SURESCRIPTS CA
CERTIFICATION PRACTICE STATEMENT

DATE: 10/29/2020

DOCUMENT CHANGE LOG

Version	Date	Details
1.0	03.21.2013	Whole doc
1.0.a	04.25.2013	Whole doc
2.0	03.13.2014	Formatting, Ownership and contact information, and updates to IDP processes
3.0	09.28.2015	Combined in practices for issuing TLS certificates under Federal Bridge program and Webtrust 2.0
3.0a	10.09.2015	Updated subscriber requirements and subscriber document retention
3.1	11,11.2015	Updated certificate revocation procedures
1.3	1.30.2017	Updated OID, HISP policy reference, contact information, change log format
1.3.2	2/22/2017	Updates for SSL Baseline changes in Dec 2016 for Webtrust
1.3.3	3/20/2017	Addition of section 5.7.5 Business Continutiy Plan
1.3.4	1/25/2018	Webtrust 2.2 updates
1.4.0	10/9/2018	Direct Trust v1.4 CP updates
1.4.1	8/19/2019	Webtrust Updates
1.4.2	10/29/2020	Annual Updates for DirectTrust Accreditation guidelines

SURESCRIPTS CPS

PUBLISHED BY
SURESCRIPTS, L.L.C.
920 2ND AVENUE S.
MINNEAPOLIS, MN 55402
PHONE: 866-267-9482
FAX: 651-855-3001

2800 CRYSTAL DRIVE
ARLINGTON, VA 22202
PHONE: 866-797-3239
FAX: 703-921-2191

Internal Use Only

TABLE OF CONTENTS

List of Tables

SECTION 1 INTRODUCTION

1.1 OVERVIEW

The Surescripts CA Practice Statement (CPS) describes the practices, such as PKI, used to comply with DirectTrust policies, WEBTRUST Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 2.4.1, and identity vetting requirements of NIST 800-63-2 looking forward to upcoming requirements for NIST 800-63-3. The CPS follows the structure of the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure (PKI) Certificate Policy and Certification Practices Framework (RFC 3647).

The CPS supports entities and applications involved in the exchange of electronic messages grounded in the specification of the Direct Project, sponsored by the Office of the National Coordinator (ONC) for Health Information Technology. 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. This CPS also supports certificate requirements for entities utilizing Transport Layer Security (TLS) and Mutual Authentication TLS (MATLS).

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine parts that cover the security controls, practices and procedures for certificate and related services within the Surescripts PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation."

This CPS describes the practices under which the Surescripts Certificate Authority operates for two levels of assurance: LoA 2 and 3 (software only). Specifically, this document defines the creation and life-cycle management of X.509 version 3 public key certificates for use in applications supporting Direct Message exchange.

The terms and provisions of this CPS shall be interpreted under and governed by applicable Federal law. In addition, all requirements and control provisions herein are independently audited annually for compliance with *Version 2.4.1 of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security* current version requirements.

1.1.1 CERTIFICATE POLICY (CP)

Surescripts, L.L.C. (“Surescripts”) utilizes a Certificate Policy (CP) to describe its policies for operating a CA. Surescripts has adopted the Direct Trust Community X.509 Certificate Policy (DirectTrust CP), current version 1.4.

Digital certificates that are issued conforming to this CP contain at least one registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a level of assurance at LoA 3 as established by the CP which is available to Relying Parties. A certificate issued by a conforming CA asserts the OID in the certificatePolicies extension.

The Surescripts CA is responsible for the oversight of all registration authority (RA) duties and obligations, including all identification and verification duties related to such applications and the verification of revocation requests. Such duties related to the RA are performed by different teams

within Surescripts and separate from the duties of the CA. The Surescripts CA utilizes the PKI Repository (as further described in Section 2.1) to publish certain documents and information regarding this CA and its participants. This information is available only to those entities affiliated with the Surescripts CA; the general public may not have access to this information.

Information Security Compliance has published this CPS, in accordance with ISMS Document Management Standards and as approved by Surescripts PKI Management,to define the practices and procedures the Surescripts CA employs when issuing, signing, supporting, and revoking certificates and cryptographic keys. Provisions in this CPS supercede requirements in Direct Trust CP where deviations exist.

1.1.2 RELATIONSHIP BETWEEN THE SURESCRIPTS CPS AND THE DIRECTTRUST CP

Information Security analyzes the DirectTrust X.509 Certificate Policy and makes a determination of the suitability for cross-certification and the requirement to publish custom requirements.

1.1.3 RELATIONSHIP BETWEEN THE SURESCRIPTS CPS AND DIRECTTRUST HISP POLICY

For its HISP services, Surescripts has adopted and complies with DirectTrust HISP Policy version 1.1. Requirements not specifically identified in this CPS may be found in the related DirectTrust Policy.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the Surescripts CA Certification Practice Statement (CPS) and was approved for publication by Information Security, in accordance with ISMS Document Management Standards. The CPS corresponds to the policy requirements described in the Surescripts Issuing CA CP, which maps to the DirectTrust Community X.509 Certificate Policy version 1.4.

This CPS defines multiple levels of assurance which are assigned a unique object identifier (OID). The set of policy OIDs are registered under an arc of assigned organizational identifiers as registered in the ISO/ITU OID Registry.

The OID breakdown for Direct Trust is defined as follows:

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

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 Versions	id-DTorg-policies.(version)	1.3.6.1.4.1.41179.0.1
DT.org CP Versions	id-DTorg-policies.(v1.4)	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
Surescripts PKI		1.3.6.1.4.1.37583
Surescripts Low Assurance Policy		1.3.6.1.4.1.37583.509.50.1.1
Surescripts Basic Assurance Policy		1.3.6.1.4.1.37583.509.50.1.2
Surescripts Medium Assurance Policy		1.3.6.1.4.1.37583.509.50.1.3

Certificates issued under DirectTrust policies by this CA are performed at levels of assurance or conform to the requirements for a given healthcare entity category (Cat) at the appropriate OID or OIDs, as defined above in the Certificate Policies X.509 v3 standard extension. See sections 3.2.2 and 3.2.3.1 for details of each LoA and Cat.

Certificates used for TLS or MATLS conform to WebTrust for Certification Authorites - SSL Baseline with Network Security Version 2.4.1 and are identified by the OID's for Surescripts PKI policies.

This CPS completely applies to any entity asserting one or more of the Surescripts OIDs identified above with the exception of SS-TLS. Unique differences for Surescripts PKI policy certificates are identified in their respective sections. All other OIDs mentioned herein belong to their respective owners. Subsequent revisions to this CPS might contain additional OID assignments than those identified above.

1.3 PKI PARTICIPANTS

The community governed by this CPS is the Surescripts PKI. The Surescripts PKI is established to support Surescripts customers needing to securely exchange information over the Internet. Participants are located in the United States of America. The following participants are applicable in the administration and operation of the Surescripts PKI:

1.3.1 SURESCRIPTS PKI MANAGEMENT

The management team of Surescripts has established the PKI, overseas and is responsible for governance of the PKI. This CPS is established under the authority and approval of Surescripts PKI management.

1.3.2 CERTIFICATION AUTHORITIES

1.3.2.1 ROOT CA

The Surescripts Root CA is a trust anchor for certificate holders of a PKI domain when the certificate holders act as the relying party. The Surescripts Root CA issues a CA signing certificate to the Surescripts CA. Additionally, the Surescripts Root CA issues signing certificates to multiple CAs.

The Surescripts Root CA creates, signs, and issues public key certificates to Surescripts Subordinate CAs to issue certificate holder certificates.

The Surescripts Root CA is the trust anchor for relying parties.

1.3.2.2 DIRECT CA

The Surescripts Direct CA is a Subordinate Issuing CA whose primary function is to issue certificates to the end entities for Direct messaging exchange. It does not issue certificates to other CAs with the exception of the cross-certificate to the DirectTrust Root CA.

1.3.2.3 CROSS CERTIFIED CA

A Cross-Certified CA is an organization that is operating a CA that has cross-certified with Surescripts through the Surescripts Direct CA. The DirectTrust CA is an example of a CA which has cross-certified with the Surescripts Direct CA.

1.3.2.4 ISSUING CA

The Surescripts Issuing CA is a Subordinate Issuing CA whose primary function is to issue certificates to the end entities for server and client authentication.

1.3.3 REGISTRATION AUTHORITIES

The Surescripts Registration Authority (RA) is a combination of people and system processes requests for certificates, collects and processes Subscriber information for verification. The RA collects and verifies identity information from Surescripts Subscribers using procedures that implement the identity validation policies set forth in this document. The RA is also augmented by the Surescripts Legal team to execute Subscriber Agreements (Business Associate Agreements) and Services Contracts that establish the legal relationship between verified healthcare entities, assigns terms for Trusted Agents, establishes the subscriber organization's (customer) healthcare status (as a BA or CE as described later) and their authorized representatives. The RA communicates with the CA on all matters prior to the issuance of a certificate, including, but not limited to Orgnization and Identity Vetting, certificate requests and any changes affecting the validity of certificates. This team is internal to Surescripts and uses internal systems only to communicate with the CA personnel in conjunction with their dutes. The

Surescripts Registration Authority (RA) is the only accredited RA for the Surescripts Certificaton Authority.

1.3.4 TRUSTED AGENTS

Trusted Agents are individuals who act on behalf of the Surescripts CA or RA to collect and/or verify information regarding Subscribers, and where applicable to provide support regarding those activities to the Subscribers. Trusted Agents SHALL be an Individual who, while not an employee of the CA or RA, has 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 (Identity Proofing and authorization to use certificate enabled healthcare services and systems) regarding Subscribers.

The CA or RA MAY provide the Trusted Agent with material to facilitate the activities being performed by the Trusted Agent on behalf of the CA or RA, including, but not limited to: software products, dedicated web pages, electronic or paper forms, instruction manuals, and training sessions.

All activities of the Trusted Agent SHALL be performed in accordance with this CPS.

1.3.5 SUBSCRIBERS, SUBJECTS AND APPLICANTS

A Surescripts Direct Subscriber is an entity who uses Direct services and PKI to support Direct transactions and communications. Subscribers are not the party identified in a certificate when Direct Organizational certificates are issued to a Health Domain address. Candidates Distinguished Name must be unique and linked to one legal entity per section 3.1.1. The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the subject of the certificate and the entity that contracted with the Surescripts CA for the certificate's issuance in accordance with this CPS. A Subscriber may contract a third party to manage their subscriptions; e.g. in the case of a *Group* certificate managed by a HISP, an authorized officer at the HISP is also a Subscriber and each Subscriber abides by the required Subscriber Agreements. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

1.3.5.1 CUSTODIAN

A Custodian acts in the capacity of an agent for the Subscriber for the purposes of enabling health information exchange by holding and managing Private Keys associated with a Certificate on behalf of that Subscriber in a Custodial Subscriber Key Store.

1.3.5.2 HEALTH INFORMATION SERVICE PROVIDERS (HISPS)

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

1.3.6 AFFILIATES

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

1.3.7 RELYING PARTIES

A Relying Party uses a Subscriber'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 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).

1.3.8 OPERATIONAL AUTHORITY (OA)

The Surescripts Operational Authority is the organization that operates and maintains the Surescripts Certificate Servers, including issuing certificates, posting those certificates and Certificate Revocation Lists (CRLs) into the Surescripts PKI Repository, and ensuring the continued availability of the repository to all users. The Trusted Role descriptions are in section 5.2.1.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The primary use for a Direct X.509 certificate, asserting a policy identifier other than the ss-tls policy, is in the exchange of electronic messages grounded in the specification of the Direct project. This includes S/MIME message signature verification and S/MIME message encryption. Certificates issued under this CPS are only used for the purposes designated in the key usage and extended key usage fields found in the certificate.

The primary use of certificate that asserts the ss-tls policy is the establishment and encryption of sessions employing TLS or MATLS communication.

However, each Relying Party must evaluate the application environment and associated risks before deciding on whether to accept a certificate issued by this CA for a particular transaction.

An Affiliate that is a healthcare provider or healthcare organization SHALL 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, except when the Covered Entity is providing services to or on behalf of the Business Associate.

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 stated level of assurance when the certificate was issued. Certificates issued under this Certification Practice Statement may not be used where prohibited by law.

Except as allowed in Section 1.4.1 above, all other uses of Certificates are prohibited. Without limiting the foregoing, Subscribers will not: (i) use Certificates on behalf of any other entity; (ii) sell or otherwise transfer the Certificate; (iii) copy, enhance, modify or decompile the Certificate (except as allowed by applicable law; or (iv) perform any public or private key operations with the Certificate or associated public key or private key with a name other than that in the Subject field in the Certificate.)

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

Information Security Compliance, in accordance with ISMS Document Management Standards is responsible for this CPS.

1.5.2 CONTACT PERSON

Questions regarding this CPS are to be directed to:

Certificate Policy Manager
Surescripts LLC
920 Second Avenue South
Minneapolis, MN 55402

Inquiries may be forwarded to certificate.services@Surescripts.com.

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE CERTIFICATE POLICY

Surescripts Information Security Compliance is responsible for maintaining CPS suitability and will ensure compliance between this CPS and the appropriate Direct CP (current v1.4), as well as compliance with Webtrust principles for mTLS certificates A review will be conducted during the policy amendment process.Third party services may be used to attest to this compliance.

1.5.4 CERTIFICATION PRACTICE STATEMENT APPROVAL PROCEDURES

When a change to this CPS is required, the Surescripts IS Compliance team will prepare the changes and request a meeting with the Surescripts PKI Management for review and subsequent revision approval.

The Surescripts CA submits this CPS to a compliance analysis and audit against each applicable CP as described in Section 8 of this CPS. The CA's CPS shall be required to meet all facets of its policy. The CA may not declare conformance with this CPS until the compliance analysis and audit is complete and all discrepancies resolved.

1.6 DEFINITIONS AND ACRONYMS

Table 1 Definitions and Acronyms

Term	Definition
Authentication	The process of establishing that individuals, organizations or things are who or what they claim to be.
CA	Certification Authority
CCB	Change Control Board (In this document, the term refers to the Surescripts Security Operations CCB.)
CP	Certificate Policy: a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements
CPS	Certification Practice Statement
CRL	See Certificate Revocation List
CSR	Certificate Signing Request
Certificate	Data structure that: 1) identifies the Certification Authority issuing it; 2) names or otherwise identifies its Subject and Subscriber; 3) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; 4) identifies its period of validity; and (5) contains a certificate serial number and is digitally signed by the CA issuing it.
Certificate Class	All the certificates issued under a particular named Certificate Policy.
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 Revocation List (CRL)	A list maintained by a Certification Authority of the certificates that it has issued which are revoked prior to their stated expiration date.
Certificate Signing Request (CRL)	A special data structure containing all the information necessary to request a digital certificate from a certification authority. Per the PKCS10 v1.7 standard: “A certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. Certification requests are sent to a certification authority, which transforms the request into an X.509 public-key certificate.”
Certification Authority (CA)	Entity that authorizes and issues a certificate. The CA: 1) identifies and authenticates the intended Subject to be named in the Certificate; 2) verifies that certain Subscribers possess the Private Key that corresponds to the Public Key that will be listed in the Certificate 3) creates and digitally signs the Certificate. For this Surescripts CA CPS, the Surescripts CA is the body responsible for generating and certifying the Public Key Certificates for the Surescripts business.
Certification Practice Statement (CPS)	Document that specifies practices a CA employs in issuing and revoking certificates.

Term	Definition
Confirm	To ascertain through appropriate inquiry and investigation.
DN	Distinguished Name
IA5String	ASN.1 notation representing a free text value
ID	Identity
IETF	Internet Engineering Task Force A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
ISSO	Information Systems Security Officer An individual responsible for establishing and maintaining the Systems Security enterprise vision, strategy and program as it relates to ensuring that Information assets are adequately protected.
LoA	Level of Assurance
Non-production	Describes a system, environment, subscriber, or relying party that does not interact or participate in a Surescripts business' Production environment.
Object Identifier	The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. A number that identifies an object's position in a global object registration tree.
OCSP	Online Certificate Status Protocol
OID	Object Identifier
Participants	An individual or organization that plays a role within the PKI for the Surescripts business as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.
Pass Phrase	A string of words and characters (usually 20 characters or more) that a user types into a computer to confirm his or her identity. A more secure form of a password or PIN.
PIN	Personal Identification Number that the Subscriber selects and uses to import the Private Key into its own software package.
PKI	See Public Key Infrastructure.
PKI Repository	A networked electronic information resource, available to Surescripts PKI Subscribers and Relying Parties, to which CA Certificates, CRLs, PKI policies, and related information can be published.
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.

Term	Definition
RA	See Registration Authority.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects. Component of a Surescripts CA that provides the user interface and business logic for issuing and administering user certificates.
Relying Party	Person who has received a Certificate and a digital signature verifiable with reference to a Public Key listed in the certificate, and who is in a position to rely on them.
Repository	Trustworthy system for storing and retrieving Certificates or other information relevant to Certificates.
Revoke a Certificate	Permanently end the operational period of a certificate from a specified time forward.
RFC	Request For Comments
Root CA	Top-level Certification Authority in a trust hierarchy.
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL Baseline Requirements	*Version 2.4.1 of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security*
Subject	The person or device that is the subject of a Certificate.
Subordinate CA	Lower-level Certification Authority in a trust hierarchy. Subordinate CA certificates are signed by the Root CA and are checked for authenticity against the Root CA.
Subscriber	A Subscriber is an entity that does not itself issue certificates to another party and is either (1) the subject named or identified in a certificate issued to that entity, or (2) holds, 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 the person or entity being issued Private Keys and/or Certificates under terms of this Surescripts CA CPS.
Surescripts CA	Body responsible for generating and certifying the Public Key certificates for the Surescripts Direct business.
Surescripts PKI	The PKI developed for the Surescripts Direct business.
Surescripts Security Operations	Surescripts Security Operations is the organizational unit responsible for developing and maintaining the Certification Authority and other Surescripts PKI entities.
Surescripts Security Operations CCB	The Surescripts Security Operations Change Control Board (CCB) is the organizational unit responsible for ensuring Surescripts Security Operations develops the PKI according to requirements
Trustworthy System	Computer hardware, software, and procedures that: 1) are reasonably secure from intrusion and misuse; 2) provide a reasonably reliable level of availability, reliability, and correct operation; 3) are reasonably suited in performing their intended functions; 4) adhere to generally accepted security principles.
URI	Universal Resource Identifier

Term	Definition

SECTION 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The Surescripts CAs and RAs operate repositories in support of operations required by this CPS and CP. The CA ensures that its root certificate and the revocation data for issued certificates are available through an externally-facing repository. All other documentation such as subscriber agreements are confidential and maintained in internal repositories.

2.1.1 REPOSITORY OBLIGATIONS

The repositories holding certificate status data are operated 24 hours a day, 7 days a week within an active cluster with a high availability expectation to exceed 99% availability overall per year.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

The Surescripts CA maintains a Certificate Revocation List (CRL) and exposes its location in the CRL Distribution Points X.509v3 extension. The Surescripts CA maintains an equivalent Online Certificate Status Protocol (OCSP) Responder and expose its location in the Authority Information Access X.509 extension. This is done in accordance with the relevant Sections within 4.9 and 7.3.

CA and End Entity certificates contain valid Uniform Resource Identifiers (URIs) that are accessible by Relying Parties. The CA publishes its CA certificate and any other intermediate or trust anchor certificates necessary to validate the Surescripts CA.

The publicly accessible directory system shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

The certificate status server (CSS) shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

2.2.2 PUBLICATION OF CA INFORMATION

The Surescripts CA freely publishes its Surescripts CA Certification Practices Statement(CPS) and information concerning the CA necessary to support its

operation and use for customer subscribers. Information on how to obtain a copy of its CPS shall be provided to any party with legitimate interest.

2.2.3 INTEROPERABILITY

No stipulation.

2.3 FREQUENCY OF PUBLICATION

The Surescripts CPS and any ensuing changes, shall be made publicly available within 14 days of approval through the Surescripts consensus process.

This Surescripts CA Certification Practice Statement (CPS) is considered proprietary and confidential to Surescripts and will be published internally and available only to parties contracted for services.

CRLs expire every 7 days or less and must be updated immediately when a new entry is added to it, or every 7 days, whichever is earlier.

2.4 ACCESS CONTROLS ON REPOSITORIES

The Surescripts CA and RA protect repository information not intended for public dissemination or modification. The Surescripts CA provides unrestricted read access to its repositories for legitimate uses and has implemented logical and physical controls to prevent unauthorized write access to such repositories.

The Surescripts CA and RA repository is instantiated within the Microsoft Active Directory Certificate Services platform. This repository can only be modified by the Surescripts CA application or authorized representatives.

SECTION 3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

All Organizational certificates use non-null and unique DN name forms for the Issuer and Subject names. Non-unique DN names will fail in the certificate issuance process. As specified in the published document “Direct Project Applicability Statement for Secure Health Transport v 1.2”, certificates tied to full Direct addresses (“Address certificates”) contain the Direct address in the subjectAltName extended attribute as an rfc822Name. Certificates tied to a Direct domain (“Organizational certificates”) contain the domain name in two places:

1. The subjectAltName extension formatted as a DNSName, and

2. The CN of the Subject DN.

The subjectAltName extension and Subject Common Name (CN) field may not contain reserved IPs or internal server names. Any existing certificates with such extension or field settings will be revoked by October 2016.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

Names used in certificates uniquely identify the organization or person to which they are assigned and are easily understood by humans. RA and CA Officers are responsible for verifying prior to Certificate issuance.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

This CA does not issue anonymous certificates. Pseudonymous certificates are issued when the name space uniqueness requirements are met.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

No stipulation.

3.1.5 UNIQUENESS OF NAMES

The OA enforces name uniqueness of the certificate subject DN within the CA's X.500 namespace. Our CA Systems are configured to confirm that the requirements for unique Subject DN values for different end entities are met before allowing a Certificate to be issued.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Subscribers cannot request certificates with any content that infringes the intellectual property rights of another entity. This CA will reject any application or require revocation of any certificate that is part of a trademark dispute.

This CA will implement a process to prevent any certificate attributes from including a name, DBA (doing business as"), trade name, trademark, address, location, or other text that refers to a specific or natural person or Legal Entity unless the CA has verified this information. Initial Identity Validation

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

All CSRs provided by subscribers must be signed by the private key for which the certificate is to be issued.

In cases when the private key is generated by the Surescripts RA/CA; no additional proof of private key possession is required.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Table 2. Authentication requirements

Certificate	Validation
Organizational Certificates for Direct Messaging	Requests for organizational certificates for Direct messaging include the Legal organization name, mailing address, and a Clinical Interoperability Agreement and Business Associate Agreement that verifies of the existence of the organization as well as the requested domain name that will appear in the certificate (see section 3.1.1 for details). For Address-Bound and Domain-Bound Certificates, the requested Health Domain Name or Health Endpoint Name that will appear in the Certificate MUST also be included. The requesting organizations are qualified in one of the following categories: • HIPAA Covered Entity. • HIPAA Business Associate The RA verifies the applicant organization's healthcare category in submitted request for certificates in accordance with the process established in this CPS that the requesting organization MUST be a legally distinct entity.
	Category requirements for Healthcare Organizations

DT.org CE	Applicant represents that it is a Covered Entity as defined in HIPAA. Such verifications required by the Registration Authority functions shall ensure contracts are in place, thereby vetted by the Legal team, that indicate the validity and Healthcare Category as required for certificate issuance. The RA also verifies the organization information submitted, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.
DT.org BA	Applicant represents that it will limit its use of any Digital Certificate issued to it pursuant to the CPS for purposes required in its capacity as a Business Associate (BA), as defined in HIPAA. The RA will confirm that such representation has been made in an appropriate legally binding agreement vetted by the Legal team Relying Parties may be required by government statute or regulations to have additional agreements in place with the BA.
DT.org HE	NOT SUPPORTED. Applicant represents in a statement, such as a signed Certificate application, that it is a Non-HIPAA Healthcare Entity (HE),
DT.org Non-Declared	NOT SUPPORTED.
Certificate	**Validation**
Surescripts TLS Certificates	If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then the CA SHALL verify the country associated with the Subject using a verification process meeting the requirements of *Version 2.4.1 of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security* 4.2 and If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then the CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of this section and that is described in the CA's Certificate Policy and/or Certification Practice Statement in section 3.2. The CA SHALL inspect any document relied upon under this section for alteration or falsification.
	Subject Identity If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following: 1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition; 2. A third party database that is periodically updated and considered a Reliable Data Source; 3. A site visit by the CA or a third party who is acting as an agent for the CA; or 4. An Attestation Letter or contractual agreement. The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

	Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable
	DBA/Tradename If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following: 1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition; 2. A Reliable Data Source; 3. Communication with a government agency responsible for the management of such DBAs or tradenames; 4. An Attestation Letter accompanied by documentary support; or 5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.
	Individual Applicant If an Applicant is a natural person, then the CA SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request. The CA SHALL verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA SHALL inspect the copy for any indication of alteration or falsification. The CA SHALL verify the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. The CA MAY rely on the same government issued ID that was used to verify the Applicant's name. The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.
	Country If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following: (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; (c) information provided by the Domain Name Registrar; or (d) *Version 2.4.1 of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security*2.15 The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

An organization's identity may be considered authenticated for purposes of an Application if the same organization's identity has been previously authenticated in conjunction with another Certificate issued by us, and that Certificate is valid at the time of Application approval, the information in the previous Certificate relating to the organization matches the information in the current Application, and the individual submitting the Application on behalf of the organization has been authenticated according to the requirements of CPS § 3.2.3.1

at a level of assurance equal to or higher than the level of assurance requested on the Application.

If a certificate asserts an organizational affiliation between a human Subscriber and an organization (e.g. Direct Organizational Certificates), the Surescripts RA or CA obtains authoritative documentation from the organization that recognizes the affiliation and obligates the organization to provide updates on Subscribers' access to Group certificates where applicable or to request modification or revocation of the certificate where necessary, if that affiliation ends. See Sections 3.2.3.3, 4.9.1 and 9.6.1.

> **NOTE**: Certificates asserting an organizational affiliation may also assert the OID corresponding to that organization's healthcare category.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

3.2.3.1 AUTHENTICATION OF HUMAN SUBSCRIBERS

Validation of the identity of an individual is required in several cases:

(1) To verify the identity of a representative of an organization requesting a Direct Organizational certificate;

(2) To verify the identity of an Information Systems Security Officer (ISSO) (or equivalent) at the organization physically controlling the private key in the case of a Group certificate;

(3) To verify the identity of an individual requesting a Direct Address certificate.

Identity proofing LoAs are intended to provide equivalent assurances to identity proofing LoAs as defined by NIST SP 800-63-2. The following table includes the LoA's supported by Surescripts. At a minimum, the CA or the RA SHALL proof an individual's identity in accordance with one of the following LoAs:

Table 3. Levels of Assurance for Identity Verification Requirements

DT.org LoA 2 (Equivalent to NIST 800-63-2 Level 2)	Applicant supplies his or her full legal name, an address of record, and date of birth. **For In-Person vetting**: the applicant also provides valid government issued photo ID. **RA** inspects photo ‐ ID; compares picture to Applicant; and records the ID number, address and date of birth (DoB). **CA** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records – or – confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in the records – or – sends notice to claimed address after issuance. **For Remote vetting**: the applicant provides valid government issued PhotoID identifier + a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID or account. **RA** inspects both ID and account numbers supplied (e.g. for correct number of digits) and verifies either the ID number OR the account number information provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. (For utility or financial account numbers, confirmation may be performed by verifying knowledge of recent account activity, when applicable). **CA** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records – or – confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in the records – or – sends notice to an address confirmed in the records check after issuance. Any of the identity verification methods listed for a higher level is also acceptable.

DT.org LoA 3 (Equivalent to NIST 800-63-2 Level 3)	Applicant supplies his or her full legal name, an address of record, and date of birth. **For In-Person vetting**: the applicant also provides valid government issued photo ID. The **RA** inspects the photo-ID and records the ID number; compares picture to Applicant; and verifies information provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application. The **CA** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications at phone number associated with the Applicant in records – or – confirms the ability of the Applicant to receive mail at the claimed address– or – sends notice to the confirmed physical address associated with the Applicant in the records after issuance. If the telephone method is used, CA also records Applicant's voice or uses alternative means that establish an equivalent level of non-repudiation. **For Remote vetting:** the applicant provides valid government issued Photo ID identifier and a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID and account. **RA** verifies both ID and account numbers provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application. (For utility or financial account numbers, confirmation may be performed by verifying knowledge of recent account activity, when applicable). The **CA** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or email address associated with the Applicant in records – or – confirms the ability of the Applicant to receive mail at a physical address associated with the Applicant in the records. Any of the identity verification methods listed for a higher level is also acceptable.

In-Person vetting for LoA 2, LoA 3 and LoA4 MAY be performed by the RA, Trusted Agent of the RA, or an entity certified by a State or Federal Entity as being authorized to confirm identities. A trust relationship between the Trusted Agent and the Applicant which is based on an in-person antecedent MAY suffice as meeting the In-Person identity vetting requirements for LoA 2, LoA 3 or LoA 4.

If the requested Surescripts Direct digital certificate is to be used by a patient (currently not supported) or on behalf of a patient, the RA verifies the patient identity with the process established at Section below:

DT.org Patient	Applicant represents that any Surescripts Digital Certificate issued pursuant to its CP will be used for their personal healthcare Surescripts Direct message exchange purposes.

	The **RA** verifies that the patient or the patient's authorized representative has made this representation.

3.2.3.2 3.2.3.2 AUTHENTICATION OF HUMAN SUBSCRIBERS FOR ROLE-BASED CERTIFICATES

We do not issue role-based Certificates.

3.2.3.3 AUTHENTICATION OF HUMAN SUBSCRIBERS FOR GROUP CERTIFICATES

A Group Certificate corresponds to a credential with a private key that is shared by multiple entities. A Direct digital certificate that is held and managed by a Health Information Service Provider (HISP) on behalf of a Subscriber organization is an example of a group certificate. Identity Verification of the Subscriber organization and its representative is covered in sections 3.2.2 and 3.2.3.1.

For HISP managed group certificates, the RA also records the information identified in Section 3.2.3.1 for the Information Systems Security Officer (or equivalent) of the HISP, before issuing the certificate.

In addition to the authentication of the Subscriber (and their organization when required), the following procedures are performed:

- The HISP Information Systems Security Officer or equivalent is responsible for ensuring control of the private key, including maintaining a list of any Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.
- The subjectName DN does not imply that the subject is a single individual.
- The Custodian (e.g. HISP) ISSO or equivalent SHALL maintain a list of those holding the shared Private Key that must be provided to, and retained by, the applicable CA or its designated representative.

Users MUST be identity proofed at a level corresponding to the LoA asserted in the Certificate. If the identity proofing component is performed by the Subscriber Organization, then the compliant RA MUST retain documentation that the Subscriber Organization is bound through a legally binding contract with or an attestation to the RA to identity proof Users in accordance with the requirements corresponding to the LoA of the associated Certificate. This information MUST be made available by the Subscriber Organization to the RA upon request.

The Subscriber may be able to leverage its existing relationship as an employer or affiliate of a User to meet the identity verification requirements. For example, Federal Employment Eligibility Verification Form I-9 may be sufficient, either alone to meet LoA 2, or with supplemental verification of submitted information to meet LoA 3 requirements.

3.2.3.4 AUTHENTICATION OF DEVICES

Not supported.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

All Subscriber information placed in a Surescripts CA certificate uses pre-completed templates and is verified by the RA within the application process. Non-verified Subscriber information SHALL NOT be included in a Certificate.

3.2.5 VALIDATION OF AUTHORITY

The Surescripts RA verifies the association between an organization requesting an organizational certificate and the individual representing the organization.The Subscriber is responsible for any information provided by their agent to us and must promptly notify us of any misrepresentations or omissions made by their agent. The RA or a Trusted Agent will verify that a representative is authorized to act on behalf of and as an agent of the Applicant. For organizations, this authorization may be submitted by an officer, owner, or other authorized official of the organization. Organization's will designate personnel to work with Surescripts to implement certificates in accordance with the appropriate Surescripts Implementation Guides and other Surescripts materials in accordance with legally contracted services.

We may use any means of communication at our disposal to ascertain the identity and authority of an organizational or individual Applicant or their representative. Identity Proofing of organizational representatives in accordance with 3.2.3 will be performed for net new customers.

Surescripts SHALL validate each Fully-Qualified Domain Name (FQDN) listed in the Certificate by using any qualified method of confirmation. For MATLS or TLS certificates, Surescripts will maintain documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the Fully Qualified Domain Name (FQDN).

3.2.6 CRITERIA FOR INTEROPERATION

To be deemed a conforming Surescripts Issuing CA, the CA issues certificates according to the Surescripts Certificate Policy.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY CERTIFICATE

Re-Key or modification is currently not supported. All certificates are issued new using the same process. Subscribers with a valid certificate, are not required to go through initial identity verification if certificates are issued using the same DN and certificate information.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

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

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

All revocation requests are authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised. Revocation requests must come through Surescripts support and a case opened in Salesforce for the organization request. Revocation requestors are indisputably identified and authenticated as a responsible party of the subscriber organization by verifying them as an employee of the subscriber organization’s support or business team. Other requestors must manage their case for a revocation working with their Surescripts support liaison.

SECTION 4 CERTIFICATE LIFE-CYCLE

4.1 APPLICATION

This section specifies practices for the initial application for a Surescripts CA certificate.

4.1.1 SUBMISSION OF CERTIFICATE APPLICATION

The certificate application or CSR is submitted to the CA/RA in the beginning stages of implementation for Surescripts connectivity or the initiation of any Direct messaging projects. For all certificates, a Subscriber, or its Custodian/Affiliate, creates the official certificate request based on input received from the Subscriber as validated by the CA/RA during the identity verification process. Applications may be submitted by applicant's authorized representatives once the contracting process and business associate agreements are executed. Personnel are designated by the subscriber organization to Surescripts teams supporting the onboarding of new services. Information collected and validated is covered in 3.2.2.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

A Subscriber is responsible for providing accurate information about themselves and the organization when submitting the certificate request. Identity validation is performed in accordance with section 3.2.3 of this CPS prior to the issuance of a certificate. The Surescripts CA/RA authenticates and protects all internal communication made during the certificate application and approval process. Communication must be made on internal networks or utilizing encrypted VPN sessions.

4.2 CERTIFICATE APPLICATION PROCESSING

The Surescripts CA/RA are responsible for verifying that the information in a certificate request is accurate and reflect the information presented by the Subscriber.

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The identity verification of Subscribers is done by the Surescripts CA/RA as specified in section 3.2

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

A certificate application may be rejected by the Surescripts CA/RA due to missing or inaccurate information. The Surescripts Operational Authority retains the right to reject Direct certificate applications if, in its judgment, the requesting individual or organization does not have a legitimate reason to possess a Direct certificate.

4.2.3 TIME TO PROCESS CERTIFICATION APPLICATIONS

All Subscriber information placed in a Surescripts certificate is verified and a certificate issued within 30 days of completion of verification.

4.2.4 REVIEW OF CAA RECORDS

Surescripts must review CAA records as part of the certificate approval process for mTLS certificates. DNS entries for FQDN's are verified through registered internet domain record sources as appropriate.

As part of the mTLS issuance process, the Surescripts MUST check for a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued. If found, follow the processing instructions set down in RFC 6844 for any records found.

4.3 ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

The Surescripts CA ensures that the public key is bound to the correct Subscriber and generates the certificate. The Surescripts CA publishes the certificate as specified in section 4.4.2.

The Surescripts CA performs all its actions during the certificate issuance process within a perimeter-protected network using encrypted transmissions. The RA personnel may enter certificate request information into the secured certificate creation portal or for Direct certificates, information is entered into the Direct certificate processing system.

4.3.2 NOTIFICATION TO SUBSCRIBER OF CERTIFICATE ISSUANCE

The Subscriber is notified via e-mail that his certificate has been issued. All certificate issuance is facilitated by the Surescripts teams responsible for assisting Subscribers that are implementing solutions that use certificates.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Certificates are published in the Direct Messaging repository and testing is conducted to ensure Direct messages are being sent and received successfully. Failure to object to the certificate or its contents, or actual use of the Certificate, constitutes the Subscriber's acceptance of the certificate.

All SSL Certificate (mTLS) Subscribers are required to sign a Subscriber Agreement Form which stipulates the terms of certificate acceptance and use. The signing of this form and the use of the credential is considered certificate acceptance.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The Surescripts CA makes its certificates available to the public using Microsoft's Lightweight Directory Access Protocol (LDAP).

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

Subscribers, or their authorized Custodian representatives (e.g. Surescripts as a HISP), who take possession of their subscriber Private Key, SHALL protect it from access by unauthorized parties and SHALL use the Private Keys only as specified by the *certificatePolicies* and *keyUsage* extensions of the corresponding Certificate. Private keys for Direct are held and managed exclusively by Surescripts (HISP).

mTLS certificate subscribers are required to sign a Subscriber Agreement which stipulates the terms of certificate usage, acceptance of operational requirements for certificate issuance and private key security, including, protecting it from access by unauthorized parties and using their certificate and key pair as specified in the key usage extension of the corresponding Certificate.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Surescripts certificates conform to the policies provided by this CPS and the Direct CP (for Direct Certificates). Relying parties should review this document and understand those policies. The Surescripts CA publishes a certificate revocation

list (CRL) and maintains an OCSP Responder. Relying parties need to process the CRL on a regular basis and reject certificates found on it and/or respect the certificate status reflected in an OCSP response.

4.6 CERTIFICATE RENEWAL

Certificate renewal is not allowed at this time.

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Certificate renewal is not allowed at this time.

4.6.2 WHO MAY REQUEST RENEWAL

Certificate renewal is not allowed at this time.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

Certificate renewal is not allowed at this time. Certificates expire and new certificates are issued.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Notification of Certificate issuance follows the manual process defined in Section 4.3.2

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Certificate renewal is not allowed at this time

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

Certificate renewal is not allowed at this time

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No stipulation.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate will be assigned a different validity

period, key identifiers, specify a different CRL distributionPoint or OCSP Responder location, and/or be signed with a different key. Re-key of a certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness.

After certificate re-key, the old certificate is not be revoked, but is not further re-keyed, renewed, or modified.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

A certificate is re-keyed before it's the end of its validity period and when no other information besides its keys and validity period are changing. A revoked certificate is not re-keyed.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

A Surescripts RA or the Subscriber or their authorized representative may request the re-key of a Subscriber certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

The Surescripts RA approves or rejects Subscriber certificate re-keying requests. Identity verification of the Subscriber is equivalent to the initial identity verification.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See section 4.3.2.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

See section 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

See section 4.4.2.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See section 4.4.3.

4.8 MODIFICATION

Certificate modification is not allowed at this time.

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

Certificate modification is not allowed at this time

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Certificate modification is not allowed at this time

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Certificate modification is not allowed at this time

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See section 4.3.2.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

See section 4..0000.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

See section 4.4.2.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 CIRCUMSTANCES FOR REVOCATION

A certificate is revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate become invalid,
- The Subscriber can be shown to have violated the stipulations of its Subscriber agreement, or
- The private key is suspected of compromise, and the Subscriber asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate is revoked, placed on the certificate revocation list (CRL) and has its revoked status reflected in OCSP responses.

4.9.2 WHO CAN REQUEST REVOCATION

The RA or OA may request revocation of a certificate, or it may entertain requests from a Subscriber or their authorized representative to revoke a certificate in accordance with 4.9.3.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Any request for certificate revocation identifies the certificate to be revoked by serial number and explains the reason for revocation. A Surescripts RA and CA shall ensure that the certificate revocation request is not malicious and will verify that the reason for revocation is valid. If the reason for revocation is valid, the Surescripts CA will place the certificate's serial number and any other required information on its certificate revocation list (CRL) and/or have its revoked status reflected in OCSP responses.

Subscribers (customers) may request revocation of a certificate for problems related to fraud, misuse, or compromise by filing a "Certificate Problem Report" to Customer Support who will process the request to the CA/RA personnel. Surescripts customers should follow the appropriate support procedure or open a self-service support ticket at surescripts.com.

4.9.4 REVOCATION REQUEST GRACE PERIOD

There is no grace period for revocation under this CPS. Subscribers and authorized PKI entities request the revocation of a certificate as soon as the need for revocation comes to their attention.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

Surescripts will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party.

4.9.7 CRL ISSUANCE FREQUENCY

The Surescripts CA CRL is issued and posted to the repository listed in section 2.2.1 every 7 days even when there are no changes or updates to be made to ensure timeliness of information. A CRL may be issued more frequently than every 7 days if new entries are made to the CRL. The Surescripts CA ensures that superseded CRLs are removed from the public repository upon posting of the latest CRL.

Certificates will be revoked as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published. Exceptiong those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

4.9.8 MAXIMUM LATENCY OF CRLS

CRLs are posted upon generation but within no more than four hours after generation. Furthermore, a new CRL is published no later than the time specified in the nextUpdate field of the most recently published CRL.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

The Surescripts CA deploys an Online Certificate Status Protocol (OCSP) responder. Status information must be updated and available to relying parties within 18 hours of certificate revocation. See section 2.2.1 for repository information.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

No stipulation.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No other form of revocation advertisement is required.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

No stipulation.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

The Surescripts CA does not support suspended certificates.

4.9.14 WHO CAN REQUEST SUSPENSION

No stipulation.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

No stipulation.

4.9.16 LIMITS ON SUSPENSION PERIOD

No stipulation.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

The status of public certificates is available via a CRL or OCSP responder. These services are included in an high availability (HA) cluster where reponders are available concurrently in multiple data center locations.

4.10.2 SERVICE AVAILABILITY

Certtificate Status Services are available 24 X 7 without scheduled interruption.

4.10.3 OPTIONAL FEATURES

OCSP is an optional status service that is available.

4.11 END OF SUBSCRIPTION

Certificates that have expired prior to or upon end of subscription are not required to be revoked. A Subscriber with an unexpired certificate who is no longer using the certificate in an approved manner (e.g., for Surescripts secure communications) should have his certificate revoked.

4.12 KEY ESCROW AND RECOVERY

Not supported.

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

No stipulation.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation. Not supported.

SECTION 5 FACILITY MANAGEMENT AND OPERATIONS CONTROLS

5.1 PHYSICAL CONTROLS

Surescripts has implemented commercially sound, security controls in order to protect its CA from environmental, physical and other threats.

5.1.1 SITE LOCATION AND CONSTRUCTION

The Surescripts CA components are housed within a commercially contracted data center grade environment that deters, prevents and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

5.1.2 PHYSICAL ACCESS

Access to the Surescripts data center is restricted by magnetic key card and biometric readers. Entry is restricted to authorized CA Administrators personnel only and controlled by Surescripts Operations.

- Physical access to CA infrastructure requires approved data center access for appropriate Administrators.
- All changes must be authorized in accordance with Surescripts Change Management Policies, Standards, and Procedures.

The Surescripts CA private keys are protected by FIPS 140-2 level 3 Hardware Security Modules.

5.1.3 POWER AND AIR CONDITIONING

The Surescripts CA utilizes the same power and cooling protection as other Surescripts critical systems. This includes:

- power systems to ensure continuous, uninterrupted access to electric power, sufficient for a minimum of 6 hours operation in the absence of commercial power, and
- heating and air conditioning systems to control temperature and relative humidity

5.1.4 WATER EXPOSURES

The Surescripts CA has systems in place to minimize the impact of water exposure on any Surescripts CA component. The same safeguards protect other Surescripts critical systems.

5.1.5 FIRE PREVENTION AND PROTECTION

The Surescripts CA is protected by systems designed to prevent and extinguish fires and/or prevent damage from exposure to flame or smoke. These systems have been designed to comply with local fire safety regulations.

5.1.6 MEDIA STORAGE

All media containing production data or software related to the Surescripts CA is housed within Surescripts facilities or in secure off-site storage facilities with appropriate physical and logical controls designed to limit access to unauthorized personnel and to provide protection against accidental damage.

Media located within the Surescripts campus is controlled by the Surescripts Security Operations team.

5.1.7 WASTE DISPOSAL

Any media containing unencrypted critical data is disposed of by erasure or destruction, as specified in the DoD National Industrial Security Program Operating Manual (NISPOM).

5.1.8 OFF-SITE BACKUP

The Surescripts CA routinely performs backups of critical system data, audit log data, and other sensitive information. Backup procedures are addressed within individual Disaster Recovery plans: Clinical Interoperability DR plan (Direct) and PKI Failover procedures.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

5.2.1.1 ADMINISTRATOR

The administrator role is responsible for:

- Installation, configuration, and maintenance of the CA.

- Establishing and maintaining CA system accounts.
- Configuring certificate profiles or templates, audit parameters, generating and backing up CA keys.
- Administration of the PKI infrastructure, the certificate management system console, software installation or configuration, and the support of the Hardware Security Modules.
- Administrators do not issue certificates to Subscribers.

5.2.1.2 OFFICER

The officer role is responsible for:

- Registering new Subscribers and requesting the issuance of Certificates.
- Verifying the identity of Subscribers and accuracy of information included in Certificates.
- Approving, Requesting and executing the issuance or revocation of Certificates.
    - Certificate renewal and revocation requests may come in through the Customer Service Support team or other operational support teams. Such requests will be forwarded to the appropriate team for action.

5.2.1.3 AUDITOR

The auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs.
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS.

5.2.1.4 OPERATOR

The CA operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

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

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

A person occupying a Trusted Role SHALL authenticate himself to the CA or RA system. Active Directory and the appropriate AD domain authentication shall be used for all administrative and priviledged activities.

5.2.4 SEPARATION OF ROLES

Due to the multiple individuals required for tasks, a single individual may be assigned multiple roles unless stated otherwise here. Any individual MAY assume the Operator role. No one individual SHALL assume both the Officer and Administrator roles.

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, and must be U.S. citizens or cleared to wok in the US. Trusted roles are Identity Proofed at the highest LoA commensurate with the systems working with.

Qualifications: Surescripts CA personnel are experienced with PKI concepts and standards, and security best practices.

Experience: Surescripts CA operational and support personnel are experienced with system and applications administration, cryptographic systems management, and security policies and procedures.

Clearance: Surescripts CA personnel are cleared for each role they fill as appointed by Operations Management or Information Security.

5.3.2 BACKGROUND CHECK PROCEDURES

CA personnel shall, at a minimum, pass a background investigation in accordance with Surescripts Human Resources, covering the following areas:

- Employment;
- Education;
- Ability to work in health care;
- Law Enforcement;
- Other checks, as required.

5.3.3 TRAINING REQUIREMENTS

All Surescripts CA personnel are required to complete all Surescripts employee training required of trusted employees, as well as training on this Surescripts CA CPS. All personnel operating in Surescripts CA specific roles are also required to be trained, according to their roles, in related Certificate Policies, the Surescripts CA applications, the Surescripts CA HSM, and related operating procedures.

Officers receive job specific training by the Integration Team management. Job rotation is not recommended at any frequesncy due to training requirements. Annual validation specialist training is conducted during team meetings to review certification and validation processes and procedures

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Individuals responsible for Trusted Roles are aware of changes in CA operation. If Surescripts operations change, Surescripts will provide a training (awareness) plan, and the execution of such plan is documented. Documentation is maintained identifying all personnel who received training and the level of training completed.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

Surescripts takes appropriate administrative and disciplinary actions against personnel who violate this CPS. Sanctions for unauthorized actions on, or affecting, the Surescripts CA may range from reprimand and corrective re-training to termination and possible criminal prosecution according to internal Surescripts Security and Privacy Sanctions Standard.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Independent contractors will be subject to same qualification, clearance, experience and training requirements as employees.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Surescripts CA personnel are supplied with copies (physical or electronic) of the Surescripts CA CPS and access to Surescripts CA system, application, and operations documentation, as well as standard documentation provided to Surescripts personnel.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CA. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 TYPES OF EVENTS RECORDED

Each audit record includes the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator, where appropriate
- The identity of the entity and/or operator (of the Issuing CA) that caused the event

Detailed audit information collected is listed in the table below. All security auditing capabilities of the Issuing CA operating system and CA applications required by this CPS are enabled. As a result, most of the events identified in the table are automatically recorded. Where events cannot be automatically recorded, the Surescripts CA implements manual procedures.

Table 4. PKI Auditable Events

Auditable Event	
SECURITY AUDIT	• Any changes to the audit parameters, e.g., audit frequency, type of event audited • Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS	• Successful and unsuccessful attempts to assume a role • The value of maximum number of authentication attempts is changed • Maximum number of unsuccessful authentication attempts reached during user login • An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts • An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY	• All security-relevant data that is entered in the system
REMOTE DATA ENTRY	• All security-relevant messages that are received by the system

Auditable Event	
DATA EXPORT AND OUTPUT	• All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION	• Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE	• The loading of Component Private Keys • All access to certificate subject Private Keys retained within the CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE	• Any change to the trusted public keys, including additions and deletions
SECRET KEY STORAGE	• The manual entry of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT	• The export of private and secret keys (keys used for a single session or message are excluded)
CERTIFICATE REGISTRATION	• All certificate requests, including issuance, re-key, and renewal • Certificate issuance
CERTIFICATE REVOCATION	• All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL OR REJECTION	• Certificate status change approval or rejection
CA CONFIGURATION	• Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION	• Roles and users are added or deleted • The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT	• All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT	• All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	• All changes to the certificate revocation list profile
TIME STAMPING	• A third party time stamp is obtained

Auditable Event	
MISCELLANEOUS	• Appointment of an individual to a Trusted Roleel for multiparty control • Designation of person • Installation of an Operating System • Installation of a PKI Application • Installation of a Hardware Security Module • Removal of a Hardware Security Module • Destruction of a Hardware Security Module • System Startup • Logon attempts to PKI Application • Receipt of hardware / software • Attempts to set passwords • Attempts to modify passwords • Backup of the internal CA database • Restoration from backup of the internal CA database • Posting of any material to a repository • Access to CA internal database • All certificate compromise notification requests • Loading tokens with certificates • Shipment of tokens • Zeroizing HSMs • Re-key of the Component
CONFIGURATION CHANGES	• Hardware • Software • Operating System • Patches • Security profiles
PHYSICAL ACCESS / SITE SECURITY	• Personnel access to room housing CA • Access to the CA server • Known or suspected violations of physical security

Auditable Event	
ANOMALIES	• System crashes and hardware failures • Software error conditions • Software check integrity failures • Receipt of improper messages • Misrouted messages • Network attacks (suspected or confirmed) • Equipment failure • Electrical power outages • Uninterruptible power supply (UPS) failure • Obvious and reported network service or access failures • Violations of a CP or CPS • Resetting Operating System clock

5.4.2 FREQUENCY OF PROCESSING LOG

The Surescripts CA logs are rolled daily (the previous day's logs are archived and a new log is begun). Auto-vetting log files are rolled when they reach or exceed a preset size, for example, one megabyte. System log roll-over is controlled by configuration settings managed by the system administrators. Archived log files are processed monthly.

5.4.3 RETENTION PERIOD FOR AUDIT LOGS

Security audit log data are available on the CA equipment for a minimum of two months.

5.4.4 PROTECTION OF AUDIT LOGS

Only authorized personnel (CA administrators and auditors) have access to the logs, and only authorized personnel archives the logs. CA configuration and access control processes enforce these requirements.

5.4.5 AUDIT LOG BACKUP PROCEDURES

Security audit data are backed up at least monthly and stored off-site in a redundant CA repository maintained in a data center grade environment.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

All security audit processes are invoked at CA startup and cease only at shutdown. Should it become apparent that an automated security audit system has failed; the

CA ceases all operation except for revocation processing until the security audit capability can be restored.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this CPS.

5.4.8 VULNERABILITY ASSESSMENTS

A formal vulnerability assessment was used to guide the design of the Surescripts CA systems and their security controls and safeguards.

Periodic vulnerability assessments are conducted at least annually.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF EVENTS ARCHIVED

CA archive records are sufficiently detailed as to verify that the CA was properly operated as well as to verify the validity of any certificate throughout its validity period. Records required to be archived are created and stored electronically by the event (system or process) used to create such records. At a minimum, the following data is archived for the retention specified :

1. Any accreditation of the Issuer CA.

2. CP and CPS versions.

3. Contractual obligations and other agreements concerning the operation of the CA.

4. System and equipment configurations, modifications, and updates.

5. Certificate and revocation requests.

6. Identity authentication data.

7. Any documentation related to the receipt or acceptance of a certificate or token.

8. Subscriber Agreements.

9. Issued certificates.

10. A record of certificate re-keys.

11. CRLs.

12. Any data or applications necessary to verify an archive's contents, 13 months.
13. Compliance auditor reports.
14. Any changes to the Issuer CA's audit parameters.
15. Any attempt to delete or modify audit logs.
16. Key generation (excluding session keys).
17. Access to Private Keys for key recovery purposes.
18. Changes to trusted Public Keys.,
19. Export of Private Keys.
20. Approval or rejection of a certificate status change request.
21. Appointment of an individual to a trusted role.
22. Destruction of a cryptographic module.
23. Certificate compromise notifications.
24. Remedial action taken as a result of violations of physical security.
25. Violations of the CP or CPS.

5.5.2 RETENTION PERIOD FOR ARCHIVE

CA archives are retained for 6 years, minimum. Certificate and key operations information is stored for 3 years, minimum. Information system and security audit logs for system activity are maintained as listed in 5.4.3 and archived for 13 months.

5.5.3 PROTECTION OF ARCHIVE

Only authorized individuals are permitted to add to or delete from the archive. Archive media are stored in a separate, safe, secure storage facility.

5.5.4 ARCHIVE BACKUP PROCEDURES

CA/RA servers are subject to a common server backup procedure using data protection software and used for all server assets within the enterprise. This includes a weekly FULL backup that is retained for 30 days. This is same backup procedure for any of the items mentioned in 5.5.1 as are archived to file server shares. Data repositories are configured with redundant architectures that utilized synchronized copies of data in 2 data centers for high availability and reliability.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

As they are created, CA archive records are automatically time-stamped using a trusted time service provided by Network Time Protocol.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

No stipulation.

5.5.7 PROCEDURES TO OBTAIN & VERIFY ARCHIVE INFORMATION

All CA/RA data archived can be browsed for validation|restore using the related system referencing document timestamps for modification. Documents stored in file systems are dated, are backed up and recoverable.

5.6 KEY CHANGEOVER

The CA does not issue Subscriber certificates that extend beyond the expiration date of its own CA certificates and public keys, and the CA certificate validity period extends one Subscriber certificate validity period past the last use of the CA private key. To minimize risk to the PKI through compromise of a CA's key, the private signing key is changed more frequently, and only the new key is used for certificate signing purposes from that time. The older, but still valid, certificate is available to verify old signatures until all of the Subscriber certificates signed under it have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key is retained and protected. Direct subscribers will be notified about key changeovers via the RA and Subscriber support personnel. If key changeover is required to compromise, all certs will be revoked and reissued by the OA and RA/CA personnel.

The corresponding new CA Public Key certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4. Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs. The CA self-signed root certificate is valid for 20 years.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

If a hacking attempt or other form of potential compromise of a CA becomes known, it is investigated in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 are followed. Otherwise the scope of potential damage is assessed

in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

The CA's Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS. Surescripts Incident Management processes will be invoked to ensure service reporting, escalation and management of the incident or compromise.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

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

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

If the Root CA key is compromised, the trusted self-signed certificate is removed from each Relying Party application, and a new one distributed via secure out-of-band mechanisms. We will notify by automated email all Subscribers with Certificates with a CA Chain containing that Root CA at their contact addresses on file. This notification will include notice of the compromise or suspected compromise of the Root CA Certificate, notice that the corresponding self-signed Certificate must be removed from any Relying Party application, and the location of a new Root Certificate that shall be distributed.

If a Subordinate CA key is compromised or is reasonably suspected by us of being compromised, the old Subordinate CA Certificate will be revoked and all Subscriber Certificates that are not revoked or expired that were signed with the revoked CA Certificate will be re-issued using a different uncompromised Subordinate CA Certificate. The original Subscriber Certificates signed by the compromised CA will also be revoked. Additionally, all Subscribers with Certificates that were signed by the compromised Subordinate CA will be notified by email at their respective contact email addresses on file with us.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA shall have recovery procedures in place to reconstitute the CA within 72 hours of failure.

If the CA cannot reestablish revocation capabilities prior to the next update field in the latest CRL issued by the CA, then the Surescripts Crisis Management Team decides whether to declare the CA private signing key as compromised, and reestablish the CA keys and certificates and all Subscriber certificates, or allow additional time for reestablishment of the CA's revocation capability. In the case of a disaster whereby the CA installation is physically damaged and all copies of the

CA signature key are destroyed as a result, the CA is completely rebuilt by reestablishing the CA equipment and generating new private and public keys. Finally, all Subscriber certificates are re-issued. In such events, any Relying Parties who continue to use certificates signed with the destroyed private key after proper notification do so at their own risk and the risk of others to whom they forward data.

5.7.5 BUSINESS CONTINUITY PLANS AND TESTING

Business Continuity Plans will be maintained for the CA environment. Continuity Plans for CA operations will be sections within larger production systems recovery procedures. Plans will document:

- When operationing conditions warrant activating the Business Continuity Plan (the Plan).
- What constitutes an acceptable system outage and recovery time.
- Emergency and fallback procedures.
- Resumption procedures and timelines, including recovery time objective (RTO). Frequency of backup copies of essential business information and software must be published as required by 5.5.4 above.
- Procedures for securing its facility, to the extent possible, during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.
- Requirements to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location.

The Business Continuity Plan shall be tested at least annually, reviewed, and updated appropriately.

Surescripts will train appropriate personnel during awareness and education sessions covering the responsibilities of the individuals, and provide regular testing of contingency plans with appropriate personnel.

5.8 CA AND RA TERMINATION

For Surescripts Certificates:

In the event of CA termination, certificates signed by the CA SHALL be revoked. Certificates will be revoked and listed in CRL's and OCSP services for Relying Party validation.

For Surescripts TLS Certificates:

The CA shall provide archived data to an archive facility for a period of 2 years.

In the event of an RA termination, a new RA will be established. New certificates shall be issued to replace any certificates in the event of credential comprimise or a compromise that affects the integrity of the RA processes. Certificates will be revoked and listed in CRL's and OCSP services for Relying Party validation.

SECTION 6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

6.1.1.1 CA KEY PAIR GENERATION

The CA cryptographic keying material used to sign certificates or CRLs are generated on a tamper-proof hardware secure module (HSM) rated at FIPS 140-2 level 2 minimum.

6.1.1.2 SUBSCRIBER KEY PAIR GENERATION

The CA cryptographic keying material generated for Subscriber certificates is created on physical hardware that is rated at a FIPS 140-2 level 2. Group, Role and Device certificates are not supported at this time. Public Keys utilize RSA 2048.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

Private keys are not delivered to subscribers.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

No delivery is required if keys are generated by the Direct Issuing CA system. Public keys for subscribers are generated by the respective CA only. mTLS certificates are delivered to subscribers via Surescripts project implementation personnel once generated from a customer submitted CSR.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

Each of our CAs public keys is available within its respective CA Certificate. Each CA Certificate is available online at a location specified in each Sub-CA or Subscriber Certificate issued by that CA,

The CA root public key may also be delivered, when requested, within a self-signed certificate using a commercially reasonable out-of-band medium trusted by the relying party (email).

Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs.

6.1.5 KEY SIZES

The Surescripts CA generates and use the following keys, signature algorithms, and hash algorithms for signing certificates, CRLs, and certificate status server responses:

- Minimum 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256)
- Minimum 384-bit ECDSA Key with Secure Hash Algorithm version 2 (SHA-256)

All but the first-listed above is utilized for Subscriber keys.

The Surescripts CA issues end-entity certificates that contain at least 2048-bit public keys for RSA, DSA, or Diffie-Hellman, or at least 224 bits for elliptic curve algorithms, except for certificates issued to smart cards or other hardware devices that are incapable of accepting 2048-bit RSA certificates. Role and Device certificates are not supported at this time.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The Surescripts CA generates Public Key parameters for signature algorithms and perform parameter quality checking in accordance with FIPS 186.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

Surescripts CA	DirectTrust
Subscriber Certificates	Surescripts CA public keys that are bound into certificates are certified for use in signing and encryption of S/MIME packages. Specifically, Subscriber certificates assert the following key usage bits:
	• digitalSignature
	• KeyEncipherment: Subscriber certificates that are dual-use certificates do not assert the non-repudiation bit.
	Subscriber certificates also assert an extended key usage bit of *emailProtection* and a BasicConstraint of *CA:FALSE*.

Root Certificate	The Surescripts CA root certificate asserts the following key usage bits:
	• cRLSign
	• keyCertSign
	The Surescripts CA root certificate also asserts a Basic Constraint of *CA:TRUE*.
Surescripts Issuing CA	MTLS
Subscriber Certificates	Surescripts Issuing CA public keys that are bound into certificates are certified for use in client authentication and server authentication. Subscriber certificates assert the following key usage bits:
	• digitalSignature
	• KeyEncipherment: Subscriber certificates that are dual-use certificates do not assert the non-repudiation bit.
	• TLS Web Server Authentication
	• TLS Web Client
	Subscriber certificates also assert a BasicConstraint of *CA:FALSE*.
Root Certificate	The Surescripts Issuing CA root certificate asserts the following key usage bits:
	• cRLSign
	• keyCertSign

	• Off-line CRL Signing
	The Surescripts Issuing CA root certificate also asserts a Basic Constraint of *CA:TRUE*.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

All HSMs are validated to the FIPS 140 level 2

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

No stipulation.

6.2.3 PRIVATE KEY ESCROW

Private keys (CA or Subscriber) are not escrowed.

6.2.4 PRIVATE KEY BACKUP

The Surescripts CA root private signature key is backed up to a secure offsite location to facilitate disaster recovery. Issuing CA keys are stored in redundant HSM's.

All private keys are stored in encrypted stores in accordance with FIPS 140-2 standard for HSMs and software encryption. PKI systems must be in a dedicated secure zone and private keys must be transferred on internal networks to production systems utilizing encrypted key stores.

Any Subscriber private keys are backed up to a redundant offsite location to facilitate disaster recovery.

6.2.5 PRIVATE KEY ARCHIVAL

No stipulation.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

Private Keys MAY be transferred only into a cryptographic module meeting the requirements of section 6.2.1 as applicable for the entity. Private keys SHALL NOT exist in the clear outside of a cryptographic module.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

6.2.8 PRIVATE KEYS STORED IN A CRYPTOGRAPHIC MODULE.

Once the HSM has been turned on, the private key may be used by the Issuing CA and certificate management application, in accordance with the specifications of the cryptographic module manufacturer.. The private key is available for use until the application is stopped or other interruption of service occurs (e.g. shutdown).

The Surescripts HSM Operator/Administrator can activate the private keys after authentication

6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS

The Surescripts CA deactivates its Private Keys and stores its off-line HSMs in secure containers when not in use. The Surescripts CA prevents unauthorized access to any activated cryptographic modules.

6.2.10 METHOD OF DESTROYING PRIVATE KEYS

CA Administrators destroy private signature keys when they are no longer needed.

Subscriber private signature keys are destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

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

6.3.2 CERTIFICATE OPERATIONAL PERIODS/KEY USAGE PERIODS

The Surescripts CA root private key is used for a maximum of 20 years. Issuer CA certificates expire expires after a maximum of 20 years.

Surescripts Direct Certificates	Private keys	Subscriber private keys are used for a maximum of 4 years.
	Subscriber	Subscriber public certificates expire after two years.
Surescripts TLS Certificates	Root	Root certificates expire after 20 years.
	Subscriber	Subscriber certificates expire after two years.

. For OCSP responders operating under this policy and all other subscriber public keys, the maximum usage period is three years.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The Surescripts CA or Subscriber generates activation data that has 13 randomly generated characters to protect its respective Private Keys.

If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. Activation data is never transmitted to a subscriber.

6.4.2 ACTIVATION DATA PROTECTION

The Surescripts CA protects data used to unlock private keys from disclosure using a tamper-proof HSMs and physical access control mechanisms. Activation data is recorded and secured at the level of assurance associated with the activation of the cryptographic module, and is not stored with the cryptographic module.

The Surescripts CA requires personnel to memorize and not write down their password. The Company protects all shared secrets and has implemented processes to temporarily lock access to secure CA processes if a certain number of failed log-in attempts occur.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The Surescripts CA configures its CA systems, including any remote workstations, to:

- Authenticate the identity of users 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 for all transactions,
- Enforce domain integrity boundaries for security critical processes, and
- support recovery from key or system failure.

The Surescripts CA authenticates and protects all communications between a trusted role and its CA system.

6.5.2 COMPUTER SECURITY RATING

No stipulation.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

All CA software was purchased from recognized software and hardware manufacturers. These applications are dedicated to performing CA functions. The protection of CA hardware and software containing private keys is part of the terms for Subscriber and Trusted Role Agreement Forms.

Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with *(e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device)*.

6.6.2 SECURITY MANAGEMENT CONTROLS

The configuration of a CA system as well as any modifications and upgrades are documented and controlled through Change Control Practices. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system.

The firewall protecting the Surescripts CA system from external networks is managed by a Surescripts Operations firewall expert, under the supervision of the Surescripts CA Manager. Firewall logs are collected and analyzed periodically. KMS-0706, Firewall Rule Set, defines the firewall configuration and management.

A centralized security management tool is run on the computers of the Surescripts CA system to enforce access policies, manage user accounts, and log significant events. A set of Information technology (IT) procedures, approved by Security Operations , govern operations of the Surescripts CA system computers.

6.6.3 LIFE CYCLE SECURITY RATINGS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Information to be transferred from the Surescripts CA is done through secure networks. Firewall devices are configured that no access to CA systems is allowed except through secure networks. All changes to firewall configurations are documented.

Appropriate security measures are employed to ensure that CA systems are protected from unauthorized access and intrustion attacks. All CA and network equipment shall turn off unused network ports and services.

RA workstations to not directly access CA systems. All workstations used to access CA systems are specifically authorized for PKI and CA support personnel using mulit-factor authentication

6.8 STAMPING

The system clock time for the CA system is derived from a trusted time service. This CA is implemented as a Microsoft Active Directory Certification Services CA, where all member servers and domain controllers sync to a domain controller holding Primary Domain Controller (PDC) Emulator role. The PDC Emulator role syncs to an external timesource time.nist.gov and pool.ntp.org.

Asserted times shall be accurate to within three minutes.

SECTION 7 CERTIFICATE, CRL, AND OCSP PROFILE FORMATS

7.1 CERTIFICATE PROFILE

The Surescripts CA SHALL issue Certificates in accordance with approved DirectTrust Certificate Profiles corresponding to this CPS version (V1.4).

7.1.1 VERSION NUMBERS

The Surescripts CA issues X.509 v3 certificates, which means the version field should contain the integer 2.

7.1.2 CERTIFICATE EXTENSIONS

The Surescripts CA uses standard certificate extensions that are compliant with IETF RFC 5280.

- The Key Usage, Extended Key Usage, and Basic Constraints extensions is populated as specified in section 6.1.7 of the Surescripts CA CPS
- The CRL Distribution Points extension may be populated with a CRL URL as specified in section 2.2.1 of the Surescripts CA CPS.
- The Authority Information Access extension may be populated with an OCSP Responder location as specified in section 2.2.1 of the Surescripts CA CPS.
- The Subject Alternative Name extension is populated as specified in section 3.1.1 of the Surescripts CPS.
- The Certificate Policies extension is populated as defined in section 7.1.6 of the Surescripts CPS.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

End Entity Certificates signed by the Surescripts CA uses the SHA-256 signature algorithm and identify it using the following OID:

```
sha256WithRSAEncryption: {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) 11}
```

Certificates issued by the Surescripts CA shall use the following OID for identifying the subject public key algorithm:

```
rsaEncryption: {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) 1}
```

7.1.4 NAME FORMS

See section 3.1.1 of this Surescripts CA CPS.

7.1.5 NAME CONSTRAINTS

No stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

Certificates assert at least one of the policy OIDs (or a policy OID of a superior CP that has been successfully mapped to the DirectTrustCP) defined in section 1.2 of the Certificate Policy.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

The Surescripts CA Certificate Policy does not require the `certificatePolicies` extension to be critical. Relying Parties, whose client software does not process this extension, risk using certificates inappropriately.

7.2 CRL PROFILE

7.2.1 VERSION NUMBERS

The Surescripts CA issues X.509 version 2 CRLs, which means the version field should contain the integer 1.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

The Surescripts CA conforms to the CRL and CRL Extensions profile defined in IETF RFC 5280.

The Surescripts CA signs the CRL using the SHA-256 signature algorithm and identify it using the following OID:

```
sha256WithRSAEncryption: {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) 11}
```

The CRL contains a CRL Reason Code entry extension for each entry.

7.3 OCSP PROFILE

The status of public certificates is available via a CRL or OCSP responder. Responders operate in accordance with OCSP Protocol define in RFC 2560. These services are iconfiguredin an high availability (HA) cluster where reponders are available concurrently in multiple data center locations

7.3.1 VERSION NUMBERS

OCSP responders will operate in accordance with version 1 of the OCSP protocol

7.3.2 OCSP EXTENSIONS

No stipulation.

SECTION 8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS

The Surescripts CA has a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced. Surescripts uses a compliance auditor that is independent from the CA.

Surescripts provides a DirectTrust/EHNAC supplied assertion package to make a self-attested, legally binding Declaration of Conformance to this CPS to the Direct CP (v1.4 currently) biennially. Surescripts is EHNAC/DirectTrust Accredited for CA, RA and HISP operations.

The practices in this CPS are designed to meet or exceed the requirements of the latest version of the *Version 2.2 of WebTrust Principles and Criteria for Certification Authorities* and *Version 2.4.1 of WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security* Independent Audit for PKI operation

Annually, Surescripts PKI practices and infrastructure will undergo a Webtrust Audit. The audit occurs at once per year.

8.1 IDENTITY/QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and corresponding CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

The CA Declaration of Conformance describes the compliance assessor's relationship to the CA, indicating that the assessor is an independent compliance auditor

8.2 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The CA Declaration of Conformance describes the compliance assessor is an independent compliance auditor. If DirectTrust provides an accreditation program to certify the compliance of CAs, RAs, and HISPs, in which case the Surescripts CA adheres to this program.

8.3 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of the CP and the CA's CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

8.4 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Surescripts takes all items of non-conformance seriously. For every item of non-conformance, Surescripts drafts a Mitigation Plan including level of effort and expected resolution.

The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the FPKIPA and appropriate Relying Parties.

The Audit Compliance Report and identification of corrective measures shall be provided to both the Surescripts Management and any third party that Surescripts is legally obligated to satisfy.

The information contained in compliance reports is restricted to Surescripts and Relying Parties on a need to know basis only.

8.5 COMMUNICATION OF RESULTS

The information contained in compliance reports is restricted to the Surescripts and Relying Parties on a need to know basis only and available by request.

SECTION 9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE/RENEWAL FEES

None. No stipulation.

9.1.2 CERTIFICATE ACCESS FEES

None. No stipulation.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

None. No stipulation.

9.1.4 FEES FOR OTHER SERVICES

None. No stipulation.

9.1.5 REFUND POLICY

None. No stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

No stipulation.

9.2.2 OTHER ASSETS

No stipulation.

9.2.3 INSURANCE/WARRANTY COVERAGE FOR END-ENTITIES

None. No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

All data and their hardware containers are considered proprietary and confidential. Handling corresponds to Surescripts policies for this classification of data. These include:

- Certificate application records.
- Transactional records (both full records and audit trail of transactions)
- Audit trail records created or retained by Surescripts or a customer
- Audit reports created by Surescripts or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public)
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of Surescripts hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

The Surescripts CA treats all information in the CPS as confidential and proprietary information.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The Surescripts CA contractually obligate employees, agents, and contractors to protect confidential information through its Trusted Role Agreement. Surescripts provides training to employees on how to handle confidential information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

All identifying information for a Subscriber is protected from unauthorized disclosure. The Surescripts CA creates and follows a publicly posted privacy policy at https://surescripts.com/our-story/privacy/that specifies how it handles personal information.

9.4.2 INFORMATION TREATED AS PRIVATE

Information deemed as private shall be defined as such in agreements between the CA and its Subscribers.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Information included in certificates is not deemed private.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

The Surescripts CA stores private non-public information securely.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

The Surescripts CA uses private information as dictated by their Clinical Interoperability Agreements with its Subscribers.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS

The Surescripts CA does not disclose private information unless allowed by agreements with its Subscribers or unless required to by law.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

Surescripts and the Surescripts CA do not knowingly violate the intellectual property rights held by others. None are implied with in this practices statement.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA AND RA REPRESENTATIONS AND WARRANTIES

The Surescripts CA will use reasonable efforts to provide the services described herein in an efficient and trustworthy manner. The Surescripts CA will take reasonable precautions to protect the confidentiality of its private keys and other information used to create Certificates.

By issuing a Certificate to a Subscriber, the Surescripts CA represents to the Subscriber, and to all qualified Relying Parties who depend on the information contained in the Certificate, that during its period of validity:

- The Surescripts CA will issue and revoke Certificates in accordance with this Surescripts CA CPS and any applicable CP when required.
- There will be no material misrepresentations of fact or errors in the Certificate as a result of the Surescripts CA's failure to use reasonable care in creating the Certificate, and the Surescripts CA will take reasonable steps to confirm the accuracy of the information in the Certificate.
- The Surescripts CA will accurately transcribe information provided by the Applicant (as defined in Section 1.3.5) in the Certificate application to the Certificate.
- The Subscriber's public and private key will constitute a functional key pair.
- The Subscriber holds the private key that corresponds to the public key listed in his/her Certificate.
- The Surescripts CA has a trustworthy system to generate, issue, and publish the Certificate.
- The Surescripts CA will revoke Certificates pursuant to the terms and conditions of this Surescripts CA CPS and any applicable CP.
- The Certificates will be reasonably fit for their intended use within the PKI for the Surescripts business.
- The Surescripts CA will process Certificate applications pursuant to the Surescripts CA CPS and any other applicable documentation.
- The Surescripts RA will request Certificates be issued by the Surescripts CA for a Subscriber verified in accordance with this Surescripts CA CPS.
- The Surescripts CA will comply with this Surescripts CA CPS.
- The Surescripts CA will give a copy of this Surescripts CA CPS and a Subscriber Agreement to each Subscriber, or direct the Subscriber to where they may get their own copies of these documents.
- The Surescripts CA will process Certificate revocation requests and submit properly vetted revocation requests to the Surescripts CA in accordance with this Surescripts CA CPS

9.6.2 RA REPRESENTATIONS AND WARRANTIES

See 9.6.1

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Each Subscriber represents to the Surescripts CA that the Subscriber will:

1. Protect its Private Keys from compromise (including if employing a HISP who uses secure processes against potential compromise),

2. Provide accurate and complete information and communication to the Issuer CA and RA,

3. Confirm the accuracy of certificate data prior to using the certificate,

4. Promptly cease using a certificate and notify the Issuer CA if (i) any information that was submitted to the Issuer CA or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,

5. Use the certificate only for authorized and legal purposes, consistent with the relevant CPS and Subscriber Agreement, (including only installing device certificates on servers accessible at the domain listed in the certificate), and

6. Promptly cease using the certificate and related Private Key after the certificate's expiration.

7. Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.

Wherever possible, subscriber documents must be digitally signed.

If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device. The delegation shall be documented and signed by both the device sponsor and the authorized administrator for the device. Delegation does not relieve the device sponsor of his or her accountability for these responsibilities.

9.6.4 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Relying parties use a Surescripts certificate for the purpose for which it was intended and check each certificate for validity.

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 Liabilities

Surescripts may limit their liability to any extent not otherwise prohibited by this CPS, provided that the Issuer CA remains responsible for complying with this CPS and the respective CP.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CPS becomes effective when approved through the Surescripts consensus process. This CPS has no specified term.

9.10.2 Termination

Termination of this Certification Practice Statement may occur if approved through the Surescripts consensus process.

9.10.3 Effect of Termination and Survival

The requirements of this Certification Practice Statement remain in effect through the end of the archive period of the last certificate issued.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

This Certification Practice Statement may be amended through the Surescripts approval process.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

Subscribers may see updated CPS at Surescripts.com.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

OIDs must be changed to reflect new versions of DirectTrust CP or Subsequent versions of this CPS.

9.13 DISPUTE RESOLUTION PROVISIONS

In the event of any dispute related to this Certification Practice Statement, a statement of guidance may be issued and published on the Surescripts website if approved through the Surescripts consensus process.

9.14 GOVERNING LAW

The laws of the United States of America shall govern this Certification Practice Statement.

9.15 COMPLIANCE WITH APPLICABLE LAW

All PKI participants shall comply with applicable laws.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

No stipulation.

9.16.2 ASSIGNMENT

No stipulation.

9.16.3 SEVERABILITY

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

9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)

No stipulation.

9.16.5 FORCE MAJEURE

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.