2 Registration Authorities (RAs)

Registration Authorities (RA) are organizations responsible for collecting and proofing a Subscriber's identity and any other information provided by Subscriber for inclusion in a Certificate. The MHIN HISP has a contract with DigiCert to act as RA. DigiCert is EHNAC DTAAP-RA accredited. RAs accredited through EHNAC for DirectTrust issuance operate under a Certification Practices Statement (CPS) that is reviewed as part of the accreditation process to ensure conformance to the policies of this HPS.

1.3.2.1. Trusted Agents

Trusted Agents are individuals who act on behalf of the CA or RA to collect and/or verify information regarding Subscribers, and where applicable to provide support regarding those activities to the Subscribers. MHIN has assigned Trusted Agents who collect documentation to verify identity of subscribers and provide identity information to DigiCert as part of the contractual relationship with DigiCert who serves as the RA and CA. All activities of the MHIN Trusted Agent SHALL be performed in accordance with the DigiCert CP.

1.3.3 Subscribers

A Subscriber is a Professional Organization identified in a certificate, such as when domain-bound or address-bound certificates are issued to an organization.

1.3.4 End Users

All End Users are Subscribers of Direct X.509 Certificates, as defined in the DirectTrust Certificate Policy. Examples of End Users in the MHIN HISP include healthcare professionals and their staff members. End Users are not always the party identified in a certificate, but are affiliated employees of the Professional Organization identified in the certificate.

1.3.4.1 Health Information Service Providers (HISPs)

MHIN is the Health Information Service Provider (HISP) that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital certificate for all MHIN Direct Subscribers. Acting in the capacity of an agent for the Subscriber, MHIN holds and manages PKI private keys associated with a Direct digital certificate on behalf of the Subscriber.

1.3.4.1.1 HISP Boundary Considerations

MHIN as an organization performs many functions and services to its customer base. Among those are the HISP functions and services. This document defines those functions that are performed within the confines of the HISP boundary and those parts of the organization's functions and services that are subject to the requirements of this HPS.

A HISP is responsible for the functions that are ALWAYS inside the HISP boundary. MHIN performs all functions of the HISP as listed below.

a. Perform Security/Trust Agent (STA) functions (decrypt inbound messages, validate counterparty signature including message digest, ensure outbound messages are properly

signed, encrypt outbound messages, send/receive MDNs and confirm receipt of message) [section 6.9.4]

b. Perform trust management functions such as maintaining trust anchor store and trust policy enablement [section 6.9.3]

c. Perform Certificate discovery functions [section 6.9.4]

d. Provide S/MIME inbound and outbound interfaces [section 6.9.4] to receive messages sent to End User Direct Addresses and transmit messages sent from End User Direct Addresses.

e. Provide HISP-side of edge protocol connection including webmail or EHR integration interfaces, or internal API or data sharing repository for unified software with integrated HISP [section 6.7.1]

f. Maintain End User encryption private key store [section 6.2]

g. Perform End User authentication (but can be tiered on authentication by EHR technology or dependent application) [section 6.7.2]

h. Maintain integrity of security and trust framework, includes review of security logs, etc.

i. Maintain privacy of electronic Protected Health Information (ePHI) [section 6.7.1, 6.9.2]

j. Perform HISP Information Systems Security Officer (ISSO) functions [section 6.2]

k. Maintain End User signing private key store, and/or provide interface for Hardware-based signing keys held by End Users

l. Provision Direct Addresses

m. Generate End User private keys [section 6.1.1.2]

n. Operate SMTP inbound or outbound server

o. Operate DNS and/or LDAP servers hosting End User certificates for discovery

p. Maintain End User message queues and/or mailboxes

q. Provide Tools or interfaces to create a message and include attachments

r. Provide End User technical support

x. Operate Provider Directory

Functions OUTSIDE the HISP boundary: (These functions are not performed by HISPs and are outside the scope of this document.)

a. Store and/or analyze EHR/PHR data
b. Perform other EHR functions including Care Coordination
c. Utilize Clinical Data Repository for HIE services
d. Provide CDA processing, validation and discovery via XCA Cross Community Exchange
e. Use of Direct credentials for other purposes results delivery and hospital admission alerts
f. Administer vendor hosted Population Health Platform
g. Health IT Consulting

1.3.5 Relying Party

A Relying Party uses an End User's X.509 certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the End User. The Relying Party is responsible for checking the validity of the Certificate by checking the appropriate Certificate status information defined in § 2.2.1.

1.3.6 Intermediate System

An Intermediate System is a healthcare application or other system that communicates with a HISP on behalf of End Users. The MHIN HISP communicates with Intermediate Systems such as Electronic Health Records and Patient Portal to provide HISP services via XDR integration. The Intermediate Systems lie outside the boundary of the MHIN HISP. The MHIN HISP does not provide user accounts to individual consumers of healthcare.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The appropriate use of X.509 certificates in the MHIN HISP that have been issued by the CA are for the exchange of electronic messages in compliance with the specifications of the Direct Project. This includes S/MIME message signature verification and S/MIME message encryption. A conforming HISP MUST use Certificates issued under the DirectTrust CP only for purposes permitted by the DirectTrust CP.

1.4.2 Prohibited Certificate Uses

The MHIN does not use certificates and private keys for any use prohibited by the DirectTrust CP

1.5 Policy Administration

1.5.1 Organization Administering the Document

MHIN through its management team and HISP workgroup is responsible for the management, approval and implementation of this document.

MHIN
220 W. Colfax Ave.
Suite 300
South Bend, IN 46601

1.5.2 Contact Person

Kelly Hahaj, CEO

1.5.3 Person Determining HISP Practices Statement Suitability for the Policy

The MHIN HISP Practices Statement (HPS) states how the HISP implements policies required by the DirectTrust HISP Policy. The MHIN HISP submits this HPS during the EHNAC Accreditation process to determine the suitability of the HPS.

1.5.4 HISP Practices Statement Approval Procedures

The MHIN HPS can be updated as needed at any time, but at a minimum, it will be reviewed annually by the MHIN management team and the HISP workgroup. This HPS will be submitted for compliance analysis and audit during the DirectTrust accreditation process.

All versions and updates shall be linked to the Direct section of the MHIN web site http://www.mhin.org.

1.6 Definitions and Acronyms

Term	Definition
Accreditation	Accreditation of a HISP through the program operated by DirectTrust in partnership with EHNAC. This may be in partnership with another accrediting entity.
Applicability Statement	The Applicability Statement for Secure Health Transport, Version 1.2, Dated August 3, 2015, or any subsequent version, published by the Direct Project.
Associate	An individual employed by Michiana Health Information Network (MHIN)
Business Associate or BA	An entity meeting the definition of a business associate under HIPAA at 45
MHIN Direct	MHIN owned and operated HISP which provides the management of security and transport as it relates to information exchange using Direct Project standards.
MHIN Direct Administrator	The Professional person who is tasked with responsibility for distribution and use of MHIN Direct capabilities within their respective organization.
MHIN HIE	A health information exchange in Northern Indiana and Southwest Michigan that uses innovative technology to bring information and insights in unprecedented forms to the healthcare community to better serve patients and clients and improve the health of the entire community.
MHIN HISP Workgroup	A group of MHIN associates including the IT Director, HISP Administrator, Project Manager, Security Officer, Privacy Officer tasked with (1) management and oversight of the HISP practices and procedures used in MHIN Direct communications, and (2) the review and approval of this HPS and updates thereto.
MHIN Management Team	The team that oversees the operation of the MHIN HIE

Certificate	A digital representation of information which (1) identifies the Certification Authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it. Unless otherwise qualified, the term "Certificate" refers to Certificates issued to a Subscriber.
Certificate Class	A classification of Certificates by type as defined in § 3.2.3.1.
Certification Authority or CA	An authority trusted by one or more users to create and assign Certificates.
Certificate Policy or CP	A specialized form of administrative policy for electronic transactions performed during Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of Certificates. The DirectTrust Ecosystem Community X.509 Certificate Policy is the governing policy on which this CPS is based in accordance with § 1.
Direct Trust Certification Policy or CP	This DirectTrust Community X.509 Certificate Policy (DirectTrust CP) describes the unified policy under which a conforming Certification Authority operates. Specifically, this document defines the creation and life-cycle management of X.509 version 3 Public Key Certificates for use in applications supporting Direct Project message exchange.
Certificate Revocation List or CRL	A list of Certificates that are revoked prior to their stated expiration date that is maintained by the CA that issued them.
Certificate Signing [illegible]	A communication sent from an applicant requesting a digital signature.
Citizen	An individual participating in their own health care.
Compromise	The unauthorized disclosure of, loss of, loss of control over, or use of a Private Key associated with the Certificate or a reasonable suspicion thereof.
Covered Entity	An entity meeting the definition of a covered entity under HIPAA at 45 CFR 160.103.
Direct Message	An electronic mail message digitally signed and encrypted according to the requirements of the Applicability Statement.
Direct Project	An initiative from the Office of the National Coordinator (ONC) for Health Information technology that created a set of standards and services that, with DirectTrust HISP Policy, Version 1.1.1apolicy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
Direct Trusted Agent Accreditation Program or DTAAP	An Accreditation program that validates the technical, security, trust, and business practice conformance of Trust Agents involved in the Direct Project.
DirectTrust Certificate Policy of CP	Any one of the current Active Versions of the DirectTrust Certificate Policy, as further defined in Section 1.1.2.
Distinguished Name or DN	A name given to an individual or organization which uniquely identifies it in the respective system.
Domain Name System or DNS	The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network.

Electronic Healthcare Network Accreditation Commission or EHNAC	An independent, federally recognized, standards development organization and accrediting body designed to improve transactional quality, operational efficiency and data security in healthcare.
End User	An end entity that uses a HISP's Direct Services. An End User may act in the role of sender or recipient of a Direct message.
Health Information Service Provider or HISP	An entity that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital certificate. Acting in the capacity of an agent for the Subscriber, the HISP may hold and manage PKI private keys associated with a Direct digital certificate on behalf of the Subscriber. For purposes of this HPS, the HISP is MHIN.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, as amended.
DirectTrust HISP Policy	The document, written by DirectTrust, to define the requirements to be a "conforming HISP".
HISP Practices Statement or HPS	A document written by a HISP to demonstrate how the HISP meets the requirements of this DirectTrust HISP Policy, including both technical and organizational.
Identity or ID	Information used to establish or prove a person's individuality.
Information Systems Security Officer or ISSO	An individual responsible for establishing and maintaining the enterprise vision, strategy and program as it relates to information systems security, to ensure information assets are adequately protected.
Intermediate System	An Intermediate System communicates with a HISP or another Intermediate System to send and/or receive Direct messages on behalf of End Users using an edge protocol supported by both systems.
Internet Engineering Task Force or IETF	A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
International Organization for Standardization or ISO	ISO is an organization that develops and publishes International Standards.
Object Identifier or OID	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.
Online Certificate Status Protocol or OCSP	An internet protocol used for obtaining Certificate Revocation Lists.
Protect Health Information or PHI	PHI under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Professional	An individual who acts on behalf of an organization which is a covered entity or business associate under HIPAA, or is a healthcare related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a Certificate.
Public Key Infrastructure or PKI	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke Public Key Certificates.
Registration Authority or RA	Entity responsible for identification and authentication of Certificate subjects, but that does not sign or issue certificates (i.e. a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Relying Party	An individual or entity who has received information that includes a Certificate and a digital signature verifiable with reference to a Public Key listed in the Certificate, and is in a position to rely on them. Responsibilities of the Relying Party are outlined in http://wiki.directproject.org/Best+Practices+for+HISP- HISP+Agreements.
Repository	The Certificate storage mechanism.
Relying Party HISP	The HISP used by a Relying Party. This may be a different HISP than the HISP used by the End User.
Secure Multipurpose Internet Mail Extensions or S/MIME	A standard for public key encryption and digital signing of email messages.
Subscriber or MHIN Direct Subscriber	An individual or organization that (1) is the subject named or identified in a Certificate issued to that individual or organization, (2) uses the Private Key corresponding to the Public Key listed in the Certificate for purposes of Direct Project message encryption, and (3) does not itself issue Certificates to another party.
Subscriber Applicant	An individual that requests MHIN Direct enabled communication on behalf of their organization.
Subscriber Agreements	Documents which set forth legal responsibilities and expectations concerning use of MHIN Direct.
Trust Anchor Certificate	A Certificate identifying a trusted issuer of Certificates.
Trust Anchor Store	A collection of Trust Anchors.
Trusted Agent	An organization authorized to act as a representative of a Subscriber in confirming the Subscriber Applicant identification during the registration process.
Trust Bundle	A collection of trust anchors that comply with a common set of policies and represent trust communities.
Workforce	Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether or not they are paid by the entity.

2 Publication and Repository Responsibilities

2.1 Repositories

The MHIN HISP utilizes MirthMail as its HISP Software platform which functions as a repository for all certificates generated by Digicert who provides CA and RA services for the MHIN HISP. The Public and Private keys are stored within the MirthMail software.

MHIN implements strict authorization and access controls where the Subscriber Agreements are stored. The network drive where the Subscriber Agreements are located can only be accessed by key individuals at MHIN.

2.1.1 Repository Obligations

The Repository operated by the MHIN HISP mentioned in § 2.1 is located on redundant/highly available servers, operated 24 hours a day, 7 days a week with a minimum of 99% availability overall per year.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate status

The MHIN HISP supports discovery of Subscriber Public Keys through DNS. Using the Standards Implementation and Testing Environment, Direct Certificate discovery tool, the MHIN HISP is able to demonstrate that the Certificate and the Public Key within the certificate are discoverable through DNS.

2.2.2 Publication of CA Information

No stipulation.

2.2.3 Interoperability

To promote interoperability, certificates managed by the MHIN HISP meet the requirements of the DirectTrust Certificate Policy.

2.3 Time or frequency of publication

This HPS is updated and published in accordance with § 1.5.4. Subscriber Agreements are posted to an internal document repository, and accessible only by those within the Trusted Roles defined in § 5.2.1.

2.4 Access controls on repositories

The MHIN HISP protects repository information not intended for public dissemination or modification. The MHIN HISP provides unrestricted read access to its repositories and has implemented logical and physical controls to prevent unauthorized write access to such repositories.

3 Identification and Authentication

This section pertains only to naming rules and identity validation for initial certificate issuance, and

identification and authentication for re-key and revocation requests for existing certificates. Subsequent identification and authentication of End Users and Intermediate Systems in order to use existing keys for signing or decryption of Direct messages are discussed in Sections 6.7.2 and 6.7.3 of this document.

3.1 Naming

3.1.1 Types of Names

As specified in the Direct Project Applicability Statement for Secure Health Transport, Domain-Bound Certificates contain a Health Domain Name in the form of a dNSName in the subjectCommonName and subjectAlternativeName extensions of the Certificate. Table 1 contains the CA Certificate DN attributes for the MHIN HISP.

Table 1: x.501 Distinguished Name Attributes in MHIN Direct CA Certificates

Attribute	Value
Country (C) =	US
Organization (O) =	Michiana Health Information Network
Organizational Unit (OU) =	www.mhin.com
State or Province (S) =	Indiana
Locality (L) =	South Bend
Common Name (CN) =	MHIN Direct CA

Table 2 contains a listing of the Certificate DN attributes. The attributes have been authenticated according to § 3.2.

Table 2: x.501 Distinguished Name Attributes in MHIN Certificates

Attribute	Value
Country (C) =	US
Organization (O) =	Subscriber Organization Name on file.
Organizational Unit (OU) =	Not used.
State or Province (S) =	Subscriber Organization State.
Locality (L) =	Subscriber Organization Locality.
Common Name (CN) =	Subscriber Organization Direct Email Domain Name (Professional Organization Class Certificate Use Only)
E-Mail Address (E) =	Email of the IT Director and Security Officer

3.1.2 Need for names to be meaningful

The Subscriber Organization Name used in the Organization attribute of the DN is the business name as verified in § 3.2.2.

3.1.3 Anonymity or Pseudonymity of Subscribers

The MHIN HISP utilizes DigiCert as its CA. DigiCert issuance of certificates complies with the DirectTrust Certificate Policy in regard to Anonymity and Pseudonymity of Subscribers.

3.1.4 Rules for interpreting various name forms

No Stipulation.

3.1.5 Uniqueness of Names

The MHIN HISP CA, Digicert enforces name uniqueness of the Certificate subject DN within the CA's X.500 namespace, as documented in the DigiCert Certificate Policy, in accordance with the DirectTrust Certificate Policy.

3.1.6 Recognition, Authentication and Role of Trademarks

MHIN HISP Subscribers SHALL NOT request Certificates with any content that infringes the intellectual property rights of another entity. DigiCert the issuer CAs MAY reject any application or require revocation of any Certificate that is part of a trademark dispute in accordance with the DirectTrust Certificate Policy.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Private Key is generated by the MHIN HISP. The MHIN HISP sends the Private Key to the Issuer CA. According to the DigiCert Certificate Policy, DigiCert establishes that the Applicant holds or controls the Private Key corresponding to the Public Key by performing signature verification or decryption on data purported to have been digitally signed or encrypted with the Private Key by using the Public Key associated with the certificate request.

3.2.2 Authentication of Organization Identity

Requests for Certificates that assert organization affiliation MUST include the organization name, mailing address, and documentation of the legal existence of the organization as well as the requested Health Domain Name or Health Endpoint Name that will appear in the Certificate (see section 3.1.1 for details).

The MHIN HISP requires the requesting organization to complete the Declaration of Identity Form in conformance with the DigiCert Certification Practices Statement. The DigiCert CPS section 3.2.2 describes the process that is followed to validate the organization the affiliation of the representative.

3.2.3 Authentication of Individual Identity

The MHIN HISP performs LOA3 identity verification in accordance with the DigiCert Certification Practices Statement (see section 3.2.3 of the DigiCert CPS).

MHIN utilizes DigiCert for CA and RA services. MHIN ISSOs who request and process certificates on behalf of the HISP are appointed by DigiCert. DigiCert authenticated three representatives from MHIN to act as ISSOs authenticated at a Medium Assurance Level (LOA3). For each organization registered in the Direct Cert Portal by a MHIN ISSO, the organization and an appointed representative are authenticated at a Medium Assurance Level (LOA3). In addition, MHIN ISSOs only order the DigiCert Organization Cert Medium certificate type for all organizations. DigiCert authenticates appointed organizational representatives using the Direct Representative Declaration form.

See also sections 3.2.5, 4.9.1 and 9.6.1.

3.2.3.1 Authentication of Human Subscribers

The MHIN HISP requests domain bound certificates for Professional Organizations. A Professional Organization Certificate Class is defined as a Professional seeking a Certificate on behalf of the organization they are representing. Identity of the Professional shall be established by in-person identity proofing before a MHIN Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities (e.g., notary public). A trust relationship between the Trusted Agent and the Subscriber Applicant which is based on an in- person antecedent may suffice as meeting the in- person identity proofing requirement. Credentials required are a state or federally issued picture identification. Credentials presented must be unexpired. Identity vetting process is performed in compliance with DirectTrust.org Level of Assurance (LoA) 3.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

Not Applicable

3.2.3.3 Authentication of Human Subscribers for Group Certificates

Not Applicable

3.2.4 Non-verified Subscriber information

All Subscriber information included in the Certificate is verified. A list of the Subscriber information specified in the Subject DN is outlined in § 3.1.1.

3.2.5 Validation of Authority

For Direct Organization Certificates the subscriber authorizes the MHIN HISP to order the

certificate and use the related private key on the Subscriber's behalf. The MHIN HISP ISSO is responsible for tracking access to and ensuring proper use of the private key.

3.2.6 Criteria for Interoperation

Certificates requested by the MHIN HISP are intended to facilitate interoperability pursuant to the Direct Project specifications for the purposes of Direct message exchange. The certificates issued by the CA DigiCert conform to the DirectTrust Ecosystem Community X.509 Certificate Policy.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

MHIN manages this process on behalf of the Subscriber as it relates to their use of the MHIN Direct HISP. MHIN defines re-key as generation of a new key pair to replace the expiring key pair. Re-keys are performed by the MHIN ISSO to minimize any interruption in service due to expiry.

3.3.2 Identification and Authentication for Re-Key after Revocation

If a Certificate is revoked, the Subscriber shall go through the initial identity verification process described in section 3.2 to obtain a new certificate.

3.4 Identification and Authentication for Revocation Request

The MHIN HISP ISSO reviews the revocation request. The MHIN HISP CA, DigiCert authenticates all revocation requests referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4 Certificate Life Cycle

4.1 Application

This section specifies requirements for the initial application for a DirectTrust Certificate.

4.1.1 Submission of Certificate Application

The MHIN Trusted Agent obtains information from the Subscriber for identity proofing. The MHIN ISSO creates the Certificate Signing Request (CSR) based on input received from the Subscriber as validated by the CA, DigiCert during the identity proofing process.

4.1.2 Enrollment Process and Responsibilities

A Subscriber is responsible for providing accurate information about himself/herself and his/her organization during identity proofing. The Issuer CA, DigiCert is responsible for ensuring that the identity of

each Applicant is proofed in accordance with the DirectTrust CP and the applicable DirectTrust CPS prior to the issuance of a Certificate. DigiCert authenticates and protects all communication made during the Certificate application process.

4.2 Certificate Application Processing

DigiCert serves as the Issuer CA and RA and is responsible for verifying that the information in a CSR is accurate and reflect the information presented by the Subscriber.

4.2.1 Performing Identification and Authentication Functions

The identity proofing of Subscribers is performed by DigiCert the Issuing CA and RA as specified in section 3.2 using procedures detailed in the DigiCert CPS.

4.2.2 Approval or Rejection of Certificate Applications

A Certificate application MAY be rejected by DigiCert the Issuing CA and RA due to missing or inaccurate information. DigiCert retains the right to reject Certificate applications if, in its judgment, the requesting individual or organization does not have a legitimate reason to possess a DirectTrust Certificate or has not provided sufficient information for issuance.

4.2.3 Time to Process Certificate Applications

DigiCert the issuing CA verifies Subscriber information placed in a Certificate in accordance with the DirectTrust CP Section 3.2.2 and issues a Certificate within 30 days of completion of verification.

4.3 Issuance

4.3.1 CA Actions During Certificate Issuance

In accordance with the DirectTrust CP, DigiCert confirms the source of a certificate request before issuance. DigiCert does not issue end entity certificates directly from its root certificates. After issuance is complete, DigiCert Stores the certificate in a database and sends the certificate to the MHIN HISP.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Digicert notifies the MHIN HISP via email when a Certificate has been issued for the Subscribing Organization, at which time the Subscriber Applicant shall become a Subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Certificates are considered accepted 30 days after the certificate's issuance, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

4.4.2 Publication of the Certificate by the CA

The MHIN HISP utilizes DigiCert as its CA. DigiCert publishes all CA certificates in its repository. DigiCert publishes end-entity certificates by delivering them to the MHIN HISP on behalf of the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The MHIN HISP protects Private Keys from unauthorized use or disclosure and discontinues using a Private Key after expiration or revocation of the associated certificate. The MHIN HISP uses Certificates in accordance with their intended purpose as specified by the *certificatePolicies* and *keyUsage* extensions of the Certificate.

The MHIN HISP does not deliver private keys to end user Subscribers.

The MHIN HISP delivers public keys to DigiCert, our Certificate Authority (CA) to request participant organization certificates. The MHIN HISP follows a formal process for key generation as documented in Phase 2 of the Direct Enrollment Process.

The MHIN HISP is a member of DirectTrust Accredited Trust Community. MHIN HISP trust anchor certificate is in the DirectTrust Accredited Trust Bundle. Other members of the Direct Trust Accredited Trust Community are able to download the MHIN HISP trust anchor certificate via the DirectTrust Accredited Trust Bundle. The MHIN HISP does not exchange trust anchor certificates with other Relying Parties that are not members of the DirectTrust Accredited Trust Community. This is documented in the Direct Trust Anchor Policy.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates conform to the policies provided by the Direct Trust Community X.509 Certificate Policy. The MHIN HISP publishes a certificate revocation list (CRL) and maintains an OCSP Responder as described in § 2.2.1. Relying Parties should process the CRL on a regular basis and reject Certificates found on the CRL or respect the Certificate status reflected in an OCSP response.

4.6 Certificate Renewal

Certificate renewal consists of issuing a new Certificate with a new validity period and serial number while retaining all other information in the original Certificate including the Public Key. After Certificate renewal, the old Certificate is not further re-keyed, renewed, or modified.

4.6.1 Circumstances for Certificate Renewal

The MHIN HISP renews a Certificate if the Public Key has not reached the end of its validity period, the associated Private Key has not been compromised, and the Subscriber name and attributes are unchanged.

4.6.2 Who May Request Renewal

On behalf of the Subscriber, the MHIN ISSO serves as an authorized representative to request certificate renewal with the RA/CA, DigiCert.

4.6.3 Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the certificate's original issuance. The MHIN HISP Issuer CA or RA, DigiCert approves or rejects Subscriber Certificate renewal requests, according to the DigiCert CPS § 4.6.3.

4.6.4 Notification of New Certificate Issuance to Subscriber

The MHIN HISP CA/RA DigiCert notifies the MHIN ISSO via email when the certificate is issued. The MHIN ISSO is authenticated with user id and password to the protected location and downloads the certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

No stipulation beyond conformance with the DirectTrust CP.

4.8 Modification

The MHIN HISP does not support Certificate modification, rather, relies on Certificate issuance and posting of Certificate information via the methods described in § 2.2.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

The MHIN HISP Certificate Revocation Policy defines the circumstances that would require the revocation and/or suspension of MHIN HISP domain certificates.

A Certificate SHALL be revoked when the binding between the subject and the subject's Public Key defined within a Certificate is no longer considered valid. Whenever any of the circumstances detailed below occur, the associated Certificate SHALL be revoked and placed on the Certificate Revocation List (CRL) and, when applicable, have its revoked status reflected in Online Certificate Status Protocol (OCSP) responses.

Examples of circumstances that invalidate the binding include:

- The identifying information or affiliation components of any names in the Certificate become invalid
- The Subscriber can be shown to have violated the stipulations of the Subscriber agreement
- The Private Key is suspected of compromise, and the Subscriber or RA requests Certificate revocation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of public Certificates is available via CRL and an OCSP responder.

4.10.2 Service Availability

No Stipulation

4.10.3 Optional Features

No Stipulation

4.11 End of Subscription

A Subscriber's subscription service ends if its certificate expires or is revoked.

4.12 Key Escrow and Recovery

No Stipulation

5 Facility Management and Operational Controls

MHIN's corporate office, located at: Colfax Place – 220 West Colfax Avenue, South Bend, Indiana.

MHIN occupies Suites 200 and 300 of Colfax Place. MHIN leases these suites from Holladay Properties. Administrative and technical functions are conducted at MHIN's corporate offices. Within the corporate office suites at MHIN, the network room houses computing equipment for administrative functions. No PHI is stored on servers physically located at the corporate office.

MHIN's primary data center is located at The Medical Foundation (TMF) in South Bend, Indiana. The primary data center is leased from TMF. That organization has principal responsibility for safeguarding the data center on its premises and has well established security measures in place. MHIN's Technical Director collaborates with TMF to ensure appropriate defenses are in place within the leased data center

5.1 Physical controls

5.1.1 Site Location and Construction

As required by our Facility Security and Maintenance Policy, strong facility access controls are in place at MHIN Corporate Office and MHIN's data centers. The entrance to each remains locked at all times, limiting access only via key card. Access logs at each location are maintained and routinely reviewed.

5.1.2 Physical Access

As required by our attached Facility Security and Maintenance Policy, strong facility access controls are in place at MHIN's data centers at The Medical Foundation (TMF) and Union Station. The entrance to each data center remains locked at all times, limiting access only via key card. The Medical Foundation maintains the TMF Data Center Badge Access Log that shows entries.
Authorized personnel undergo extensive background checks and drug testing prior to being issued a key card. Similar processes are in place at the Union Station Data Center for authorizing access to MHIN personnel. Data Center personnel monitor the entrances to each data center. At all times, each data center restricts access to authorized personnel or visitors who sign in and require that visitors be accompanied by authorized personnel.

5.1.3 Power and Air Conditioning

The Medical Foundation's (TMF) Data Center is a secure Class 4 Data Center, which includes; triple power grids (UPS & APS sources), dual UPS power sources each with its own backup generator, uninterrupted transfer of power with UPS and Automatic Transfer Switching, both 120 and 208, single and three phase circuits, systems and cabinets with N+1 power, Backup on-site generators, redundant climate control technology, 24/7 temp and humidity monitoring and recording by operations staff and electronically with out-of-range warning alerts to operations staff, network manager and supervisor, redundant N+1 hvac cooling controlled to approx. 70˚ and humidity levels approx. 45%

Union Station DataCenter is a 100,000+ Square Feet facility classified as a Tier 3 high availability data center with access to 50+ carriers with scalable connectivity. It has clean and redundant power/power grids with data center cooling and controlled humidity.

Netarx/Union Station DataCenter
Overview of Facility Security Environment
Physical and Environmental

- Tier3 High Availability
- Access to 50+ Carriers
- 100,000+ Square Feet
- Scalable Connectivity
- Clean and Redundant Power/Power Grids
- Data Center Cooling and Controlled Humidity
- FM200 Fire Protection
- Physical Access Control/Monitoring
- Video Surveillance

Netarx Data Center Employee Security Checks

- Professional Background Checks
- Security Clearance
- Criminal History Report
- Credit Report
- Driving Record
- Education Verification
- Employment/Salary Verification
- Reference Checks

5.1.4 Water Exposures

The MHIN HISP equipment is installed on the second floor at The Medical Foundation Data Center to prevent exposure to water other than water from fire prevention and protections systems.

5.1.5 Fire Prevention and Protection

The Medical Foundation's (TMF) Data Center and Union Station haveFM-200 Fire Suppression, fire detection and gas suppression system with fail safe alarm, and 24 x 7 x 365 manned monitoring. The local city fire departments inspect the fire system annually, as does a contracted third party supplier. All fire systems are connected to emergency backup power sources.

5.1.6 Media Storage

The MHIN HISP Data Backup Plan documents that media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). The Mirth Mail Appliance Backup Topology demonstrates that media containing audit, archive, or backup information is duplicated and stored in a location separate from the HISP equipment and is be protected from unauthorized access.

The Hardware and Electronic Media Management Policy has been implemented for managing receipt and removal of hardware and electronic media that contains electronic Protected Health Information (ePHI). MHIN is very careful to ensure that when any hardware is moved, the data is secured, backed up and retrievable. In addition, MHIN does not re-use hardware or media that contains ePHI; instead, MHIN disposes of any sensitive information from hardware and/or media according to clearly defined procedures that meet national standards.

5.1.7 Waste Disposal

MHIN does not reuse or release any hardware or electronic media containing electronic Protected Health Information (ePHI). All hardware or electronic media is destroyed according to MHIN's Hardware and Electronic Media Management Policy. MHIN uses Integra to dispose of hardware and electronic media.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the HISP is weakened. The functions performed in these roles form the basis of trust for all uses of the HISP. Two approaches should be taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. The requirements of this policy are defined in terms of five roles:

1. Administrator

2. Information Systems Security Officer (ISSO)

3. Operator

Additional roles required by HIPAA:

4. HIPAA Security Officer

5. HIPAA Privacy Officer

MHIN has formally identified a Privacy Officer and a Security Officer. They serve as each other's backups. The MHIN organizational chart notes the backup roles. In addition, the Compliance Coordinator supports the activities of the Privacy and Security Officers. All three individuals are also key members of the Security Incidence Response Team. These responsibilities are documented, including a description of their responsibilities, and communicated internally.

MHIN's new employee orientation includes a privacy and security in-service where the employee receives education on Privacy and Security roles and responsibilities. Privacy and/or Security items are standing agenda items in all staff meetings.

5.2.1.1 Administrator

The Administrator role is responsible for installing, configuring, and maintaining the HISP software. The Administrator establishes, maintains and configures HISP user accounts.

5.2.1.2 Information Systems Security Officer

The Information Systems Security Officer (ISSO) is responsible for generating, managing, installing and backing up End User private keys. The ISSO configures End User profiles or templates and manages End User access to private keys stored by HISP. The ISSO also manages HISP-wide trust decisions, e.g. addition or deletion of trust anchors, trust bundles, or policy enforcement rules, if applicable.

5.2.1.3 Operator

The operator role is responsible for the routine operation of the HISP equipment and operations such as system backups and recovery or changing recording media.

5.2.1.4 HIPAA Security Officer

The MHIN resource who holds the title of Information Systems Security Officer is authorized to make changes about the system security policy.

5.2.1.5 HIPAA Privacy Officer

The MHIN resource who holds the title of Privacy Officer is authorized to be a point of contact for reporting and assisting in the investigation of any data breach that might take place.

5.2.2 Number of Persons Required Per Task

At least two people are trained for each task but only one is required to execute each task.

5.2.3 Identification and Authentication for Each Role

MHIN provides a unique identity for each Associate performing a role on the HISP system, which is used to authenticate that the Associate is authorized to perform HISP system activities for their respective role.

5.2.4 Separation of Roles

No stipulation.

5.2.5 Access to Electronic PHI

The MHIN HISP has a User List Management policy on maintaining a list of all individuals, contractors, and Business Associates with access to Electronic PHI (ePHI). The purpose of this policy is to describe the standards for managing the list of users with access to electronic ePHI in compliance with applicable requirements of the HIPAA Privacy and Security Rules.

5.2.6 Policies and Procedures

MHIN records and maintains the policies and procedures implemented to comply with HIPAA, HITECH and other related privacy and security laws and regulations. A digital version is available for all employees to access on-demand in a shared network drive. A hard copy is also made available at a central location. MHIN routinely reviews and updates these policies as new regulations are introduced or if there are operational changes affecting the security of the Electronic PHI. At a minimum, all policies are reviewed annually.

5.2.7 Hybrid Entities

The MHIN HISP is not part of a Hybrid Entity.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

MHIN has a team of dedicated and highly skilled personnel responsible for all aspects of MHIN's operation and administration, thus ensuring that MHIN's mission is realized. MHIN's workforce has extensive experience with healthcare and information technology, with a strong commitment to customer service and patient confidentiality for streamlined electronic access to clinical information through all of MHIN's clinical applications. The qualifications of each key individual in a leadership position are detailed in the Summary of Key Personnel document. The number of personnel and respective titles are detailed in the MHIN Organizational Chart along with the key functions of each department.

5.3.2 Background Check Procedures

The MHIN Workforce Clearance and Security Policy describes the steps taken to accomplish appropriate workforce clearance for every workforce member.

- Check employment references listed on the applicant's resume to verify work history and determine desirability for employment at MHIN.
- Confirm the applicant is not restricted from working with PHI by the United States Office of the Inspector General (OIG), by entering the applicant information into the OIG Exclusion List at http://exclusions.oig.hhs.gov/.
- Collect identity verification documents in accordance with the I9 form requirements.

5.3.3 Training Requirements

MHIN takes responsibility to ensure that employees receive thorough, relevant and accurate training. All MHIN employees receive formal training on a wide range of topics when joining the organization. New Employee Orientation includes thorough training for new employees. MHIN also utilizes an Orientation Checklist to ensure that all avenues of training have been covered.

MHIN conducts annual HIPAA/HITECH educational programs that all employees are required to attend. This material is also covered with all new employees upon hire. MHIN contracts with HIPAA Secure Now! to provide formal HIPAA Privacy and Security online training. Even though the training is conducted online, training sessions are conducted as a group. During these sessions, the Privacy Officer details how the training specifically applies to MHIN. Upon completion of the training, each employee is required to take an exam which tests their knowledge on the material discussed.

MHIN ensures that personnel are trained on new software tools and applications used by MHIN clients. In addition, MHIN develops various job aids for specific tasks associated with MHIN systems, especially when new processes are defined.

MHIN employees participate in personal development plans to enhance job skills. Individual employee goals are established and reviewed during MHIN's formal annual employee performance review process.

5.3.4 Retraining Frequency and Requirements

The MHIN Privacy and Security Awareness and Training Policy ensures that all workforce members have been trained in, and fully understand MHIN's privacy and security policies. In addition, all workforce members will be coached on methods for integration of privacy and security practices into their daily activities

5.3.5 Job Rotation Frequency and Sequence

No Stipulation

5.3.6 Sanctions for Unauthorized Actions

The MHIN Sanction Policy for Workforce and Client Users ensures that all members of its workforce and client users comply with the privacy and security policies of the organization as well as state and federal regulations.

5.3.7 Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated in the MHIN Sanction Policy for Workforce and Client Users.

5.3.7.1 Business Associates of HISP

The MHIN HISP does not utilize the services of a third party to create, receive, maintain, or transmit PHI on behalf of the HISP or its end users.

5.3.7.2 Cloud Service Providers as Business Associates of HISP

The MHIN HISP does not utilize the services of cloud service providers.

5.3.8 Documentation Supplied to Personnel

MHIN ensures that all personnel are trained on all new software tools and applications that are used by MHIN Clients. MHIN develops various job aids for specific tasks associated with MHIN systems, especially when new processes are defined.

5.4 Audit Logging Procedures

In accordance with the MHIN Information Systems Activity Review and Audit Controls Policy, the MHIN HISP generates audit log files for all events occurring within the HISP boundary that relate to the security of the HISP. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 Types of Events Recorded

At a minimum, event auditing capabilities will be enabled on all systems that process, transmit, and/or store sensitive information. Types of events to be audited may include, and are not limited to, logins, logouts, and file accesses, deletions and modifications. MHIN ensures the protection of all audit reports and log files and evaluates the software and application tools used to review audit reports.

Audits are conducted to:

- Ensure confidentiality, integrity, and availability of sensitive information.
- Investigate possible security incidents and ensure conformance to security policies.
- Monitor user or system activity where appropriate.

Applicable audit events that are logged include but are not limited to the following:

SECURITY AUDIT

- Any changes to the audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the audit logs

AUTHENTICATION TO HISP STA SYSTEMS

Information that will be maintained in audit logs and access reports must include as much of the following data elements, whenever reasonable, appropriate and technically feasible:

- User identity
- Dates and times of log-on and log-off
- Successful and rejected system access attempts

HISP CONFIGURATION

- Any security-relevant changes to the configuration of a HISP system component

ACCOUNT ADMINISTRATION

- Roles and users are added or deleted
- The access control privileges of a user account or a role are modified

TRUST MANAGEMENT PROFILES

- All changes to End User trust management profile, including policy enforcement rules, enabling or disabling trust anchors or trust bundles.

CONFIGURATION CHANGES

- Hardware
- Software
- Operating System
- Software Version Update

PHYSICAL ACCESS / SITE SECURITY

- Known or suspected violations of physical security
- Anomolies
- System crashes and hardware failures
- Software error conditions
- Software check integrity failures
- Network attacks (suspected or confirmed)

- Equipment failure
- Violations of the HP or HPS

5.4.2 Frequency of Processing Log

Audit logs are reviewed and monitored regularly to ensure that any irregularities are identified and handled properly.

5.4.3 Retention Period for Audit Logs

Audit logs are maintained in conformance with applicable law or regulation.

5.4.4 Protection of Audit Logs

The MHIN HISP is configured to ensure that the audit logs are not modified. Safeguards are deployed to protect against unauthorized changes and operational problems such as editing of logs, alterations to message types, and deactivation of logging capabilities.

5.4.5 Audit Log Backup Procedures

The MHIN HISP is locally hosted on a MHIN server that utilizes VEEAM backup and replication. The VMWare cluster which includes the MirthMail server is connected via the MHIN Network to the VEEAM server for nightly backups which is then stored at an off-site location.

5.4.6 Audit Collection System (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level at all times while the HISP is in operation. Should it become apparent that an automated security audit system has failed, MHIN will cease all HISP operations until the security audit capability can be restored.

5.4.7 Notification to Event-Causing Subject

The subject is not notified of the audit event.

5.4.8 Vulnerability Assessments

The MHIN HISP utilizes an independent third party to conduct an accurate and thorough annual assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the HISP. The MHIN HISP's technology team conducts, on a quarterly basis, threat and vulnerability assessments and has an improvement process based on the results of those assessments. The Privacy and Security Team routinely reviews the Security Management Plan and updates it with any new threats and/or vulnerabilities.

5.5 Records Archival

5.5.1 Types of Events Archived

The MHIN HISP maintains a written and/or electronic record of any action, activity, or assessment that may be required by applicable Federal and State regulations included but not limited to the following.

- Accreditation of the HISP
- HPS versions
- Contractual obligations and other agreements concerning the operation of the HISP, notably
- BAAs
- System and equipment configurations, modifications, and updates
- Certificate signing and revocation requests
- Any documentation related to the receipt or acceptance of a certificate or token
- End User Agreements
- Compliance auditor reports
- Any changes to the HISP's audit parameters
- Any attempt to delete or modify audit logs
- Key generation
- Access to Private Keys for key recovery purposes
- Changes to trusted Public Keys
- Export of Private Keys
- Appointment of an individual to a trusted role
- Certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of the HPS

5.5.2 Retention Period for Archive

Then MHIN HISP retains the documentation described in Sections 5.2.6 and 5.5.1 of this document for a minimum of 6 years from the date of creation or the date when it was last in effect.

5.5.3 Protection of Archive

No Stipulation

5.5.4 Archive Backup Procedures

Archives are backed up according to the same requirements as § 5.4.5.

5.5.5 Requirements for Time-Stamping of Records

The MHIN HISP retains a date and time stamp on all certificates as they are downloaded from the CA DigiCert.

5.5.6 Archive Collection System (Internal vs. External)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

No stipulation.

5.6 Key Changeover

No stipulation beyond conformance with the DirectTrust CP.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The MHIN HISP has an Intrusion Detection and Mitigation Policy that defines the process of identifying and responding to suspected or known security incidents; mitigate harmful effects of security incidents that are known to the HISP or its Workforce; and appropriately document security incidents and their outcomes.

The MHIN HISP has a risk management plan to handle suspected breaches of PHI access. The protocol includes a risk assessment to determine if the incident is reportable, and includes at least the following evaluations: the unauthorized person(s) who received and/or used the PHI, the extent to which the risk to the PHI has been mitigated, whether the PHI was actually used/accessed/viewed, and the type and amount of PHI involved including the types of identifiers and likelihood of re-identification. The MHIN HISP has security and breach notification procedures in place in conformance with HIPAA and HITECH requirements. These procedures require that the notifications are to be delivered without unreasonable delay. The MHIN HISP has a Breach Management Policy that defines the plan for breach notification, including determination of proper entities to notify.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

The MHIN HISP maintains backup copies of system, databases, and private keys in order to rebuild the MHIN HISP capability in case of software and/or data corruption. Prior to resuming operations, the MHIN HISP ensures that the system's integrity has been restored.

5.7.3 Entity Private Key Compromise Procedures

No stipulation.

5.7.4 Business Continuity Capabilities after a Disaster

The MHIN HISP has developed a Business Continuity Plan (BCP) to be used in the event of emergencies such as natural disasters, system failures, vandalism and other emergency situations that prevent access to MHIN systems. It contains information about restoring operability and continuing business operations if a catastrophe occurs.

The MHIN HISP routinely evaluates all systems, applications and data that contain electronic Protected Health Information (ePHI) to assess and rank the criticality of applications and data containing ePHI. This is part of our ongoing risk management activities.

The Business Continuity Plan (BCP) includes procedures to be followed for emergency access to the facility if typical access is not available. Names and addresses of recovery facilities are listed along with steps to be taken should an emergency arise. A designated member of the Business Continuity Management Team will be responsible for all aspects of the Emergency Operations Center. The BCP includes quick response steps, an emergency phase section, an emergency operations center section, and staff and facility contacts.

The Facility Security and Maintenance Policy includes a Facility Security Plan. The plan lists various Physical/Technical Safeguards, including "A specially designed 'high security' key fob is issued to each authorized MHIN employee" and "Smoke detectors are strategically installed in the corporate office suites."

The MHIN Downtime access to PHI Policy establishes procedures for accessing necessary Electronic PHI during an emergency.

5.8 HISP Termination

No stipulation.

5.9 Backup of Electronic PHI

The MHIN HISP has established and implemented Data Backup and Storage Policy that describes the procedures that are followed to create, archive, index and maintain retrievable exact copies of Electronic PHI.

As described in our Hardware and Electronic Media Management Policy, the MHIN HISP ensures that sensitive information is removed from electronic media before it is physically relocated.

The MHIN HISP delivers all trusted Direct messages received on behalf of its End Users to the intended recipient's HISP-managed mailbox or to an Intermediate System authorized to accept messages on behalf of the End User. The MHIN HISP does not divert, copy, or redistribute incoming messages received on behalf of an End User to any other recipient, destination, application, or database, except as required for routine inline processing of messages for the End User.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

No Stipulation.

6.1.1.2 Subscriber Key Pair Generation

The MHIN HISP generates cryptographic key pairs for Subscriber Certificates on physical hardware that is well protected. The cryptomodule used for key generation SHALL be in accordance with section 6.2.1 of this HPS.

6.1.2 Private Key Delivery to Subscriber

The MHIN HISP does not deliver private keys to the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

The MHIN HISP generates key pairs and submits the Public Key to DigiCert the CA in a CSR as part of the certificate request process.

6.1.4 Public Key Delivery to Relying Parties

6.1.4.1 HISP Trust Anchor Delivery

The MHIN HISP delivers the CA Certificate Public Key to the DirectTrust Accredited Trust Bundle for distribution to Relying Parties. The MHIN HISP does not deliver CA Certificate Public Keys outside of the DirectTrust Accredited Trust Bundle.

6.1.4.2 End User Subscriber Public Key Delivery

The MHIN HISP Delivers End user Subscriber Public keys within Certificates made available for discovery through DNS or LDAP in accordance with Section 2 of this document.

6.1.5 Key Sizes

No Stipulation.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The MHIN HISP complies with the x.509 Certificate Policy as described in the DirectTrust Certificate Policy. This policy supports entities and applications involved in the exchange of electronic Direct messaging. The MHIN HISP enforces the permitted key usages when using certificates for which it holds the private key.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

To ensure that private keys have the strongest protection from unauthorized use, MHIN implements strict authorization and access controls where the certificate infrastructure resides, including private keys. The network drive where the encrypted file is located can only be accessed by key individuals at MHIN.

This network drive is used exclusively for direct certificates. MHIN routinely engages independent third-party health information technology professionals to conduct thorough threat and vulnerability assessments. MHIN contracted Healthy Security Solutions for a security risk assessment, which included a threat and vulnerability assessment. Since the private keys reside on MHIN's network, the risk assessment conducted by Health Security Solutions included the location and security of the private keys.

All private keys and certificates are encrypted with KeePass, which requires a password to access the encrypted file where the certificates and private keys are stored. In addition, the password used to access the private keys is managed through an encrypted database.

The MHIN Direct Role Based Access policy defines how users are provisioned with access based on job function. Within the Mirth Mail Administrative User Interface, only users with Administrative rights have access to the Direct Domains built in the system, and the corresponding certificate files. Currently, three MHIN users have Administrative rights. Even with access to the Direct Domains, the certificate files cannot be extracted from the Administrative User Interface once uploaded.

The MHIN HISP has a designated Information Systems Security Officer responsible for ensuring adequate protection of cryptographic keys and tracking who has access to said keys at any given point.

6.2.1 Cryptographic Module Standards and Controls

The MHIN HISP Cryptographic modules are compliant with the FIPS PUB 140 level 2.

6.2.2 Private Key (n out of m) Multi-person Control

No Stipulation beyond conformance with the DirectTrust CP.

6.2.3 Private Key Escrow

No stipulation beyond conformance with the DirectTrust CP.

6.2.4 Private Key Backup

The MHIN HISP utilizes MirthMail as its HISP Software platform. The Public and Private keys are stored within MirthMail. MirthMail is locally hosted on a MHIN server that utilizes VEEAM backup and replication. The VMWare cluster which includes the MirthMail server is connected via the MHIN Network to the VEEAM server for nightly backups which is then stored at an off-site location.

6.2.5 Private Key Archival

No stipulation beyond conformance with the DirectTrust CP.

6.2.6 Private Key Transfer into or from a Cryptographic Module

No stipulation beyond conformance with the DirectTrust CP.

6.2.7 Private Key Storage on Cryptographic Module

The MHIN HISP stores Private Keys into a cryptographic module meeting the requirements of section 6.2.1 as applicable for the entity.

6.2.8 Method of Activating Private Keys

No stipulation beyond conformance with the DirectTrust CP.

6.2.9 Methods of Deactivating Private Keys

No stipulation beyond conformance with the DirectTrust CP.

6.2.10 Method of Destroying Private Keys

Private Key signatures that are no longer needed are destroyed by Associates in trusted roles.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

Public keys are archived as part of the Certificate archival process.

6.3.2 Certificate Operational Periods/Key Usage Periods

Subscriber Certificates in the MHIN HSIP have a maximum lifetime of 3 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The MHIN HISP on behalf of the Subscriber generates activation data that has sufficient strength to protect its respective Private Keys. The MHIN HISP on behalf of the Subscriber only transmits activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

6.4.2 Activation Data Protection

No stipulation beyond conformance with the DirectTrust CP.

6.4.3 Other Aspects of Activation Data

No Stipulation

6.5 Computer Security Controls

The requirements of Sections 6.5 apply only to workstations and systems controlled by the MHIN HISP, which include any remote workstations operated by HISP personnel.

6.5.1 Specific Computer Security Technical Requirements

The MHIN HISP ensures that hardware, including any virtualized HISP hardware, and software containing End User private keys is well protected.

The MHIN HISP configures its systems to:

- Authenticate the identity of HISP personnel before permitting access to the system or applications
- Manage the privileges of HISP personnel and limit these users to their assigned roles
- Generate and archive audit records for all transactions listed in Section 5.4.1
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

The MHIN HISP authenticates and protects all communications between a trusted role and its HISP system. The MHIN HISP has a Password Management and Unique User Identification policy that ensures that access to the systems and networks owned and managed by MHIN are protected from improper access through the use of unique user identification and strong passwords. In accordance with the MHIN Log-In Monitoring Policy, the MHIN HISP locks access to secure HISP processes after 3 failed login attempts occur. All passwords are to be treated as sensitive, confidential MHIN information.

The MHIN HISP maintains a spreadsheet listing all sites that create, receive, maintain, or transmit PHI for the delivery of the services provided, whether company sites or outsourced organizations. The PHI Data Flow Document includes the site's name, address, relationship to the HISP, and the functions performed.

The MHIN HISP maintains and routinely updates inventories of all hardware and software, including software used to store, transmit and maintain electronic Protected Health Information (ePHI).

As outlined in MHIN's Intrusion Detection and Mitigation Policy, MHIN has deployed Intrusion Detection System (IDS) capabilities throughout its systems and technology environment at all locations. MHIN utilizes TrendMicro Office Scan v.11 for detecting viruses and malware on PCs and exchange servers. Cisco ASA is used for threat analysis and detection. As discussed further in Section 6.7.1, these safeguards do not extend to detection of malicious software that may be contained in Direct messages sent by or received on behalf of End Users.

During the privacy and security review conducted as part of new employee orientation, MHIN's policy regarding the use of personal, unlicensed, and/or unapproved software on workstations is explained to each new hire. Prior to deployment of a workstation to a MHIN employee, a set of approved licensed software programs are installed for workstation use. At that time, employees are reminded of their obligation to request new or additional software through the Technology Department rather than installing software independently. Random audits are conducted to validate only approved licensed software programs are installed on MHIN devices. When new software is requested for work-related use, a process for validating new software includes the use of a separate workstation to test and explore potential new software.

The MHIN HISP does not use web-based databases within MHIN's environment, so this criterion does not apply to any of MHIN's current business practices or services. MHIN contracts with Digital Hill for our website

The MHIN HISP utilizes the Mirth Mail product, which is accessed via a web site that is secured by an Entrust SSL certificate. The Mirth Mail Webmail Login Screen uses Entrust as the Certificate Authority and the HTTPS protocol. The application is Linux based and allows secure TLS mutual authentication connections, which requires installation and configuration of certificates, configuration of ports and IPs on MHIN's firewall, and setup and configuration within the Mirth Mail application. MHIN has contracted with Health Security Solutions to conduct a security risk assessment.

The MHIN HISP ensures that workstations with access to systems containing electronic Protected Health Information (ePHI) follow specific guidelines to safeguard ePHI. MHIN's Workstation Use and Security Policy outlines physical safeguards to implement for all workstations that access ePHI. MHIN has implemented physical and technical safeguards for all workstations that access PHI to restrict access to authorized users. The MHIN HISP has implemented automated time outs on all systems, networks, applications and other components of the technical environment.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

The requirements of Section 6.6.1 – 6.6.3 apply only to systems controlled by the HISP.

6.6.1 System Development Controls

The MHIN HISP utilizes the MirthMail software for Direct Messaging Service. MHIN does not participate in the software development or testing, though we may be asked to provide feedback as it pertains to end-user perspective of the product and proposed developments. Mirth provides updates for the Mirth Mail product, which the MHIN HISP system administrator downloads and installs through the

appliance's control panel. When upgrades are available and necessary, MHIN's Mirth Mail application is upgraded in accordance with the Change Management Policy.

The MHIN HISP implements the processes outlined in the Change Management Policy for managing changes to the MHIN HISP software application and supporting hardware. The Change Management Procedures address roles, responsibilities, and procedures for appropriate change control.

The MHIN HISP, as a member of DirectTrust participates in an ongoing interoperability testing program through DirectTrust including reporting of interoperability results as defined by such program.

6.6.2 Security Management Controls

The configuration of the MHIN HISP system as well as any modifications and upgrades are documented and controlled in compliance with the MHIN Change Management Policy. When loading software into the MHIN HISP system, MHIN verifies that the software is the correct version and is supplied by the vendor free of any modifications.

The MHIN HISP utilizes specific processes for initiating patches as described in the Enterprise Patch Management Procedure. A core team meets routinely to review any patches that are needed in the MHIN HISP application. Any patches deemed as necessary are installed in the Non-Production domain and validated. Before the patches can be configured in the Production domain, they are approved through the Change Management process.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The requirements of this section apply only to systems and networks controlled by the HISP. The MHIN HISP has a Portable Device Policy that prohibits HISP personnel from storing unencrypted PHI on personal computers, consumer devices, and removable storage media.

The MHIN HISP operates all wireless networks in a secure manner to ensure the confidentiality, integrity, and availability of all sensitive information transmitted over wireless networks. MHIN will ensure that all wireless devices are configured and operated according to the requirements set forth in The Wireless Security Policy.

The MHIN HISP utilizes a Cisco ASA5520 firewall which delivers a wide range of security Services with Active/Active high availability.

The MHIN HISP has implemented an Intrusion Detection and Mitigation Policy that sets forth the processes and procedures to monitor and/or block intrusion attempts or attacks from the Internet and provide alarms to appropriate personnel.

6.7.1 End User Data Storage and Edge Protocols

The MHIN HISP has implemented the Wireless Security Policy describing the MHIN's wireless network design to protect the privacy of data during transmission and in storage.

The Mirth Mail Application has a security infrastructure in place to ensure the security of user mailboxes in adherence to the standard HIPAA privacy rules defined at 45 CFR Part 160 and Subparts A and E of Part 16. Only authorized individuals can access Direct Project messages using MHIN Direct Messaging services.

Mirth Mail supports the XDR and XDM for Direct Messaging v1.0 specification. This process involves TLS mutual authentication, the exchange of public certificates with the client integrating with MHIN Direct Messaging. In addition to the exchange of certificates, additional system setup is required to recognize the XDR connection for successful completion of the SSL handshake, including firewall and system configurations.

The MHIN HISP provides the user with the ability to send and receive Direct Project messages from the webmail application or an XDR service.

The MHIN HISP has Business Associate Agreements in place that obtain satisfactory assurances that the Business Associate will uphold applicable Federal and State regulations. The MirthMail application safeguards PHI to prevent access to the Direct Message content that is only viewable by the Direct Message recipient. For administrative auditing purposes, access is limited to auditing transaction counts, and collecting source and destination information.

The MHIN HISP offers Cross-Enterprise Document Reliable Interchange (XDR) as an edge Protocol. This connectivity is in conformance with the XDR and XDM for Direct Messaging Specification, Version 1, published 9 March 2011 by the Direct Project.

6.7.2 Authentication of End Users

MHIN implements strict authorization and access controls with a minimum LoA-2. When registering for MHIN Direct Messaging, each organization must follow the Client Direct Enrollment Instructions, which illustrates the enrollment process, and required user security forms, for provisioning direct addresses.

For integration of external systems in the MHIN HISP, following the XDR and XDM for Direct Messaging v1.0 specification, this protocol utilizes TLS authentication.

The MHIN HISP has implemented the Password Management and Unique User Identification Policy that establishes all potential pathways for End User authentication, including mechanisms for password resets and initial password distribution, in a manner consistent with the minimum LoA-2 for end user authentication.

6.7.3 Authentication of Intermediate Systems

The MHIN HISP offers 2 different methods for accessing the HISP.

The first method is webmail access. End User Authentication of the webmail access to the MHIN HISP between the end user's device and the webmail client is accomplished via an https connection utilizing SSL/TLS encryption. Users are authenticated into the system by providing the unique user name and password combination.

The second method is XDR integration between the MHIN HISP and an organization's EMR. The intermediate systems are authenticated into the MHIN HISP using the XDR TLS authentication. They implement the underlying IHE Cross-Enterprise Document Reliable Interchange (XDR) Specification. An accounting of End User access is tracked both by the MHIN HISP and the Intermediate System.

6.7.4 Access Controls (Internal Access)

MHIN has implemented comprehensive procedures to determine the level of access to PHI needed by MHIN personnel, vendors, contractors and client users. Access is based on the prospective user's role and the minimum necessary PHI required to perform his/her job function; this determination guides access capabilities for each user and is carefully documented according to relevant policies and forms.

The Workforce Clearance and Security Policy states, "MHIN shall ensure all workforce members are only accessing systems and information to which they are authorized. To establish, review, and modify the privileges to access a workstation, transaction, software program, or process based on role or job function; MHIN will continually assess the need for access to sensitive information and PHI." Further, the attached Information Systems Access Policy states, "MHIN workforce members and client users are granted access only to that PHI to which they are authorized in order to perform their job role or associated job function."

MHIN's Workforce Clearance and Security Policy addresses termination procedures for MHIN workforce members stating "MHIN will terminate access to all systems and facilities when a member of the workforce has been terminated or no longer requires access to information or facilities in order to perform their assigned job role." This policy also includes a termination checklist for this process. When a MHIN employee is terminated, reference is made to the original Internal User Request form to determine which systems the user was provided access to as well as what hardware was issued to the individual

MHIN's Information Systems Access Policy addresses termination procedures for MHIN client users. The policy states, "Upon client notification of a change in a user's role, transfer or termination, user accounts are modified within one business day to reflect the change."

In addition, MHIN works closely with client security officers at each client organization with user access to MHIN applications. MHIN's HIE Participation Agreement Form states "Participant will designate an individual(s) as a privacy and/or security officer… will be responsible for… notifying MHIN of employee terminations, separations, and/or changes in individual employment status. Privacy and/or security officer will also be responsible for providing a current list of Authorized End Users to MHIN on an annual basis." MHIN receives notices to ensure timely notification and processing of termination or transfer for employees within those organizations. MHIN also conducts routine reviews of users at each client site to identify any inactive users and terminate their access.

The MHIN HISP as part of the MHIN HIE implements the same policies and procedures for access to PHI.

MHIN has implemented extensive policies regarding access authorization. MHIN uses role-based access, requires managerial authorization for user access to any application containing PHI, and requires that training of new users includes a review of MHIN's security standards before the user account is activated. All users sign the Application User Security Agreement. MHIN also has a formal process in place for modifying user access based on changes in roles or status within the organization, including a termination checklist. Well established processes are in place with our client security officers (or their designees) to send routine notifications of transfers, terminations and changes for existing users. In addition, audits of existing users are conducted on at least an annual basis.

MHIN has designed the security of its systems to ensure that MHIN's workforce, system users and systems can access only the type and amount of sensitive information necessary to carry out their assigned job role or function. As described in the Information Systems Access Policy, this design includes role-based access controls for each user that are based on the user's position and job responsibilities. Positions are created to meet the needs of users in specific roles within the MHIN or client workforce. An additional supporting policy is the Systems/Entity Authentication Policy.

End User access to the MHIN HISP is implemented according to the rules set forth in The Information Systems Access Policy.

Access to the MHIN HISP applications is restricted to authorized users or systems that have been approved by the client and MHIN security officers. When a system is assigned access to a database for monitoring or other system level activities, read-only access is assigned. User and system access is monitored continually to ensure that technical safeguards are in place and users and systems are complying with MHIN policies and procedures.

All MHIN applications containing electronic Protected Health Information (ePHI) require a unique username and password for access as stated in The Password Management and Unique User Identification Policy. Role based access is utilized for assigning user accounts. All MHIN applications provide audit trails that indicate activities performed by the individual user.

The MHIN HISP has implemented electronic procedures that terminate an electronic session after 15 minutes of inactivity.

6.8 Time Stamping

To ensure accuracy and precision across its HISP environment, The MHIN HISP utilizes NTP (Network Time Protocol) to synchronize its clock. The NTP host on the Mirth Mail server is 'north-american.pool.ntp.org'. The HISP environment is a virtual machine that is preconfigured by our vendor.

6.9 Direct Messaging Operations

6.9.1 CA and RA Services

The MHIN HISP utilizes DigiCert, a DirectTrust accredited Certification Authority and a DirectTrust accredited Registration Authority for all services it offers as DirectTrust accredited HISP Services.

6.9.2 End User/Subscriber Agreements

The MHIN HISP has implemented the Business Associate Agreement and Other Arrangements Policy, MHIN assesses contractual obligations based on the business relationship with the entity exchanging PHI. MHIN's Business Development Team engages all prospective clients and facilitates the execution of appropriate contracts after a Statement of Work is signed by the new client. As an internal verification, MHIN's Project Managers incorporate a standard set of preliminary tasks that confirm appropriate contracts, such as a Business Associate Agreement, are executed prior to the exchange of PHI with a client.

On an annual basis, MHIN conducts internal audits to confirm all legal documents including Business Associate Agreements are on file for MHIN clients, vendors, subcontractors, and trading partners.

All clients utilizing MHIN Direct Messaging services for exchanging or routinely accessing electronic PHI must follow the Client Direct Enrollment Instructions for onboarding, which includes required contractual agreements such as MHIN's Direct Subscription Agreement and a Business Associate Agreement.

MHIN has a Privacy and Security Statement for MHIN Products that encompasses all services provided by MHIN. During the contract negotiation for services to End Users or entities who are evaluating the MHIN HISP, this policy is available for review prior to entering into a contractual agreement.

The Privacy and Security Statement for MHIN Products is posted on the MHIN website under Privacy Commitment using the following link: http://www.mhin.org/about-us/confidentiality-access-and-security-policy/

6.9.3 Trust Management

The MHIN HISP manages trust anchors on behalf of End Users. MHIN participates within the Trust Bundles facilitated by DirectTrust. As stated in the MHIN HISP Direct Trust Anchor Policy MHIN only uploads trust anchors to the MHIN HISP production system from a Trust Bundle facilitated by DirectTrust that MHIN has contributed an anchor.

The MHIN HISP evaluates trust in counterparties via whitelist by Direct Domain, End Entity Certificates, and Certificate Authority. When evaluating a counterparty certificate, the MHIN HISP supports the capability to make trust decisions by matching the Distinguished Name and Public Key of an issuing CA in the certificate chain, or of the counterparty itself when the certificate is self-signed, against a local list of explicitly trusted anchors.

MHIN's Privacy Policy includes a HISP Policy for controlling counterparty trust Community. The MHIN HISP controls counterparty trust to End Users by only exchanging Trust Anchor Certificates with members of the DirectTrust Accredited Trust Community. During the contract negotiation for services to End Users or entities who are evaluating the MHIN HISP, this policy is available for review prior to entering into a binding contract for services.

The MHIN Privacy Policy is also posted on the MHIN website under Privacy Commitment using the following link: http://www.mhin.org/about-us/confidentiality-access-and-security-policy/

6.9.4 Direct Messaging Protocols

The MHIN HISP performs the STA functions defined in Section 1.3.4.1.1(a) of this document to securely route messages from sender's address to intended recipient's address as specified in the

Applicability Statement for Direct Secure Health Transport. Evidence of this functionality exists in the validation reports from the NIST Edge Testing Tool.

The MHIN HISP supports both DNS and LDAP methods for discovering recipient certificates as specified in the S&I Framework Certificate Discovery for Direct Project Implementation Guide. The MHIN HISP has successfully performed the DCDT Discovery Test Cases within the Discovery tab of the NIST Direct Certificate Discovery Testing Tool.

6.9.4.1 Message Disposition Notifications (MDNs)

The MHIN HISP provides final message storage for the recipient and generates final delivery notification upon request in the form of MDNs as specified in the Implementation Guide for Delivery Notification in Direct. The MHIN HISP does not delay the transmission of processed MDN's. A processed MDN is transmitted once the message has been fully decrypted, trust is verified and delivery is attempted. If such delivery attempt subsequently fails, the MHIN HISP transmits failure notification to the sender.

When the MHIN HISP delivers messages to an intermediate system, then a positive delivery notification is issued by the MHIN HISP upon successful handoff of the message by the MHIN HISP to the intermediate system, as defined by the edge protocol. A positive delivery notification is not a "read receipt" and does not imply that the message was opened, viewed, or acted upon by the recipient

The MHIN HISP has established time-out interval of 180 minutes for receipt of expected message disposition notifications from Counterparty HISPs. The MHIN HISP provides failure notifications when time-out intervals have been exceeded.

The MHIN HISP allows the end user to request final delivery notification as well as a return receipt for any outbound Direct messages.

6.9.4.2 Message Wrapping

The MHIN HISP generates a wrapped message by including the full MIME message submitted by or constructed on behalf of the End User in a message/rfc822 MIME wrapper to apply S/MIME security services to the wrapped header fields as specified in Section 3.1 of the "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," RFC 5751.

The MHIN HISP validates that sender and recipient information for an incoming message is consistent with the protected headers within the message/rfc822 wrapper and with the signer and encryption certificates used.

The MHIN HISP processes any message disposition notification requests included in the wrapped headers. Message disposition notifications sent in response to a wrapped message sets the value of Original-Message-ID field of the outgoing message disposition report to the value of the Message-ID field within the protected inner headers if this value is different from the outer Message-ID.
.

6.9.4.3 Case Sensitivity

For incoming messages, the MHIN HISP treats the Direct addresses that it services in a case insensitive manner. The domain part of any Direct address and any dnsName included in a domain-bound certificate is always treated in a case-insensitive manner.

6.9.4.4 Message Canonicalization

The MHIN HISP prepares the message content for signing in accordance with Section 3.1 of RFC 5751. This preparation includes conversion of all leaf parts of the MIME content to canonical form as detailed in Section 3.1.1 of RFC 5751 prior to computation of the message digest for the digital signature.

Before computing the message digest on an incoming message to validate a digital signature, The MHIN HISP treats the received content as if it were properly canonicalized by the sender.

6.9.4.5 Delivery Status Notifications

The MHIN HISP as the receiving STA when generating a Delivery Status Notification (DSN) sets a per-message extension field of X-Original-Message-ID with a value of the original RFC822 message ID to enable the original sending STA to correlate a DSN with the original message.

6.9.5 Directory Services

The MHIN HISP does not provide directory services for identifying the Direct addresses of counterparties.

7 Certificate, CRL, and OCSP Profiles Format

7.1 Certificate Profile

The MHIN HISP processes and uses certificates issued in conformance with the certificate profiles defined in the DirectTrust CP.

7.1.1 Version Numbers

The MHIN HISP utilizes DigiCert for CA Services. All certificates issued by DigiCert are X.509 version 3 certificates.

7.1.2 Certificate Extensions

No stipulation beyond conformance with the DirectTrust CP.

7.1.3 Algorithm Object Identifiers

No stipulation beyond conformance with the DirectTrust CP.

7.1.4 Name Forms

No stipulation beyond conformance with the DirectTrust CP.

7.1.5 Name Constraints

No stipulation beyond conformance with the DirectTrust CP.

7.1.6 Certificate Policy Object Identifier

No stipulation beyond conformance with the DirectTrust CP.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The MHIN HISP rejects a certificate if it encounters a critical extension it does not recognize or a critical extension that contains information that it cannot process.

7.2 CRL Profile

The MHIN HISP utilizes DigiCert for CA services DigiCert follows the FPKIPA's X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards. The MHIN HISP processes and uses CRLs issued in conformance with the CRL profile defined in the DirectTrust CP.

7.2.1 Version Numbers

No stipulation beyond conformance with the DirectTrust CP.

7.2.2 CRL and CRL Entry Extensions

No stipulation beyond conformance with the DirectTrust CP.

7.3 OCSP Profile

No Stipulation.

8 Compliance Audits and Other Assessments

The MHIN HISP has attained EHNAC DTAAP accreditation status effective October 1, 2016.

8.1 Frequency and Circumstances of Assessment

The MHIN HISP participates in the DTAAP Accreditation process every 2 years.

8.2 Identity/Qualifications of Assessor

The MHIN HISP participated in the EHNAC DTAAP Accreditation program in 2016 with a qualified compliance auditor provided by EHNAC to obtain DTAAP Accreditation. In 2018, at the required two year interval, the MHIN HISP will participate in the DirectTrust DTAAP Accreditation program with a qualified compliance auditor provided by DirectTrust.

8.3 Assessor's Relationship to Assessed Entity

The DirectTrust DTAAP Accreditation program provides the compliance assessor that performs the assessment. The program outlines the requirements in respect to the relationship of assessors to the assessed.

8.4 Topics Covered by Assessment

The MHIN HISP participates in the DirectTrust Accreditation program to certify HISP compliance. The program will outline the topics covered by assessment.

8.5 Actions Taken as a Result of Deficiency

The MHIN HISP will not claim conformance with reference to the DirectTrust HP unless it is in full compliance with the provisions and requirements of the DirectTrust HP. DirectTrust may take such steps as it deems appropriate to limit inaccurate claims of conformance.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

The fees associated with the cost of Certificate Issuance and Renewal, on behalf of the Subscriber, are passed onto the Subscriber as outlined in the Direct Subscription Agreement.

9.1.2 Certificate Access Fees

The MHIN HISP does not charge fees for the access and use of the certificates by the Subscribers.

9.1.3 Revocation or Status Information Access Fee

The MHIN HISP does not charge a fee for access to revocation or status information.

9.1.4 Fees for other Services

The MHIN HISP does not charge a Counterparty HISP a fee to exchange a Direct message on behalf of an End User.

9.1.5 Refund Policy

The MHIN HISP does not issue refunds for fees related to HISP services.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The MHIN HISP considers the following as confidential information within the HISP.

- Private Keys
- Audit Logs for event types specified in § 5.4.1
- Policies and procedures related to the MHIN HPS.

9.3.2 Information not within the scope of Confidential Information

Confidential Information will not include any information that is publicly available.

9.3.3 Responsibility to Protect Confidential Information

The MICHIANA HEALTH INFORMATION NETWORK PROPRIETARY INFORMATION AND INVENTION AGREEMENT contractually obligates employees, agents, and contractors to protect confidential information. The MHIN HISP provides training to employees on how to handle confidential information as defined by the Privacy and Security Awareness Training Policy.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

All identifying information for an End User is protected from unauthorized disclosure. The Privacy and Security Statement for MHIN Products posted on the MHIN web site specifies how the HISP handles personal information.

9.4.2 Information Treated as Private

Information deemed as private is defined as such in the BAA and User Enrollment forms between the HISP and its End Users.

9.4.3 Information not deemed private

See §9.3.2.

9.4.4 Responsibility to Protect Private Information

Private information is stored securely according to the policies and processes outlined herein.

9.4.5 Notice and Consent to Use Private Information

Private information may be used by the MHIN HISP Cerner in accordance with this HPS, the Privacy and Security Statement for MHIN Products referenced in § 9.4.1, and applicable Subscriber Agreements.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

The MHIN HISP does not disclose private information unless allowed by agreements with its End Users or unless required to by law.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The MHIN HISP Does not knowingly violate the intellectual property rights held by others.

9.6 Representations and Warranties

9.6.1 HISP Representations and Warranties

The MHIN HISP represents to End Users and Counterparties the compliance of all material aspects, with the DirectTrust HP, this MHIN HPS, and all applicable laws and regulations.

9.7 Disclaimers of Warranties

MHIN expressly disclaims all other warranties, both express and implied. Specifically, and without limitation, MHIN does not warrant that the MHIN Direct services will be error-free or uninterrupted or that any defects will be corrected. There are no implied warranties of accuracy, merchantability and fitness for a particular purpose, non-infringement of proprietary rights or any other warranty as may otherwise be applicable to the MHIN Direct services.

9.8 Limitations of Liabilities

Limitation of liability is specified in the Direct Subscription Agreement between the MHIN HISP and the End User.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This HPS becomes effective when approved by the MHIN management team and the HISP workgroup. This HPS has no specified term.

9.10.2 Termination

Termination of this Policy may occur if approved by the MHIN management team and the HISP workgroup.

9.10.3 Effect of Termination and Survival

The requirements of this HPS remain in effect as long as the HISP is in operation.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The MHIN HPS is maintained by the HISP workgroup and can be updated as needed at any time, but at a minimum, it will be reviewed annually by the MHIN management team and the HISP

workgroup. All versions and updates shall be linked to the Direct section of the MHIN web site http://www.mhin.org.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

No stipulation.

9.14 Governing Law

The laws of the United States of America SHALL govern this HPS.

9.15 Compliance with Applicable Law

MHIN has policies in place that ensure compliance with all applicable federal and state requirements and regulations.

According to MHIN's Policies, Procedures, Documentation and Evaluation Policy, critical documents are reviewed at least annually. However, policies are generally updated on an ongoing basis, as the need arises. MHIN's Risk Management and Assessment Policy also outlines the steps that are conducted to identify any inconsistencies or irregularities with the requirements of the Security Final Rule.

MHIN's legal contracts clearly define MHIN's HIPAA status as the Business Associate.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this HISP Policy is incorrect or invalid, the other sections of this HISP Policy shall remain in effect until the policy is updated.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.