Updox
HISP Practices Statement

Version 1.1.1

May 25, 2018

Updox

6555 Longshore Street

Suite 200

Dublin, OH 43017

1-614-798-8170

http://updox.com

CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

This Health Information Services Provider (HISP) Practices Statement (HPS) describes the policy under which Updox operates as a HISP. These operations include: maintenance of security and trust within the Direct community, facilitation of an interoperable network of trusted Direct message recipients, minimization of risk and liability to participants exchanging Direct messages, and provision of a policy against which HISP practices can be evaluated through accreditation and audit.

This Updox HSP 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). This policy diverges from that framework where required to include additional unique aspects of HISP operations and Direct messaging for the secure 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.

Pursuant to the IETF RFC 3647 framework, this HSP is divided into nine parts that cover the security controls and practices and procedures for HISP-related Direct messaging services. To preserve 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 DirectTrust HP and Updox HPS

This HISP Practices Statement (HPS) describes how Updox meets the Direct Trust HISP Policy (HP) requirements.

1.1.2 Relationship between DirectTrust HP 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. That Workgroup 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”. Conforming HISPs SHALL use certificates in a manner that 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.

1.1.3 Relationship between the DirectTrust HP 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. Achieving accredited status can be viewed as an independent audit that the Updox HISP practices conform to the requirements of the DirectTrust HP.

1.2 Document Name and Identification

This HSP is associated with the DirectTrust HP unique object identifier (OID). The DirectTrust set of policy OIDs are registered under an arc of its assigned organizational identifier as registered in the ISO/ITU OID Registry. The applicable DirectTrust OIDs pertaining to this HP and the trust community are created under a DirectTrust arc defined as follows:

id-DTorg	iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) (41179)	1.3.6.1.4.1.41179
id-DTorg-hisp-policies	id-DTorg (5)	1.3.6.1.4.1.41179.5
DT.org HP Versions	id-DTorg-hisp-policies (version)	
DT.org HP Version 1.0	id-DTorg-hisp-policies (1) (0)	1.3.6.1.4.1.41179.5.1.0
id-DTorg-auth-LoAs	id-DTorg (6)	1.3.6.1.4.1.41179.6
DT.org Auth LoA 1	id-DTorg-auth-LoAs (1)	1.3.6.1.4.1.41179.6.1
DT.org Auth LoA 2	id-DTorg-auth-LoAs (2)	1.3.6.1.4.1.41179.6.2
DT.org Auth LoA 3	id-DTorg-auth-LoAs (3)	1.3.6.1.4.1.41179.6.3
DT.org Auth LoA 4	id-DTorg-auth-LoAs (4)	1.3.6.1.4.1.41179.6.4

This document also references the DirectTrust X.509 Certificate Policy v1.2 (OID 2.16.840.1.41179.0.1.2) and the DirectTrust Certificate policy “Draft for Trial use” version 1.1 (OID 2.16.840.1.113883.3.1313.0.1). Subsequent revisions to this HP might contain additional OID assignments beyond those identified above.

1.3 PKI Participants

The following are roles relevant to the administration and operation of the PKI within Updox operates to provide Direct messaging services.

1.3.1 PKI Authorities

1.3.1.1 Direct Project

The Direct Project (http://wiki.directproject.org/) develops and maintains the Applicability Statement for Secure Health Transport, and supporting Implementation Guides that allow for interoperability among HISPs.

1.3.1.2 DirectTrust

DirectTrust is a non-profit, competitively neutral, self-regulatory entity operated by and for participants in the Direct community. The establishment of DirectTrust was anticipated in the Direct Ecosystem Community Certificate Policy Version 0.9 that was developed and published by the Direct Project Rules of the Road Workgroup in accordance with the Direct Project consensus process.

1.3.1.3 Certification Authorities (CAs)

A certification authority (CA) in this context is an entity that signs certificate signing requests (CSRs) and issues public key X.509 certificates to Direct exchange or Direct Project organizational or individual Subscribers. Policies governing CA services are found in the DirectTrust CP.

1.3.1.4 Registration Authorities (RAs)

Registration Authorities (RA) operate identity management systems (IdMs) and collect and verify Subscriber information on the Issuer CA's behalf. RAs collect and verify identity information from Direct Subscribers using procedures that implement the identity validation policies set forth in the DirectTrust CP. Policies governing RA services are found in the DirectTrust CP.

1.3.2 End Users

An End User is an entity that uses a HISP's Direct services to support Direct transactions and communications. All End Users are Subscribers of Direct X.509 Certificates, as defined in the DirectTrust Certificate Policy, but not all Subscribers are End Users. Examples of End Users include healthcare professionals and consumers/patients. End Users are not always the party identified in a certificate, such as when domain-bound or address-bound certificates are issued to an organization.

1.3.3 Health Information Services Providers (HISPs)

An entity that conducts the exchange of Direct messages to and from Direct Addresses, in accordance with the Direct Project Applicability Statement (i.e. provides "Direct Services"), is a Health Information Service Provider (HISP). Direct Services cannot exist without a HISP. A HISP may act in the capacity of a Business Associate or Contractor for the End User, in which case the HISP may hold and manage the private keys associated with a Direct digital certificate on behalf of the End User. Alternatively, the HISP may be a component of a larger entity which provides Direct Services only to other components of the same entity.

1.3.3.1 HISP Boundary Considerations

The “HISP boundary” defines the part of the organization that constitutes the “HISP,” and is specified in order to allow for clear logical and/or physical borders where the HISP ends and other organizational functions and responsibilities begin. This document defines those functions that are inside the HISP boundary, and thereby those parts of an organization or product that are subject to the requirements of this Policy.

A HISP is responsible for the functions that are ALWAYS inside the HISP boundary, even if one or more of these functions is outsourced. For example, if an organization’s customer contract requires it to provide these functions either directly or through a subcontractor, then that organization is a HISP. If an organization and/or its subcontractors perform only some of these functions, then that organization, together with the parties performing the other functions, collectively constitute the HISP.

Functions ALWAYS inside the HISP boundary:

a) Perform Security/Trust Agent (STA) functions (decrypt inbound messages, validate counterparty signature, 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 6.7.1]
h) Maintain integrity of security and trust framework, includes review of security logs.
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

Functions SOMETIMES inside the HISP boundary: (While these functions are not performed by all HISPs, Updox does perform the ones listed in italics.)

l) Provision Direct Addresses
m) Generate End User private keys [section 6.1.1]
n) *Operate SMTP inbound or outbound server*
o) Operate POP/IMAP server
p) Operate DNS and/or LDAP servers hosting End User certificates for discovery
q) Maintain End User message queues and/or mailboxes
r) Provide Tools or interfaces to create a message and include attachments
s) Provide End User technical support

Functions OUTSIDE the HISP boundary: (These functions are not performed by HISPs and are outside the scope of this document. However, Updox does perform the ones listed in italics).

t) Perform CA and RA functions covered by CP, including any Trusted Agent role
u) Stores EHR/PHR data
v) Perform other EHR functions
w) Provide CDA processing and validation
x) *Operate Provider Directory*
y) Use of Direct credentials for other purposes

1.3.4 Counterparties

A Counterparty is either an end entity that receives a Direct message sent by the HISP's End User, or an end entity that sends a Direct message to the HISP's End User. If a HISP's End User is the sender of a Direct message, then the recipient is the Counterparty. If a HISP's End User is the recipient of a Direct message, then the sender is the Counterparty. A Counterparty 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.

1.3.5 Counterparty HISP

A Counterparty HISP is the entity providing HISP services to a Counterparty. The Counterparty HISP may be a different HISP than that used by the End User.

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. An Intermediate System may communicate directly with a HISP or two or more Intermediate Systems may form a chain of communication between the End User and the HISP. The 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.

When a single application includes components both inside and outside the HISP Boundary, such as an EHR technology with an integrated HISP, the portion of the application outside the HISP Boundary is an Intermediate System.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The primary anticipated use for a Direct Trust Community X.509 certificate is in the exchange of electronic messages grounded in the specifications of the Direct Project. This includes S/MIME message signature verification and S/MIME message encryption. Updox uses Certificates issued under the DirectTrust CP only for purposes permitted by the DirectTrust CP.

1.4.2 Prohibited Certificate Uses

Updox DOES NOT use Certificates and private keys issued under the DirectTrust CP for any purpose prohibited by the DirectTrust CP.

Note: Certificates do not guarantee that the subject of the certificate 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.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Updox manages the process for approval and administration of this document, which is aligned with the practices and procedures of the Direct Project. Updox is an LLC.

.

1.5.2 Contact Person

Questions regarding this HISP Policy should be directed to:

Updox
Attn: Compliance Director
6555 Longshore Street
Suite 200
Dublin, OH 43017 USA
1-614-547-9635
directadmin@updox.com

1.5.3 Person Determining HISP Practices Statement Suitability for the Policy

This HISP Practices Statement (HPS) states how Updox implements the policies required by the DirectTrust HISP Policy. Each conforming HISP is responsible for asserting that its HPS conforms to the DirectTrust HP. The Updox Management Team is responsible for this assertion.

Additionally, DirectTrust operates an Accreditation program in partnership with EHNAC that certifies the compliance of HISPs with the requirements of the DirectTrust HP. The determination of suitability shall be based on an independent compliance auditor's results and recommendations. See Section 8 for further details.

1.5.4 HISP Practices Statement Approval Procedures

Updox submits this HPS to a compliance analysis and audit against the DirectTrust HP as described in Section 8 of this policy. The Updox HPS meets all facets of that HP policy and declares conformance upon EHNAC Accreditation.

1.6 Definitions and Acronyms

1.6.1 Acronyms

CA	Certification Authority
CP	Certificate Policy
CRL	Certificate Revocation List
DN	Distinguished Name
DTAAP	Direct Trusted Agent Accreditation Program
DTPA	Direct Trust Policy Authority
EHNAC	Electronic Healthcare Network Accreditation Commission
HISP	Health Information Services Provider or Health Information Service Provider
HP	HISP Policy
HPS	HISP Practices Statement
ID	Identity
IETF	Internet Engineering Task Force
ISO/ITU	International Organization for Standardization/International Telecommunication Union
ISSO	Information Systems Security Officer
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comments
S/MIME	Secure Multipurpose Internet Mail Extensions

1.6.2 Definitions

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 1.1, dated July 10, 2012, or any subsequent version, published by the Direct Project.
Business Associate	An entity meeting the definition of a business associate under HIPAA at 45 CFR 160.103.
Certificate	A 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	An authority trusted by one or more users to create and assign certificates. Also known as a Certificate Authority.

Certificate Policy	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates.
Certificate Practice Statement	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements typically provided in a certificate policy.
Certificate Revocation List	A list maintained by a Certification Authority identifying the certificates that it has issued that are revoked prior to their stated expiration date.
Counterparty	The end entity on the other side of a Direct transaction with a HISP's End User. The Counterparty may act in the role of sender or recipient of a Direct message. For example, when a HISP's End User sends a Direct message, the recipient specified by the sender is the Counterparty. Conversely, when a HISP's End User receives a Direct message, the sender is the Counterparty.
Counterparty HISP	The HISP used by a Counterparty. This may be a different HISP than the HISP used by the End User.
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 a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
DirectTrust CP	Any one of the current Active Versions of the DirectTrust Certificate Policy, as further defined in Section 1.1.2.
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.
HISP	A provider of Direct messaging Security/Trust Agent services to Subscriber End Users.
HISP Policy	This document, written by DirectTrust, to define the requirements to be a "conforming HISP".
HISP Practices Statement	A document written by a HISP to demonstrate how the HISP meets the requirements of this HISP Policy, including both technical and organizational aspects.
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	A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.

Information Systems Security Officer (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.
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.
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 digital certificate.
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	The entity responsible for identification and authentication of certificate subjects.
Relying Party	A person/entity that 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.
Required Elements	Those elements of this HP that MUST appear in the Accreditation criteria.
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds, directly or through its designated HISP, a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party.
Trust Anchor	See Trust Anchor Certificate.
Trust Anchor Certificate	A Certificate identifying a trusted issuer of Certificates.
Trust Anchor Store	A collection of Trust Anchors.
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 Updox repositories that support all HISP operations are located at its 3rd party data center which also contains this HPS.

2.1.1 Repository Obligations

The Updox certificate repository is available 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 Certificates are hosted in the Updox DNS and discoverable via the URL in the Common Name field of the end entity certificate.

2.2.2 Publication of CA Information

No stipulation.

2.2.3 Interoperability

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

2.3 FREQUENCY OF PUBLICATION

No stipulation.

2.4 ACCESS CONTROLS ON REPOSITORIES

Updox protects repository information not intended for public dissemination or modification.

Updox provides unrestricted read-only access to its repositories for legitimate uses. Unauthorized persons are prevented from creating, deleting, or modifying entries in the repositories through logical and physical security measures.

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

No stipulation beyond conformance with the DirectTrust CP.

3.2 INITIAL IDENTITY VALIDATION

No stipulation beyond conformance with the DirectTrust CP.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

No stipulation beyond conformance with the DirectTrust CP.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

No stipulation beyond conformance with the DirectTrust CP.

4 CERTIFICATE LIFE-CYCLE

4.1 APPLICATION

No stipulation beyond conformance with the DirectTrust CP.

4.2 CERTIFICATE APPLICATION PROCESSING

No stipulation beyond conformance with the DirectTrust CP.

4.3 ISSUANCE

No stipulation beyond conformance with the DirectTrust CP.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation beyond conformance with the DirectTrust CP.

4.4.2 Publication of the Certificate by the HISP

Updox publishes End User certificates in a repository as specified in section 2.2.1.

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

Updox manages private and public key pairs in accordance with the DirectTrust Certificate Policy. Updox does not allow a Subscriber to take possession of their Private Key.

4.5.2 Relying Party Public Key and Certificate Usage

When using Counterparty certificates in the context of sending or receiving a Direct message, Updox processes the corresponding status information as follows:

A. If a certificate in the Counterparty certificate chain to be validated lists an OCSP (Online Certificate Status Protocol) responder and/or CRL distribution point then Updox obtains status information to confirm that the certificate has not been revoked before the certificate is trusted.

   1. If the status information is available, either from newly retrieved data or from a non-stale cached version, and either (a) the OCSP response indicates a good certificate, or (b) the CRL does not list the certificate as revoked, then Updox trusts the certificate chain so long as all other trust requirements are met.

   2. If the status information is available and the certificate is marked as revoked, then Updox treats the certificate chain as untrusted.

   3. If the status information is not available due to network or other failure, then Updox treats the certificate chain as untrusted.

B. If a certificate in the Counterparty certificate chain to be validated does not list an OCSP responder or CRL distribution point, or the OCSP response (if OCSP is used) indicates a certificate status of unknown, and Updox does not have another mechanism in place to determine the revocation of the certificate, then Updox does not trust the certificate.

As required by the Applicability Statement, Updox does not send a message disposition notification back to a Counterparty sender if an incoming message intended for an End User of the HISP is not signed with at least one trusted and valid certificate meeting local policy requirements.

Updox does not allow End Users to view untrusted incoming messages but does send a notification to the recipient to contact the sender.

4.6 Certificate Renewal

No stipulation beyond conformance with the DirectTrust CP.

4.7 Certificate Re-Key

No stipulation beyond conformance with the DirectTrust CP.

4.8 Modification

No stipulation beyond conformance with the DirectTrust CP.

4.9 Certificate Revocation and Suspension

Updox will revoke a certificate due to any of the following circumstances:

- Private key is suspected of compromise
- Requested by the Subscriber
- Updox has reason to believe the Subscriber Organization is in violation of Direct agreements

4.10 Certificate Status Services

When available, Updox makes use of OCSP responders to determine the status of a Counterparty certificate.

4.11 End of Subscription

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

Updox hosts all technology necessary for support of this CPS in Updox's Data Centers (DCs). The DCs are SOC1 (SSAE 16) and SOC2 Type 2 audited, HIPAA and PCI compliant.

The DCs undergo external and internal audits against PCI, HIPAA, SOX, JSOX, GLB, NIST 800-53 based controls, SSAE 16, SOC 2 and many more standards. External Type II SSAE 16 SOC 1 and SOC 2 reports are prepared each year.

5.1.1 Site Location and Construction

The off-site DCs have been purpose-built to support the continuous operation of hosted mission critical assets. The facilities have high-density, reinforced concrete walls encasing the data center core. The design and construction provide assurance that operations are protected against fire, floods, high winds, power outages, network issues and other hazards. The buildings are rated to withstand F3 tornados. There is no exterior signage.

5.1.2 Physical Access

The DCs have multiple layers of security, including video surveillance and biometric access control, to ensure that access is granted only to the appropriate individuals. Access is logged and retained. Each data center is protected and operated by an experienced network operations center (NOC) team.

5.1.3 Power and Air Conditioning

The DC has a fully redundant, 2(N+1) power, cooling, and network infrastructures. Power is provided by multiple power feeds from separate sources Backup power is via multiple UPS devices and diesel-powered generator systems. The DCs also utilize multiple carrier-neutral, high-speed internet feeds, delivered over a secure and redundant network.

The DCs employ a cold-aisle containment system, as well as a mix of climate cooling and mechanical cooling to create reliable and efficient environmental conditions throughout the facilities.

5.1.4 Water Exposures

The DCs are located at geographic safe zones and 8-inch cement exterior walls to protect against water exposure.

5.1.5 Fire Prevention and Protection

All critical spaces in the data centers utilize a clean agent fire suppression system and are free of flammable materials. The entire data center structure has a dual-interlock pre-action sprinkler system. VESDA is utilized in the data halls as well as in the return air plenums. Master fire panel resides in the data center Network Operations Center which is staffed 24x7. Central office monitoring is in place for all fire alerts.

5.1.6 Media Storage

Updox maintains a redundant architecture for all RA, CA, and HISP activities at two separate locations: 1) primary data center and 2) back-up data center. Updox does not utilize tape, disks, or any other type of mobile media.

5.1.7 Waste Disposal

Hardware and media are disposed of in accordance with HIPAA and industry best practices. Hard drives are destroyed before disposal, and shredding is used to dispose of documents and materials containing sensitive information.

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 – authorized to install, configure, and maintain the HISP software; establish and maintain HISP user accounts; configure HISP user accounts.
2. Information Systems Security Officer (ISSO): generate and manage End User private keys.
3. Operator – authorized to perform system backup and recovery.

Additional roles required by HIPAA:

4. HIPAA Security Officer – authorized to make changes to system security policy.
5. HIPAA Privacy Officer – authorized to be a point of contact for reporting and assisting in the investigation of any data breach that might take place.

The Updox Security/Privacy Officer is Mike Witting; backup officer is Connie Patterson.

5.2.1.1 Administrator

The administrator role is responsible for:

- Installation, configuration, and maintenance of the HISP
- Establishing and maintaining HISP system accounts

5.2.1.2 Information Systems Security Officer

The Information Systems Security Officer is responsible for:

- Configuring End User profiles or templates
- Generating, installing and backing up End User keys
- Managing End User access to private keys stored by HISP
- Managing 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

Performs duties of the Security Officer under HIPAA.

5.2.1.5 HIPAA Privacy Officer

Performs duties of the Privacy Officer under HIPAA.

5.2.2 Number of Persons Required Per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

A person occupying a trusted role will be authenticated to the HISP system.

5.2.4 Separation of Roles

No stipulation.

5.2.5 Access to Electronic PHI

Updox maintains a list of all individuals, contractors, and Business Associates with access to Electronic PHI and implements policies and procedures to ensure compliance with applicable requirements of the HIPAA Privacy and Security Rules.

5.2.6 Policies and Procedures

Updox records and maintains the policies and procedures implemented to comply with applicable federal and state regulations, and are available to those that need access to them.

Updox reviews these policies and procedures annually, and updates as needed, in response to environmental or operational changes affecting the security of the Electronic PHI.

5.2.7 Hybrid Entities

Updox is not part of a hybrid entity.

5.3 PERSONNEL CONTROLS

5.3.1 Background Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity. Persons who are not United States citizens are required to provide an H1b (non-immigrant visa).

5.3.2 Background Check Procedures

All new employees must provide proper documentation for verification of identity and eligibility to work in the United States in accordance with the Federal Immigration Reform Act of 1986. A criminal background check is performed when onboarding a new workforce member.

5.3.3 Training Requirements

Persons in a trusted role receive training on the privacy, security, quality, and regulatory processes and procedures employed by Updox as well as a review of the PKI principles and operations. On-going training is based on the employee's role and is a continual part of each employee's development.

5.3.4 Retraining Frequency and Requirements

Updox provides annual training for all employees and contractors with access to PHI. This training includes breach reporting and notification, privacy, confidentiality, and security.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Sections

Any employee found to have performed unauthorized actions may be subject to disciplinary action, up to and including termination of employment.

5.3.7 Independent Contractor Requirements

Independent contractors are required to sign a non-disclosure agreement (NDA) and contract that requires compliance to the personnel requirements in this HPS.

5.3.7.1 Business Associates of HISP

Updox does not use sub-contractors in HISP operations.

5.3.7.2 Cloud Service Provides as Business Associates of HISP

Updox does not use cloud vendors in HISP operations.

5.3.8 Documentation Supplied to Personnel

Employees are provided documentation outlining their job responsibilities.

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for events related to the HISP operations. All security audit logs are retained and made available during an audit.

5.4.1 Types of Events Recorded

All security auditing capabilities in the server operating system are enabled. The audit record includes:

- Type of event
- Date and time the event occurred
- A success or failure indicator, where appropriate
- Identity of the entity and/or person that caused the event

The following type of events are automatically recorded:

- Change to audit parameters (e.g. frequency, type of events audited)
- Attempt to delete or modify audit logs
- Attempt to assume a role (successful and unsuccessful)
- Change to maximum number of authentication attempts allowed
- Maximum number of unsuccessful authentication attempts reached during user login
- Unlock of an account locked by unsuccessful authentication
- Entry of security-relevant data
- Remote data entry of security-relevant messages received
- Export/output of confidential/security-relevant information (successful/unsuccessful)
- Generation of a key (not mandatory for one-time use keys)
- Loading of component private keys
- Access to certificate subject private keys
- Change to the trusted public keys (add, delete, edit)
- Manual entry of secret keys for authentication

- Export of private and secret keys
- Certificate request (new and re-key)
- Change to the security configuration of a system component
- Change to user account (add, delete, edit)
- Change to user permissions
- Change to certificate profile
- Change to revocation profile
- Change to the certificate revocation list profile
- Installation of a PKI application
- Installation of a hardware security module
- System start-up
- Logon attempts to PKI application
- Attempt to set/modify password
- Backup of internal database
- Restore from backup
- Re-key of the component
- Change to configuration – hardware
- Change to configuration – software
- Change to configuration – operating system
- Change to configuration – patches
- Software error condition
- Software check integrity failure
- Network attack (suspected or confirmed)
- Reset of operating system clock

The following type of events are manually recorded:

- Appointment of an individual to a Trusted Role
- Installation of an operating system
- Certificate revocation request
- Certificate compromise notification request
- Violation to physical security (known or suspected)
- Violation of Certificate Policy or Certificate Practices Statement
- System crash/hardware failure
- Equipment failure

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 Log

Security audit log data is directly available on the Updox equipment for a minimum of two months. After that, audit log data is available in the archive storage.

5.4.4 Protection of Audit Log

Only authorized personnel have access and can archive the audit logs.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up per section 5.1.8.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application level at all times while Updox is in operation.

5.4.7 Notification to Event-Causing Subject

The subject is not notified of the audit event.

5.4.8 Vulnerability Assessments

Updox conducts an accurate and thorough annual assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the HISP.

Updox, on a quarterly basis, conducts network and systems threat and vulnerability assessments and have an improvement process based on the results of those assessments. Annually these assessments are conducted through an independent third party. Updox maintains a general analysis of most likely scenarios for breaches of PHI security.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

Updox maintains a record of any action, activity, or assessment that may be required by applicable Federal and State regulations. The archive records include:

1. HISP Accreditations,
2. HP and HPS versions,
3. Contractual obligations and other agreements concerning the operation of the HISP, notably BAAs,
4. System and equipment configurations, modifications, and updates,
5. Certificate signing and revocation requests,
6. Any documentation related to the receipt or acceptance of a certificate or token,
7. End User Agreements,
8. Any data or applications necessary to verify an archive's contents,
9. Compliance auditor reports,
10. Any changes to the HISP's audit parameters,
11. Any attempt to delete or modify audit logs,
12. Key generation,
13. Access to Private Keys for key recovery purposes,
14. Changes to trusted Public Keys,
15. Export of Private Keys,

16. Appointment of an individual to a trusted role,
17. Destruction of a cryptographic module,
18. Certificate compromise notifications,
19. Remedial action taken as a result of violations of physical security, and
20. Violations of the HP or HPS.

5.5.2 Retention Period for Archive

Archives are retained for a minimum of six years from the date of creation or the date when it was last in effect, whichever is later.

5.5.3 Protection of Archive

Archives are protected according to the same requirements as specified in 5.4.4.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-stamping of Records

Archive records are automatically time-stamped using a trusted time service as they are created.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and 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

Updox has a process in place to identify and respond 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.

Updox 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.

Updox 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.

Updox has a documented plan for breach notification, including determination of proper entities to notify.

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

Updox maintains backup copies of system, databases, and private keys in order to rebuild the HISP capability in case of software and/or data corruption. Prior to resuming operations, Updox will ensure 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

Updox has written policies and procedures for responding to an emergency or other occurrence such as fire, vandalism, system failure, or natural disasters that impacts systems that contain Electronic PHI.

Updox conducts a quarterly data criticality analysis by assessing the relative criticality of specific applications and data in support of other contingency plan components.

Updox has procedures that allow secure facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

Updox has procedures for accessing necessary Electronic PHI during an emergency.

5.8 HISP TERMINATION

No stipulation.

5.9 BACKUP OF ELECTRONIC PHI

Updox:

- Creates, archives, indexes and maintains retrievable exact copies of Electronic PHI.
- Creates a retrievable exact copy of Electronic PHI before movement of equipment where PHI is stored.
- Clearly defines in its Business Associate Agreements its obligations relating to the backup of PHI.

Updox has no obligation to retain or archive any message it receives that is not addressed to one of its End Users, is not a Direct message, is from an untrusted source or bears an invalid digital signature, or does not otherwise meet the Updox policy for acceptable incoming messages.

Updox attempts to deliver all trusted Direct messages received on behalf of its End Users and meeting local policy requirements to the intended recipient's HISP-managed mailbox or to an Intermediate System authorized to accept messages on behalf of the End User.

Updox 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 or as required for Updox to meet any backup, archival, disaster recovery, or other requirement under HIPAA or other regulation.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

Updox generates key pairs in a manner conforming to the DirectTrust CP.

6.1.2 Private Key Delivery to Subscriber

Private Keys are not distributed to the Subscriber; rather Updox creates, stores, and manages the key pairs.

6.1.3 Public Key Delivery to Certificate Issuer

Public Keys are not delivered to Updox; rather Updox generates the public keys.

6.1.4 Public Key Delivery to Relying Parties

6.1.4.1 HISP Trust Anchor Delivery

The Updox trust anchor certificate is delivered to Relying Parties via the DirectTrust Accredited Bundle.

6.1.4.2 End User Subscriber Public Key Delivery

End user Subscriber Public keys are delivered within Certificates made available for discovery through DNS in accordance with Section 2 of this document.

6.1.5 Key Sizes

Key sizes for keys used by Updox conform to the DirectTrust CP.

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)

Key Usage Purposes asserted in the key usage field or extended key usage extension of certificates used by Updox conform to the DirectTrust CP.

Updox enforces the permitted key usages when using certificates if the field or extension is marked as critical.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Updox performs risk assessment and risk mitigation to ensure that the private keys have the strongest protection from unauthorized use.

The Updox Systems Security Officer (ISSO) is Mike Witting, who is responsible for ensuring adequate protection of cryptographic keys held on behalf of End Users, and also for tracking and recording exactly who has access to said keys at any given point in accordance with the DirectTrust CP.

6.2.1 Cryptographic Module Standards and Controls

No stipulation beyond conformance with the DirectTrust CP.

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

Private keys managed by Updox on behalf of its End Users are backed up to a secure offsite location to facilitate disaster recovery.

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

No stipulation beyond conformance with the DirectTrust CP.

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

No stipulation beyond conformance with the DirectTrust CP.

6.2.11 Cryptographic Module Rating

No stipulation beyond conformance with the DirectTrust CP.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

No stipulation beyond conformance with the DirectTrust CP.

6.3.2 Certificate Operational Periods/Key Usage Periods

No stipulation beyond conformance with the DirectTrust CP.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No stipulation beyond conformance with the DirectTrust CP.

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 – 6.5.2 apply only to workstations and systems controlled by Updox, which include any remote workstations operated by Updox personnel.

6.5.1 Specific Computer Security Technical Requirements

Updox hardware, including any virtualized HISP hardware, and software containing End User private keys are well protected.

Updox configures its systems to:

- Authenticate the identity of user before permitting access to the system or applications
- Manage the privileges of users and limit users to their assigned roles
- Generate and archive audit records
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

Additionally, Updox:

- Authenticates and protects all communications between a trusted role and its HISP system.
- Requires HISP personnel to memorize and not write down passwords or share passwords with other individuals.
- Implements processes to temporarily lock access to secure HISP processes if a certain number of failed log-in attempts occur.
- Maintains a pictorial diagram or spreadsheet listing all essential HISP function sites including their name, address, relationship to the HISP, and the functions performed.
- Maintains a listing of all hardware and software used to store, transmit or maintain Electronic PHI, including all Primary Domain Controllers (PDCs) and servers. Documentation indicates which software resides on which hardware.
- Uses effective controls and implements procedures for guarding against, detecting, and reporting malicious software. As discussed further in Section 6.7.1, this requirement does not extend to detection of malicious software that may be contained in Direct messages sent by or received on behalf of End Users.
- Has and enforces clear policies restricting the use of personal, unlicensed, and unapproved software.
- Ensures that internal databases cannot be modified directly through an external web site, unless modified securely by authenticated users.
- Has documented web server security configurations to protect any HISP web servers from attack or intrusion.
- Has policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access Electronic PHI.

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

Updox develops in a controlled development environment with modern source code control. Hardware and software are dedicated to performing the HISP tasks. The hardware and software containing private keys are well protected. Hardware and software updates are tested and installed in a professional and controlled manner.

Updox participates in an ongoing interoperability testing program with DirectTrust, including reporting of the interoperability results.

6.6.2 Security Management Controls

Updox requires all changes to be evaluated, documented, and approved before implementation. Updox has a configuration management methodology for installation and ongoing maintenance of the HISP system.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The requirements of this section apply only to systems and networks controlled by the HISP.

Updox:

- Has policies in place that prohibit HISP personnel from storing unencrypted PHI on personal computers, consumer devices, and removable storage media.
- Has appropriate security in place for wireless networks to protect the privacy of data during transmission and in storage.
- Has a firewall configured to protect the system integrity.
- Has 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

Updox:

- Has security measures to ensure that electronically transmitted PHI is not improperly modified without detection.
- Ensures the security of the messages processed by the HISP supports adherence to the standard HIPAA privacy rules defined at 45 CFR Part 160 and Subparts A and E of Part 164.
- Encrypts all edge protocol communications that enable last mile exchange between End Users' systems or Intermediate Systems and the HISP's Direct infrastructure by using TLS.

- Documents the methods it provides for accessing Direct Project messages.
- Is not required to examine the content of messages sent or received through its HISP system for the purpose of validating clinical document or other formatting, scanning for malicious code or content, or any other purpose.
- Examines content only to the extent permitted by any applicable Business Associate Agreement and/or other service agreement.
- Optionally offers Cross-Enterprise Document Reliable Interchange (XDR) as an edge protocol, 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

The Updox End User authentication requires a user ID plus a user-defined password that is compliant with DirectTrust Auth LoA 2 (secret password, at least 8 characters, and throttling mechanism to prevent more than 100 failed login attempts within 30 days). Authentication is performed over TLS.

6.7.3 Authentication of Intermediate Systems

The Updox Intermediate System authentication requires an application ID plus an Updox assigned randomly generated application password that is compliant with DirectTrust Auth LoA 2 (secret password, at least 20 characters, and throttling mechanism to prevent more than 100 failed login attempts within 30 days). Authentication is performed over TLS.

An accounting of End User access is tracked both by Updox and the Intermediate System.

Updox provides a secure means to authenticate itself to the Intermediate System to reduce risk of man-in-the-middle attacks

6.7.4 Access Controls (Internal Access)

Updox has policies and procedures to:

- Ensure that all members of the HISP Workforce have access only to Electronic PHI necessary to perform their work assignment and to prevent access to those Workforce members who do not have a need to access Electronic PHI.

- Determine that the access of a Workforce member, vendor, contractor and their employees to Electronic PHI is appropriate and is limited to only that which is necessary to the performance of work duties.

- Withdraw access to Electronic PHI when the employment of a Workforce member ends, the Workforce member's duties no longer justify the need to access Electronic PHI, or as required by determinations made as specified in the previous paragraph.

- If part of a larger organization, protect and secure the electronic PHI handled by the HISP from unauthorized access by the larger organization as well as their employees, vendors and contractors.

- Establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
- Maintain Electronic PHI to allow access only to those persons or software programs that have been granted access rights.
- Assign a unique name and number for identifying and tracking all systems' user identity.
- To log out an electronic session after a predetermined time of inactivity.

6.8 TIME-STAMPING

The system clock time for all HISP systems is derived from one of the trusted time services on the NIST Internet Time Service web site. The Updox system clocks are accurate within five seconds of the NIST time service. Synchronization occurs every 64 to 1024 seconds.

6.9 DIRECT MESSAGING OPERATIONS

6.9.1 CA and RA Services

Updox also performs CA and RA roles and completes the additional relevant sections of the EHNAC Accreditation related to these roles.

6.9.2 End User/Subscriber Agreements

Under HIPAA, Updox is a Business Associate to other Business Associates and to Covered Entities. Legally binding contracts for Direct messaging are in place for both scenarios, as well as, Business Associate Agreements (BAAs).

When the business relationship is with another Business Associate (e.g. EHR vendor), the BAA is between Updox and the BA. The BA, in turn, has BAAs with their customers (e.g. Covered Entities).

When the business relationship is with a Covered Entity, the BAA is between Updox and the Covered Entity.

6.9.3 Trust Management

Updox evaluates trust in counterparties via a whitelist of Certificate Authorities (CA) from the DirectTrust Accredited bundle which is refreshed every 24 hours (Updox is in this bundle).

The HISPs and/or CAs associated with the anchor certificates in this bundle are required to meet DirectTrust's accreditation criteria and to be audited on a bi-annual basis.

Trust bundles are managed in compliance with the Implementation Guide for Direct Project Trust Bundle Distribution, version 1.0, 14 March 2013.

The Updox HISP, CA/RA policies are available to End Users upon request prior to entering into a binding contract for services from Updox.

6.9.4 Direct Messaging Protocols

Updox performs authentication, encryption, trust verification and acknowledgement of responsibility to deliver the message utilizing SMTP transport protocol as specified in the Applicability Statement for Direct Secure Health Transport when securely routing messages from a sender's address to an intended recipient's address.

Updox supports certificate discovery for Direct messaging recipients through DNS and LDAP methods as specified in the S&I Framework Certificate Discovery for Direct Implementation Guide.

Updox performs STA functions in accordance with the:

- Applicability Statement, as defined in Section 1.6.2, and
- Certificate Discovery for Direct Project Implementation Guide dated January 9, 2012, or any subsequent version.

6.9.4.1 Message Disposition Notifications

In accordance with the Implementation Guide for Delivery Notification in Direct, Version 1.0, dated June 29, 2012, or any subsequent version, Updox sends the following Message Disposition Notices (MDNs) to a counterparty HISP:

Scenario	MDN Status
When receiving a Direct message	Processed
When receiving a Direct message and successfully delivering to the Edge Client and sending HISP requested a Dispatched MDN	Dispatched
When receiving a Direct message and unable to deliver to Edge Client	Failure
When sending a Direct message and counterparty HISP doesn't send a Processed MDN within 60 minutes	Failure

6.9.4.2 Message Wrapping

Messages signed or encrypted with keys associated with domain-bound certificates are vulnerable to certain in-transit header re-writing attacks. Therefore, when sending a message on behalf of an End User, Updox protects the outer, non-content-related message header fields by wrapping the message as specified in Section 3.1 of the "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," RFC 5751, published by the Internet Engineering Task Force.

Updox generates a wrapped message by including the full MIME message constructed on behalf of the End User in a message/rfc822 MIME wrapper in order to apply S/MIME security services to the wrapped header fields.

Updox uses the same non-content-related message header fields in both the outer headers and the wrapped headers and also suppresses the “Subject” header field in the outer message.

When receiving a wrapped message Updox validates that the sender and recipient information for the message is consistent with the protected header within the message/rfc822 wrapper and with the signer and encryption certificate used. If an inconsistency is found the message is rejected.

Updox processes message disposition notifications (MDN) as requested in the wrapped header. The Original-Message-ID field in the outgoing MDN contains the Message-ID value from the protected inner header of the received message.

Updox accepts both wrapped and unwrapped messages.

6.9.4.3 Case Sensitivity

Updox treats both incoming and outgoing Direct addresses in a case-insensitive manner.

6.9.4.4 Message Canonicalization

Updox prepares Direct 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 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, Updox treats the received content as if it were properly canonicalized by the sender.

6.9.4.5 Delivery Status Notifications (DSNs)

When sending Delivery Status Notifications, Updox includes the original message ID in the X-Original-Message-ID extension field.

When receiving Delivery Status Notifications that don’t contain an X-Original-Message-ID extension field, Updox uses the value in the In-Reply-To field when available to correlate the DSN with the original message.

6.9.4.6 Directory Services

Updox provides a Direct address directory to its users. Users must comply with the directory usage policy which encompasses requirements from the DirectTrust Directory Sharing Policy.

7 CERTIFICATE, CRL, AND OCSP PROFILES FORMAT

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

No stipulation beyond conformance with the DirectTrust CP.

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

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Updox rejects a certificate if it encounters a critical extension it does not recognize or a critical extension that contains information that it cannot process. No stipulation is made regarding processing of unrecognized certificate policies marked as non-critical.

7.2 CRL PROFILE

7.2.1 Version Numbers

Updox processes X.509 version 2 CRLs (i.e. CRLs with the version field containing the integer 1).

7.2.2 CRL and CRL Entry Extensions

Updox processes CRLs that conform to the CRL and CRL Extensions profile defined in IETF RFC 5280.

7.2.3 OCSP Profile

No Stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Updox contracts with the following 3rd party assessors to ensure the requirements specified in this HPS and the DirectTrust HP are implemented and enforced.

- EHNAC Accreditation
- ONC Health IT Certification
- Cadre Security Assessment
- Updox 3rd party Data Centers undergo SOC1 (SSAE 16) and SOC2 Type 2 audits.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

EHNAC	Bi-annual	Covers all aspects of the HPS/HP
ONC Health IT	Bi-annual	Covers Direct messaging transport and cert discovery
Cadre Security	Annual	Covers network security and HIPAA policies
Data Centers	Annual	SOC1 (SSAE 16) and SOC2 Type 2 audits.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The independent auditor must:

- Demonstrate competence in the field of compliance audits
- Be familiar with Public Key infrastructures, certification systems, and Internet security issues as well as Updox's requirements associated with the issuance and management of certificates

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Updox uses independent auditors through EHNAC that do not have a financial interest or business relationship with Updox.

8.4 TOPICS COVERED BY ASSESSMENT

DirectTrust provides an Accreditation program in partnership with EHNAC to certify the compliance of CAs, RAs, and HISPs; the program will outline the topics covered by assessment.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law or this HPS then Updox will initiate a formal action plan to remediate the deficiencies.

8.6 COMMUNICATION OF RESULTS

The results of each audit are reported to the Updox Management Team for review and approval. DirectTrust is notified of EHNAC accreditation status. EHNAC publishes the current status on their website: https://www.ehnac.org/accredited-organizations/.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

Updox does not charge a counterparty HISP a fee to exchange a Direct message on behalf of an End User.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

Confidential Information means any information that (a) is clearly marked as confidential, (b) that by its nature or context should reasonably be understood to be confidential.

9.3.2 Information not Within the Scope of Confidential Information

Confidential Information will not include any information (i) that is publicly available through no breach of this HPS, (ii) that is independently developed by Subscriber, Updox, or (iii) that is rightfully acquired by Subscriber or Updox from a third party who is not in breach of an agreement to keep such information confidential. Except as expressly permitted by this HPS, neither Subscriber or Updox will disclose, use, copy, distribute, sell, license, publish, reproduce or otherwise make available confidential information of others.

9.3.3 Responsibility to Protect Confidential Information

Updox and Subscriber will each (i) secure and protect confidential information by using the same or greater level of care that it uses to protect its own confidential and proprietary information of like kind, but in no event less than a reasonable degree of care, and (ii) require that each of their respective employees, agents, attorneys and independent contractors who have access to such confidential information are bound to at least as restrictive confidentiality terms as this section 9.3.

Notwithstanding the foregoing, any party may disclose another party's confidential information to the extent required by applicable law or regulation or by order of a court or other governmental entity, in which case, if permitted, such party will notify the other disclosing party as soon as practicable prior to such party making such required disclosure.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

Updox protects the privacy of the information sent through Updox Direct in accordance with its privacy policy which can be found at http://updox.com/privacy-policy.

9.4.2 Information Treated as Private

See section 9.3.1.

9.4.3 Information not Deemed Private

See section 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 Updox in accordance with this HPS, the privacy policy referenced in section 9.4.1, and applicable Subscriber Agreements.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Notwithstanding the foregoing, Updox may disclose confidential and/or private information to the extent required by applicable law or regulation or by order of a court or other governmental entity, in which case, if permitted, Updox will notify the disclosing party as soon as practicable prior to such party making such required disclosure.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

Updox has and shall retain sole and exclusive right, title and interest, including copyright and all other rights, in and for the Updox Direct services. Updox hereby reserves all rights not expressly granted hereunder. Updox will not knowingly violate the intellectual property rights held by others.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 HISP Representations and Warranties

Updox warrants that it will perform the functions outlined in this HPS in accordance with applicable laws and regulations and in a professional manner.

9.6.2 CA/RA Representations and Warranties

No stipulation.

9.6.3 End User Representations and Warranties

Subscriber warrants it will:

- Provide accurate and complete information and communication to Updox
- Confirm the accuracy of certificate data prior to using the certificate
- Promptly cease using a certificate and notify Updox if (1) any information that was submitted to Updox becomes misleading or (ii) there is any actual or suspected misuse or compromise of the private key associated with the certificate
- Use the certificate only for authorized and legal purposes, consistent with this HPS and Subscriber Agreement
- Promptly cease using the certificate and related Private Key after the certificate's expiration

9.6.4 Counterparty Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Affiliated Organizations

No stipulation.

9.6.6 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

No stipulation.

9.8 LIMITATIONS OF LIABILITY

No stipulations beyond the Updox Certificate Practices Statement.

9.9 INDEMNITIES

No stipulations beyond the Updox Certificate Practices Statement.

9.10 TERM AND TERMINATION

9.10.1 Term

Upon management acceptance, the HPS is effective immediately and supersedes all prior versions.

9.10.2 Termination

Termination of this HPS may occur if approved by the Updox management team.

9.10.3 Effect of Termination and Survival

The requirements of this HPS remain in effect through the end of the archive period.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

This HPS may be amended by the Updox management team as needed.

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

All disputes regarding this HPS shall be brought to the exclusive jurisdiction and venue of courts in Franklin County, Ohio, USA. Any cause of action or claim against Updox under this HPS must be commenced within one (1) year after the claim or cause of action arises.

9.14 GOVERNING LAW

The laws of the United States of America govern this policy.

9.15 COMPLIANCE WITH APPLICABLE LAW

This HPS is subject to applicable federal, state, and local laws, rules, and regulations (the "Laws"). Updox, each Subscriber, and Relying Party shall comply with all Laws, as it relates to their responsibilities hereunder.

Updox continuously monitors and performs and annual technical and non-technical evaluation based on applicable Federal and State regulations and standards, demonstrating the extent to which an entity's security policies and procedures meet the requirements of relevant regulations. Updox subsequently responds to changes affecting the security of Electronic PHI.

Updox is Business Associate under HIPAA.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If any provision hereof is held to be invalid or unenforceable, the remaining provisions will remain in full force. All waivers of and consents to any terms of this HPS (or any rights, powers or remedies under it) must be in writing to be effective. No waiver or consent granted for one matter will be construed as a waiver or consent for a different matter.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

Updox will not be liable for failure to perform any of its obligations under this HPS if such failure is caused by an event outside its reasonable control, including but not limited to, an act of God, war, an act of terrorism, fire, or natural disaster.

9.17 OTHER PROVISIONS

No stipulation.

Document History

Date	Description	Noted By
7/15/2015	Reviewed and approved by management team (Mike Witting, Mike Harris, Connie Patterson)	Connie Patterson
3/23/2016	7.2.1 and 7.2.2 – reworded; no change to the meaning. 6.8 - Removed redundant sentence 9.10.1 – change “upon publication” to “upon management acceptance”	Connie Patterson
8/22/2016	1.6.2 Definitions – added Private Key 5.3.7.1 – indicated that Updox does not use subcontractors 5.3.7.2 Cloud Service Provides as Business Associates of HISP (new) 6.9.3 Trust Management - revised 6.9.4.3 Case Sensitivity (new) 6.9.4.4 Message Canonicalization (new) 6.9.4.5 Delivery Status Notifications (DSNs) (new) 6.9.4.6 Directory Services (new) 8.6 Communication of results – added EHNAC website 9.8 Limitations of liability – changed to refer to Updox CPS 9.9 Indemnities – changed to refer to Updox CPS	Connie Patterson
5/25/2018	Updated the Updox corporate office address, logo, and modified information regarding the data center facilities.	Connie Patterson