DataMotion Direct
Certification Practices Statement
(Abbreviated Version)

CONFIDENTIAL
Access Limited to Authorized Personnel

June 18, 2019
Part # 060013–04-A

DataMotion Direct Certification Practices Statemen (Abbreviated Version) v4-A

Publication Date: June 18, 2019

Printed in the United States of America.

DataMotion, Inc. Confidential and Proprietary Information.

Published By:

DataMotion, Inc.
200 Park Ave.
Florham Park, NJ 07932
USA

1 800-672-7233 or +1 973-455-1245

http://www.datamotion.com/

Table of Contents

List of Tables

Revision History

For a list of revisions to the document, see the ***Revision History*** on page 79.

1 Introduction

This document is the DataMotion Direct Certification Practices Statemen (Abbreviated Version) (CPS), which is also referred to as “this DataMotion Direct CPS,” “this CPS,” or “this document.” This document also serves as the DataMotion Direct Registration Practice Statement (RPS).

This document states the policies and associated practices that DataMotion, Inc. (DataMotion) employs in operating the DataMotion Direct Public Key Infrastructure (DataMotion Direct PKI) as the Certification Authority (CA) and Registration Authority (RA) for X.509 digital certificates used in the exchange of electronic messages grounded in the Direct Project’s Applicability Statement for Direct Secure Health Transport.

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, message integrity, and non-repudiation.

The DataMotion Direct CPS is based on and is governed by the Direct Trust Community X.509 Certificate Policy (DirectTrust CP), and it is compliant with the DirectTrust CP version as specified in Section 1.1.2.

DirectTrust is a non-profit, competitively neutral, self-regulatory entity operated by and for participants in the Direct community. The DirectTrust Board of Directors, with the assistance of the DirectTrust Policy Committee, is responsible for the DirectTrust CP, the approval of related practice statements, and overseeing the conformance of CA practices with its CP.

The DataMotion Direct CPS also generally conforms to the policy framework described in RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, issued by the Internet Engineering Task Force (IETF). None of the sections stipulated by RFC 3647 have been omitted; however, to preserve the framework of RFC 3647, some sections of this CPS will include the statement “No stipulation” where the CP and CPS imposes no requirements or makes no disclosure, or “Not applicable” if the particular topic addressed by that section does not apply. DataMotion reserves the right to vary from this framework in its sole discretion.

This CPS is intended to be fully consistent with US Federal Government requirements for identity proofing as described in NIST Special Publication 800-63. More specifically, identity proofing levels of assurance defined in this CPS are intended to align with NIST SP 800-63 identity proofing levels of assurance. However, this CPS also specifies requirements that further constrain the conditions under which a DirectTrust Community conformant digital certificate may be issued, utilized and managed.

Operational requirements for issuing Certification Authorities and Registration Authorities operating under this CP are intended to be, at a minimum, consistent with operational requirements defined in the U.S. Federal Bridge Certification Authority CP for an entity operating at a Basic assurance level.

References

The following list identifies documents and related information referenced in this CPS.

Table 1. List of References

Document ID	Document Name
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, 3 December 2002.
FIPS 186-2	Federal Information Processing Standard (FIPS) Publication 186-2, Digital Signature Standard (DSS), January 2000.
RFC 1034	Internet Engineering Task Force (IETF) Request for Comments 1034, “Domain Names – Concepts and Facilities,” November 1987
RFC 2560	Internet Engineering Task Force (IETF) Request for Comments 2560, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”, issued by the IETF, June 1999.
RFC 3647	Internet Engineering Task Force (IETF) Request for Comments 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,” November 2003
RFC 5280	Internet Engineering Task Force (IETF) Request for Comments 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008
NIST SP 800-63-2	National Institute of Standards and Technology (NIST) Special Publication 800-63-2, Electronic Authentication Guideline, August 2013
X.500	ITU-T X.500 Recommendation (also ISO/IEC Standard 9594-1:2008), “The Directory: Public-key and attribute certificate frameworks”, November 2008
X.509	ITU-T X.509 Recommendation (also ISO/IEC Standard 9594-8:2014), “The Directory: Public-key and attribute certificate frameworks”, October 2012

1.1 Overview

This CPS describes the practices under which the DataMotion Direct Public Key Infrastructure (PKI) 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.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.1.1 Certificate Policy (CP)

According to the ITU-T X.509 standard, a “certificate policy” (CP) is defined as “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.”

Digital Certificates that conform to this CPS must contain a minimum of three registered certificate policy object identifiers (OIDs), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. An OID specifying the version of the Direct Trust CP, an OID corresponding to an identity proofing Level of Assurance (LoA), and an OID corresponding to a healthcare category shall be available to Relying Parties. The DataMotion Direct CA asserts the appropriate OIDs in the *certificatePolicies* extension of Subscriber certificates.

1.1.2 Relationship between the DirectTrust CP and this CPS

DataMotion has determined that substantial equivalence exists between the provisions of this CPS and the DirectTrust Community X.509 Certificate Policy, Version 1.4. Accordingly, DataMotion Direct certificates issued by the DataMotion Direct CA will assert the OID(s) defined in the DirectTrust Community X.509 Certificate Policy, Version 1.4. These include the OIDs for the following:

- DirectTrust Certificate Policy v1.4 OID: 1.3.6.1.4.1.41179.0.1.4

- One of the following Identity Proofing Level of Assurance (Levels 1 through 3) OIDs:
  - 1.3.6.1.4.1.41179.1.1
  - 1.3.6.1.4.1.41179.1.2
  - 1.3.6.1.4.1.41179.1.3

- One of the following Healthcare Entity Categories (Cat) OIDs:
  - 1.3.6.1.4.1.41179.2.1
  - 1.3.6.1.4.1.41179.2.2
  - 1.3.6.1.4.1.41179.2.3
  - 1.3.6.1.4.1.41179.2.4
  - 1.3.6.1.4.1.41179.2.5

- If the certificate is issued to a device, the Device OID is also asserted:
  - 1.3.6.1.4.1.41179.3

If DataMotion determines that its policies and practices continue to conform substantively to any future version of the DirectTrust CP, DataMotion may choose to assert the updated DirectTrust CP OIDs in its certificates instead.

1.1.3 Relationship between the DirectTrust CP and the DataMotion Direct CP

If in the future DataMotion creates its own CP governing this CPS, it will assert a mapping between its CP and the DirectTrust CP in the *policyMappings* extension of its CA and/or Subscriber certificates.

1.1.4 Relationship between DirectTrust CP and DirectTrust-EHNAC Accredited Entities

Conformance to an active DirectTrust CP version is a requirement for accreditation under the DirectTrust-EHNAC accreditation program, and entities accredited under this program have been audited regarding implementation of practices in compliance with an active DirectTrust CP version in conjunction with proper use of the DirectTrust policy OIDs. DirectTrust publishes bundles of trust anchors for the purpose of assisting Relying Parties in verifying the accredited status of HISPs, CAs, and RAs, available at bundles.directrust.org.

1.2 Document Name and Identification

This document is the DataMotion Direct Certification Practices Statemen (Abbreviated Version) (CPS) version 4-A.

This CPS defines multiple levels of assurance each assigned a unique object identifier (OID). The set of policy OIDs are registered under an arc of DirectTrust.org assigned organizational identifier as registered in the ISO/ITU OID Registry. The applicable OIDs pertaining to this CPS and the trust community are defined as follows:

[iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)]

Table 2. DirectTrust.org Certificate Policy Object Identifiers

id-DTorg arc		1.3.6.1.4.1.41179
id-DTorg-policies	id-DTorg.(0)	1.3.6.1.4.1.41179.0
DT.org CP 1.4	id-DTorg-policies.(1.4)	1.3.6.1.4.1.41179.0.1.4
Id-DTorg-LoAs	id-DTorg.(1)	1.3.6.1.4.1.41179.1
DT.org LoA 1	id-DTorg-LoAs.(1)	1.3.6.1.4.1.41179.1.1
DT.org LoA 2	id-DTorg-LoAs.(2)	1.3.6.1.4.1.41179.1.2
DT.org LoA 3	id-DTorg-LoAs.(3)	1.3.6.1.4.1.41179.1.3
DT.org LoA 4	id-DTorg-LoAs.(4)	1.3.6.1.4.1.41179.1.4
Id-DTorg-Cat	id-DTorg.(2)	1.3.6.1.4.1.41179.2
DT.org CE	id-DTorg-Cat.(1)	1.3.6.1.4.1.41179.2.1
DT.org BA	id-DTorg-Cat.(2)	1.3.6.1.4.1.41179.2.2
DT.org HE	id-DTorg-Cat.(3)	1.3.6.1.4.1.41179.2.3
DT.org Patient	id-DTorg-Cat.(4)	1.3.6.1.4.1.41179.2.4
DT.org Non Declared	id-DTorg-Cat.(5)	1.3.6.1.4.1.41179.2.5
DT.org Device	id-DTorg.(3)	1.3.6.1.4.1.41179.3

DataMotion Direct CA asserts only the OIDs above when issuing under the DirectTrust arc. Policy OIDs asserting additional compliance with other CPs, i.e., under a different policy arc MAY also be asserted.

NOTE: The Direct Project specification does not explicitly require utilization of policy OIDs as a mechanism of asserting trust. Rather, a set of trust anchor certificates are maintained by a relying party and each presented certificate must chain to a certificate within this set of trust anchor certificates. The DataMotion Direct CA only issues Direct certificates, and indicates which policy OIDs it issues certificates for, in order to be effectively utilized by Subscribers that depend exclusively upon binary trust of CA certificates.

1.3 PKI Participants

The community governed by this CPS is DataMotion Direct PKI. The DataMotion Direct PKI accommodates individuals and organizations with a need to securely exchange health information over the Internet.

PKI Participants are those entities involved in the registration, issuance, use of, or reliance upon DirectTrust Certificates. Participants include DataMotion, Customers, Subscribers, Relying Parties, Certification Authorities, and Registration Authorities. This DataMotion Direct CPS applies to all Participants in the DataMotion PKI. The following are descriptions of the roles relevant to the administration and operation of the DataMotion Direct PKI.

1.3.1 DataMotion Direct Management

The DataMotion Compliance Committee (DMCC) is the management team of DataMotion Direct that has established this PKI, oversees its operation, and is responsible for governing its use. This CPS was established under the authority of and with the approval of the DMCC. The DMCC is comprised of DataMotion security and business management individuals. The DMCC represents the interests of DataMotion and is responsible for:

- Approving the CPS and any successive changes,
- Ensuring continued conformance of this CPS with the DirectTrust CP, and
- Overseeing the conformance of DataMotion Direct practices with this CPS.

1.3.2 Certification Authorities (CAs)

The DataMotion Direct CA issues public key X.509 certificates for Direct exchange or Direct Project organizational or individual Subscribers, and, through such issuance, attests to the binding between an identity and cryptographic Key Pair to a Subscriber. The DataMotion Direct CA is also referred to as the Issuing CA or the Certificate Issuer in this document. As described in other sections of this document, the DataMotion Direct CA also publishes, maintains, and revokes certificates; publishes and updates Certificate Revocation Lists; and may also provide an OCSP service.

The DataMotion Direct CA is accredited through the DirectTrust and Electronic Healthcare Network Accreditation Commission (EHNAC) Direct Trusted Agent Accreditation Program (DTAAP) for issuing DirectTrust-compliant certificates, and this CPS is reviewed as part of that accreditation process to ensure conformance to the policies of the DirectTrust CP. This CA conforms to the policies of the DirectTrust.org CP v1.4.

1.3.3 Registration Authorities (RAs)

Registration Authorities (RA) are organizations responsible for collecting and proofing a Subscriber's identity and any other information provided by the Subscriber for inclusion in a certificate. DataMotion may act as its own RA or may delegate or subcontract the collection of identity proofing to a Trusted Agent that has executed an agreement establishing the agent in the role for performing identity proofing. This CPS also serves as the Registration Authority Practice Statement (RPS).

RAs collect and verify identity information from Direct Subscriber Applicants using procedures that implement the identity validation policies set forth in this document. If DataMotion delegates RA activities, it monitors their compliance with this CPS or the DirectTrust CP and if applicable, any Registration Practices Statement (RPS) under which the RA operates.

1.3.3.1 Trusted Agents (TAs)

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. While not an employee of the CA or RA, Trusted Agents are individuals who have a direct contractual relationship with the CA or RA, either as: a) an Individual; or b) an employee of an Organization that has a direct contractual relationship with the CA or RA that involves performance of collection and/or confirmation of information regarding Subscribers.

1.3.4 Subscribers

A DataMotion Direct *Subscriber* is an individual, organization or Device to whom or to which a certificate is issued. Subscribers are named in the certificate subject and hold either directly or through its designated HISP (or other authorized third party), a Private Key that corresponds to the Public Key listed in the certificate. A Subscriber is an entity who uses Direct services and PKI to support Direct message exchange. Prior to proofing of *Applicant*.

1.3.4.1 Health Information Service Providers (HISPs)

DataMotion is accredited by DirectTrust and the Electronic Healthcare Network Accreditation Commission (EHNAC) as a Health Information Service Provider (HISP) that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant certificate. Acting in the capacity of an agent for the Subscriber, the DataMotion Direct HISP holds and manages PKI private keys associated with a Direct digital certificate on behalf of the Subscriber.

1.3.4.2 Sponsors and Sponsoring Organizations

A Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel, or non-human system components named as public key certificate Subjects. The Sponsor works with the CA and RA to register the above elements in accordance with CPS Sections 3.2.2 and 3.2.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

An organization may sponsor an individual or device to be a Subscriber to a certificate. An authenticated and authorized organizational representative shall confirm the affiliation between the individual or device and the

organization. When an organization has sponsored an individual or device as a Subscriber of a certificate, the individual or device is considered as acting on behalf of and as an agent of the sponsoring organization when using the certificate and/or the corresponding keys.

1.3.5 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. A Relying Party may use a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information (CRL or OCSP).

1.3.6 Other Participants

1.3.6.1 Affiliates

An Affiliate is an individual or organization legally distinct from the Subscriber who is permitted by the Subscriber to use Direct Addresses bound to the Subscriber's certificate, provided that the Affiliate is performing its work, duties or activities on behalf of the Subscriber when using that Direct Address.

An individual granted proxy account access by a patient, such as a parent of a minor, spouse or health care proxy for an elderly person, is considered an Affiliate.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The primary use for a DataMotion Direct CA certificate is in the exchange of electronic messages grounded in the specification of the Direct Project. Other usages include but are not limited to securing healthcare applications and providing consumer/patient access to data.

Certificates issued by this CA shall only be used for the purposes designated in the *keyUsage* extension of the certificate key usage and extended key usage fields found in the certificate. However, each Relying Party should evaluate the application environment and associated risks before deciding on whether to accept a certificate issued by this CA for a particular transaction. In accepting a certificate issued by this CA, the Relying Party accepts all risks associated with its use.

An Affiliate that is a health care provider or health care organization may only use the certificate of a Subscriber if that Affiliate provides care on behalf of the Subscriber and the Subscriber is a HIPAA Covered Entity. A Covered Entity shall only be an Affiliate of another Covered Entity and shall not be an Affiliate of a Business Associate. For example, an HIE (Business Associate) shall not allow use of its own certificate by a health care provider or health care organization (Covered Entity).

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the

certificate was verified as reasonably correct to a known level of assurance when the certificate was issued. Certificates issued under this policy may not be used where prohibited by law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The DataMotion Compliance Committee (DMCC) is responsible for this CPS.

1.5.2 Contact Person

Questions regarding this document should be directed to:

CISO
DataMotion Compliance Committee
DataMotion, Inc.
200 Park Ave.
Florham Park, NJ 07932
USA

Phone: 1 800-672-7233 or +1 973-455-1245
Fax: +1 973-455-0750

1.5.3 Person Determining Certification Practices Statement Suitability

The DMCC is responsible for determining suitability of all documents under this CPS and for approving the content of this CPS and any future changes, updates, or modifications to it. Such approval shall be declared in Section 1.1.2.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Table 3. Acronyms

Acronym	Meaning
BA	Business Associate
CA	Certificate Authority
CE	Covered Entity
CFR	Code of Federal Regulations
CN	Common Name
CP	Certificate Policy

CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As
DMCC	DataMotion Compliance Committee
DN	Distinguished Name
DS	Discovery Service
DSA	Digital Signature Algorithm cryptography
DTAAP	Direct Trusted Agent Accreditation Program
EDSA	Elliptic Curve Digital Signature Algorithm cryptography
EHNAC	Electronic Healthcare Network Accreditation Commission
EIN	Employer Identification Number
FBCA	Federal Bridge Certificate Authority
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HE	Healthcare Entity
HIPAA	Health Insurance Portability and Accountability Act of 1996
HISP	Health Information Service Provider
HITECH	Health Information Technology for Economic and Clinical Health Act (part of the American Recovery and Reinvestment Act of 2009)
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Identifier
IETF	Internet Engineering Task Force
ISSO	Information System Security Officer
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LoA	Level of Assurance
NIST	National Institute of Standards and Technology
NPI	National Provider Identifier
OCSP	Online Certificate Status Protocol
OID	Object Identifier

ONC	Office of the National Coordinator for Health Information Technology (part of the U.S. Department of Health and Human Services)
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comments
RP	Relying Party
RPA	Relying Party Agreement
RPS	Registration Practice Statement
RSA	Rivest Shamir Adleman cryptosystem
SHA	Secure Hashing Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TA	Trusted Agent
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1.6.2 Definitions

Table 4. Glossary of Terms

Term	Definition
Address-Bound Certificate	A digital certificate that contains full Direct address in the form of an RFC 822 email address in the certificate *subjectAlternativeName* extension. It may also be referred to as an Individual Certificate or Individual Address Certificate.
Affiliate	An individual or organization legally distinct from the Subscriber who is permitted by the Subscriber to use Direct addresses bound to the Subscriber's certificate, provided that the Affiliate is performing its work, duties or activities on behalf of the Subscriber when using that Direct address. See CPS Section 1.3.6.1 Affiliates.
Applicant	A person or other legal entity that submits an application and identifying information to the CA or RA for the purpose of obtaining or renewing a certificate.
Business Associate or BA	An organization that helps Covered Entities carry out health care activities and functions under a written Business Associate contract or other arrangement with the Business Associate that establishes specifically what the Business Associate has been engaged to do and requires the Business Associate to comply with the requirements to protect the privacy and security of protected health information. Business Associates in this CPS are as defined under HIPAA at 45 CFR 160.103.
Certificate	An X.509 digital representation of information which at least (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.
Certification Authority or CA	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. See CPS Section 1.3.2 Certification Authorities (CAs). Sometimes referred to as a Certificate Authority.
Certificate Policy or CP	A Certificate Policy (CP) is a specialized documentation of administrative policy describing electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, distribution, accounting, revoking, compromise recovery and administration of digital certificates.
Certification Practices Statement or CPS	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing revocation status to Relying Parties.
Certificate Revocation List or CRL	A list maintained by a Certification Authority of the certificates that are suspended or revoked prior to their stated expiration date.
Code of Federal Regulations or CFR	Regulations imposed by U.S. Federal law.
Covered Entity or CE	An individual, organization, or agency that protects the privacy and security of health information and provides individuals with certain rights with respect to their health information. Covered Entities are defined under HIPAA at 45 CFR 160.103.
Device	A non-human Subscriber of a certificate. Examples of Devices include but are not limited to routers, firewalls, servers, imaging systems, consumer diagnostics, cameras, and other devices capable of securely handling private keys and properly implementing PKI technologies, either directly or through a HISP when used for Direct messaging.
Device Certificate	A certificate issued to a device.
Direct Address	Direct Addresses consist of a Health Endpoint Name, the "@" symbol, and a Health Domain Name, which is a fully qualified domain name (FQDN). For example: janedoe@direct.datamotion.com. Direct Addresses must be linked to an associated certificate that confirms the identity either of the domain name or of the full address. The intent of a Direct Address is to provide a method of routing from an origination point to the addressed recipient, not to provide a single, definitive ID for the intended recipient. The same real-world person may have multiple Direct Addresses.
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 a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
Domain-Bound Certificate	A certificate that contains a Health Domain Name in the form of a *dNSName* in the *subjectCommonName* and *subjectAlternativeName* extensions of the certificate. Also known as an Organizational Certificate.
Group Certificate	Certificate with a private key that is shared by multiple Subscribers. An Organizational Certificate is a type of Group Certificate that is shared among authenticated employees and agents of the organization. An Individual Address Certificate is a type of Group Certificate when the private key is held by the HISP on behalf of the Subscriber.
Health Domain Name	A fully qualified domain name dedicated solely to the purposes of health information exchange. The domain name string must conform to the requirements of RFC 1034 (Domain Names – Concepts and Facilities). For example: direct.datamotion.com.
Health Endpoint	A string conforming to the local-part requirements of RFC 5322 and that expresses real-

Name	world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. For example: janedoe (referring to an individual), familypractice (referring to an organizational inbox), and diseaseregistry (referring to a processing queue).
Health Information Service Provider or HISP	An organization that provides the management of security and transport as it relates to information exchange using Direct Project standards on behalf of the sending or receiving organization or individual. The HISP assigns and maintains the Direct email addresses for EHRs, HIEs, individual providers, as well as others, and relays their medical data securely using Direct protocols.
Healthcare Entity	An entity involved in healthcare that has agreed to protect private and confidential patient information consistent with the requirements of HIPAA although it is not a Covered Entity or Business Associate as defined under HIPAA at 45 CFR 160.103.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, as amended.
HIPAA Representative	A person named by a patient granting authority to have access to the patient's Protected Health Information. The designation of HIPAA representative does not in itself grant the representative authority to make health care decisions for the patient.
Internet Engineering Task Force or IETF	A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
Individual Certificate	Certificate tied to an individual full Direct address. See Address Certificate.
Information System Security Officer or ISSO	A person at the HISP who is responsible for managing the registration process, certificate requests, and private keys for Direct. This includes ensuring adequate protection of cryptographic keys held on behalf of customers, and also for tracking and recording who has access to the keys at any given point.
Key Pair	A Private Key and associated Public Key.
Level of Assurance or LoA or LOA	The identity proofing level implemented for issuance of a certificate. LoAs as used in this CPS are intended to correspond to identity proofing LoAs as defined in NIST SP 800-63.
Non-Declared Entity	An entity that has not asserted it will protect personal health information with privacy and security protections that are equivalent to those required by HIPAA and is not a Patient/Consumer.
Non-Declared Entity Certificate	A certificate issued to a Non-Declared Entity.
OCSP	An Internet protocol used for obtaining certificate's revocation status.
OCSP Responder	An Online Certificate Status Protocol service that processes certificate status queries.
Organizational Certificate	Certificate that asserts an organization affiliation and is tied to a Health Domain Name. It is a type of Group Certificate. See Domain-Bound Certificate.
Patient	An individual using his or her Direct Address for information exchange for personal reasons and not as a health care professional, Business Associate or individual associated with a HIPAA covered entity.
Patient Certificate	An address certificate issued to a patient containing a full Direct address in the form of an RFC 822 email address in the certificate *subjectAlternativeName* extension.
Private Key	The confidential key kept secret by its holder and which is part of an asymmetric key pair. It is used to create digital signatures or to decrypt data encrypted with the holder's corresponding Public Key.

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	The non-confidential key that is publicly disclosed by the holder in the form of a digital certificate and which is part of an asymmetric key pair. It is used for validation of a digital signature or to encrypt data that may then be decrypted using the corresponding private key.
Public Key Infrastructure	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	An organization that is responsible for proofing a Subscriber's identity and verifying any other information provided by Subscriber for inclusion in a certificate.
Relying Party	A person 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.
Sponsor	An individual who fills the role of a Subscriber for non-human system components named as public key certificate subjects. The Sponsor works with the CA and RA for registration of the components and is responsible for meeting the obligations of Subscribers as defined throughout this document.
S/MIME	A standard for public key encryption and digital signing of email messages.
Subscriber	An entity that either (1) authorized application for the certificate, or (2) is the subject named or identified in a certificate issued to that entity. A Subscriber may request certificate modification, renewal, suspension and revocation and holds, directly or through its designated HISP (or other Subscriber-authorized third party), a private key that corresponds to the public key listed in the certificate.
Subscriber Applicant	An individual that requests Direct enabled communication on behalf of their organization.
Trust Bundle	A collection of CA certificates used as trust anchors by a relying party.
Trusted Agent	An organization authorized to act as a representative of a Subscriber in confirming the Subscriber Applicant identification during the registration process.
Trusted Role	A role held by individuals performing functions fundamental to the integrity of the PKI.
User	An individual authorized by a Subscriber to access or make use of a private key corresponding to a certificate for the purpose of originating or accepting delivery of Direct messages.
X.509	The ITU-T standard for certificates and their corresponding authentication framework.

NOTE: The Remainder of the Document is Available on Request.

2 The Remainder of the Document is Available on Request