Cerner Direct

Certification Practice Statement

Version 1.0

Effective Date: September 21, 2012

Cerner Corporation

2800 Rockcreek Parkway

Kansas City, MO 64117

1-816-201-1024

www.cerner.com

Table of Contents

1. INTRODUCTION 11

1.1 Overview 11

1.2 Document name and identification 11

1.3 Public Key Infrastructure (PKI) participants 11

1.3.1 Certification Authorities 11

1.3.2 Registration Authorities (RAs) 12

1.3.3 Subscribers 12

1.3.4 Relying Party (RP) 12

1.3.5 Other participants 12

1.4 Certificate Usage 12

1.4.1. Appropriate Certificate uses 12

1.4.2 Prohibited Certificate uses 12

1.5 Policy administration 12

1.5.1 Organization administering the CPS 12

1.5.2 Contact person 12

1.5.3 Person determining CPS suitability for the policy 13

1.5.4 CPS approval procedures 13

1.6 Definitions and acronyms 13

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 15

2.1 Repositories 15

2.2 Publication of Certification Information 15

2.2.1 Publication of Certificates and Certificate Status 15

2.2.2 Publication of CA Information 16

2.2.3 Interoperability 16

2.3 Time or frequency of publication 16

2.4 Access controls on repositories 16

3. IDENTIFICATION AND AUTHENTICATION 16

3.1 Naming 16

3.1.1 Types of names 16

3.1.2 Need for names to be meaningful 17

3.1.3 Anonymity or pseudonymity of Subscribers 17

3.1.4 Rules for interpreting various name forms 17

3.1.5 Uniqueness of names 17

3.1.6 Recognition, authentication, and role of trademarks 17

3.2 Initial identity validation 17

3.2.1 Method to prove possession of Private Key 17

3.2.3 Authentication of individual identity 18

3.2.4 Non-verified Subscriber information 19

3.2.5 Validation of authority 19

3.2.6 Criteria for interoperation 19

3.3 Identification and authentication for re-key requests 19

3.3.1 Identification and authentication for routine re-key 19

3.3.2 Identification and authentication for re-key after revocation 20

3.4 Identification and authentication for revocation request 20

4. CERTIFICATE LIFE-CYCLE 20

4.1 Application 20

4.1.1 Submission of Certificate application 20

4.1.2 Enrollment process and responsibilities 20

4.2 Certificate application processing 20

4.2.1 Performing identification and authentication functions 20

4.2.2 Approval or rejection of Certificate applications 20

4.2.3 Time to process Certificate applications 20

4.3 Issuance 21

4.3.1 CA actions during Certificate issuance 21

4.3.2 Notification to Subscriber of Certificate issuance 21

4.4 Certificate acceptance 21

4.4.1 Conduct constituting Certificate acceptance 21

4.4.2 Publication of the Certificate by the CA 21

4.4.3 Notification of Certificate issuance by the CA to other entities 21

4.5 Key pair and Certificate usage 21
4.5.1 Subscriber Private Key and Certificate usage 21
4.5.2 Relying Party Public Key and Certificate usage 21
4.6 Certificate renewal 21
4.6.1 Circumstance for Certificate renewal 21
4.6.2 Who may request renewal 21
4.6.3 Processing Certificate renewal requests 21
4.6.4 Notification of new Certificate issuance to Subscriber 22
4.6.5 Conduct constituting acceptance of a renewal Certificate 22
4.6.6 Publication of the renewal Certificate by the CA 22
4.6.7 Notification of Certificate issuance by the CA to other entities 22
4.7 Certificate re-key 22
4.7.1 Circumstance for Certificate re-key 22
4.7.2 Who may request Certification of a new Public Key 22
4.7.3 Processing Certificate re-keying requests 22
4.7.4 Notification of new Certificate issuance to subscriber 22
4.7.5 Conduct constituting acceptance of a re-keyed Certificate 22
4.7.6 Publication of the re-keyed Certificate by the CA 22
4.7.7 Notification of Certificate issuance by the CA to other entities 23
4.8 Modification 23
4.8.1 Circumstance for Certificate modification 23
4.8.2 Who may request Certificate modification 23
4.8.3 Processing Certificate modification requests 23
4.8.4 Notification of new Certificate issuance to Subscriber 23
4.8.5 Conduct constituting acceptance of modified Certificate 23
4.8.6 Publication of the modified Certificate by the CA 23
4.8.7 Notification of Certificate issuance by the CA to other entities 23
4.9 Certificate revocation and suspension 23
4.9.1 Circumstances for revocation 23
4.9.2 Who can request revocation 23

4.9.3 Procedure for revocation request 24
4.9.4 Revocation request grace period 24
4.9.5 Time within which CA must process the revocation request 24
4.9.6 Revocation checking requirement for relying parties 24
4.9.7 CRL issuance frequency 24
4.9.8 Maximum latency for CRLs 24
4.9.9 On-line revocation/status checking availability 24
4.9.10 On-line revocation checking requirements 24
4.9.11 Other forms of revocation advertisements available 24
4.9.12 Special requirements related to key Compromise 24
4.9.13 Circumstances for suspension 25
4.9.14 Who can request suspension 25
4.9.15 Procedure for suspension request 25
4.9.16 Limits on suspension period 25
4.10 Certificate status services 25
4.10.1 Operational characteristics 25
4.10.2 Service availability 25
4.10.3 Optional features 25
4.11 End of subscription 25
4.12 Key escrow and recovery 25
4.12.1 Key escrow and recovery policy and practices 25
4.12.2 Session key encapsulation and recovery policy and practices 25
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 25
5.1 Physical controls 25
5.1.1 Site location and construction 25
5.1.2 Physical access 26
5.1.3 Power and air conditioning 26
5.1.4 Water exposures 26
5.1.5 Fire prevention and protection 26
5.1.6 Media storage 26

5.1.7 Waste disposal 26
5.1.8 Off-site backup 26
5.2 Procedural controls 27
5.2.1 Trusted roles 27
5.2.2 Number of persons required per task 28
5.2.3 Identification and authentication for each role 28
5.2.4 Roles requiring separation of duties 28
5.3 Personnel controls 28
5.3.1 Qualifications, experience, and clearance requirements 28
5.3.2 Background check procedures 28
5.3.3 Training requirements 28
5.3.4 Retraining frequency and requirements 29
5.3.5 Job rotation frequency and sequence 29
5.3.6 Sanctions for unauthorized actions 29
5.3.7 Independent contractor requirements 29
5.3.8 Documentation supplied to personnel 29
5.4 Audit logging procedures 29
5.4.1 Types of events recorded 29
5.4.2 Frequency of processing log 30
5.4.3 Retention period for audit log 30
5.4.4 Protection of audit log 30
5.4.5 Audit log backup procedures 30
5.4.6 Audit collection system (internal vs. external) 30
5.4.7 Notification to event-causing subject 30
5.4.8 Vulnerability assessments 30
5.5 Records archival 30
5.5.1 Types of records archived 30
5.5.2 Retention period for archive 31
5.5.3 Protection of archive 31
5.5.4 Archive backup procedures 31

5.5.5 Requirements for time-stamping of records 31
5.5.6 Archive collection system (internal or external) 31
5.5.7 Procedures to obtain and verify archive information 31
5.6 Key changeover 31
5.7 Compromise and disaster recovery 31
5.7.1 Incident and compromise handling procedures 31
5.7.2 Computing resources, software, and/or data are corrupted 31
5.7.3 Entity private key compromise procedures 31
5.7.4 Business continuity capabilities after a disaster 32
5.8 CA or RA termination 32
6. TECHNICAL SECURITY CONTROLS 32
6.1 Key pair generation and installation 32
6.1.1 Key pair generation 32
6.1.2 Private Key delivery to Subscriber 32
6.1.3 Public Key delivery to Certificate Issuer 32
6.1.4 CA Public Key delivery to relying parties 32
6.1.5 Key sizes 32
6.1.6 Public key parameters generation and quality checking 33
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 33
6.2 Private Key Protection and Cryptographic Module Engineering Controls 33
6.2.1 Cryptographic module standards and controls 33
6.2.2 Private Key (n out of m) multi-person control 33
6.2.3 Private Key escrow 33
6.2.4 Private Key backup 33
6.2.5 Private Key archival 33
6.2.6 Private Key transfer into or from a cryptographic module 33
6.2.7 Private Key storage on cryptographic module 34
6.2.8 Method of activating Private Key 34
6.2.9 Method of deactivating Private Key 34
6.2.10 Method of destroying Private Key 34

6.2.11 Cryptographic Module Rating 34
6.3 Other aspects of key pair management 34
6.3.1 Public key archival 34
6.3.2 Certificate operational periods and key pair usage periods 34
6.4 Activation data 34
6.4.1 Activation data generation and installation 34
6.4.2 Activation data protection 34
6.4.3 Other aspects of activation data 34
6.5 Computer security controls 34
6.5.1 Specific computer security technical requirements 34
6.5.2 Computer security rating 34
6.6 Life cycle technical controls 35
6.6.1 System development controls 35
6.6.2 Security management controls 35
6.6.3 Life cycle security controls 35
6.7 Network security controls 35
6.8 Time-stamping 35
7. CERTIFICATE, CRL, AND OCSP PROFILES 35
7.1 Certificate profile 35
7.1.1 Version number(s) 36
7.1.2 Certificate extensions 36
7.1.3 Algorithm object identifiers 36
7.1.4 Name forms 36
7.1.5 Name constraints 36
7.1.6 Certificate policy object identifier 36
7.1.7 Usage of Policy Constraints extension 36
7.1.8 Policy qualifiers syntax and semantics 36
7.1.9 Processing semantics for the critical Certificate Policies extension 36
7.2 CRL profile 37
7.2.1 Version number(s) 37

7.2.2 CRL and CRL entry extensions 37

7.3 OCSP profile 37

7.3.1 Version number(s) 37

7.3.2 OCSP extensions 37

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 37

8.1 Frequency or circumstances of assessment 37

8.2 Identity/qualifications of assessor 38

8.3 Assessor's relationship to assessed entity 38

8.4 Topics covered by assessment 38

8.5 Actions taken as a result of deficiency 38

8.6 Communication of results 38

9. OTHER BUSINESS AND LEGAL MATTERS 38

9.1 Fees 38

9.1.1 Certificate issuance or renewal fees 38

9.1.2 Certificate access fees 38

9.1.3 Revocation or status information access fees 39

9.1.4 Fees for other services 39

9.1.5 Refund policy 39

9.2 Financial responsibility 39

9.2.1 Insurance coverage 39

9.2.2 Other assets 39

9.2.3 Insurance or warranty coverage for end-entities 39

9.3 Confidentiality of business information 39

9.3.1 Scope of confidential information 39

9.3.2 Information not within the scope of confidential information 40

9.3.3 Responsibility to protect confidential information 40

9.4 Privacy of personal information 40

9.4.1 Privacy plan 40

9.4.2 Information treated as private 40

9.4.3 Information not deemed private 40

9.4.4 Responsibility to protect private information 40
9.4.5 Notice and consent to use private information 40
9.4.6 Disclosure pursuant to judicial or administrative process 40
9.4.7 Other information disclosure circumstances 41
9.5 Intellectual property rights 41
9.6 Representations and warranties 41
9.6.1 CA representations and warranties 41
9.6.2 RA representations and warranties 41
9.6.3 Subscriber representations and warranties 41
9.6.4 Relying party representations and warranties 41
9.6.5 Representations and warranties of other participants 41
9.7 Disclaimers of warranties 41
9.8 Limitations of liability 42
9.9 Indemnities 42
9.10 Term and termination 42
9.10.1 Term 42
9.10.2 Termination 42
9.10.3 Effect of termination and survival 42
9.11 Individual notices and communications with participants 42
9.12 Amendments 42
9.12.1 Procedure for amendment 42
9.12.2 Notification mechanism and period 43
9.12.3 Circumstances under which OID must be changed 43
9.13 Dispute resolution provisions 43
9.14 Governing law 43
9.15 Compliance with applicable law 43
9.16 Miscellaneous provisions 43
9.16.1 Entire agreement 43
9.16.2 Assignment 43
9.16.3 Severability 43

9.16.4 Enforcement (attorneys' fees and waiver of rights) 43

9.16.5 Force Majeure 43

1. INTRODUCTION

This document is the Cerner Direct Certification Practice Statement (CPS) and states the policies and associated practices Cerner Corporation (Cerner) performs as the Certification Authority (CA) for digital certificates used in the exchange of electronic messages grounded in the Direct Project Applicability Statement for Secure Health Transport. The Direct Project is an initiative sponsored by the Office of the National Coordinator (ONC) for Health Information Technology to encourage adoption of secure clinical and administrative messaging within the healthcare system. The Direct Project is based on S/MIME message signatures and message encryption for the purposes of achieving privacy, authentication, and message integrity.

The Direct Ecosystem Community X.509 Certificate Policy (CP) is the governing policy on which this CPS is based and provides specific requirements necessary for identity validation and digital certificate lifecycle management to ensure the integrity of Directed exchanges within this community. This document describes how Cerner addresses these requirements for:

- maintaining the security of the infrastructure necessary to support these activities; and
- issuing, managing, renewing, and revoking Organizational Certificates used in Directed exchange.

The Direct Citizen Community Certificate Policy, which will govern the Citizen Certificate Class described in § 3.2.3.1, is currently in DRAFT status. Cerner intends to comply with the subsequent recommendations when final.

This CPS follows the structure of Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure (PKI) Certificate Policy and Certification Practices Framework (RFC 3647).

1.1 Overview

This CPS describes the policies and practices of Cerner in the creation and management of X.509 version 3 public key Certificates solely for use in supporting Cerner's HISP called Cerner Direct.

1.2 Document name and identification

This document is the Cerner Direct Certification Practice Statement (CPS). The Cerner Direct Intermediate CA Certificates and Certificates issued by the Cerner Direct Intermediate CA will contain the object identifier (OID) defined in CP § 1.2.

The CPS Pointer qualifier is http://www.cerner.com/cps and is included in the Certificate Policy Extension field of the CA Certificates.

1.3 Public Key Infrastructure (PKI) participants

1.3.1 Certification Authorities

Cerner is a Certification Authority (CA) that signs Certificate Signing Requests (CSRs) and issues public key X.509 Certificates to Cerner Direct Subscribers. Cerner issues its own self-signed Intermediate CA. This Intermediate CA is used for the sole purpose of issuing Certificates to Subscribers for purposes of securing Direct communications. Unless otherwise noted, the CA as it relates to this CPS is Cerner and the self-signed Intermediate CA will be referenced as the CA Certificate.

1.3.2 Registration Authorities (RAs)

RAs collect and verify identity information from Subscribers using procedures that implement the identity validation policies set forth in this document. The RA creates Certificate Signing Requests (CSRs) for submission to the CA. RA entities must utilize identity validation policies defined in this CPS. Cerner is the primary RA for the Cerner CA; however, Cerner may delegate the RA responsibility to other qualified entities.

1.3.3 Subscribers

A Subscriber is a Professional Organization whose identifying information appears as the subject in a Certificate and who uses its Private Key and Public Key in accordance with this CPS.

1.3.4 Relying Party (RP)

A RP uses a Subscriber's Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, and to establish confidential communications with the Subscriber. The RP is responsible for checking the validity of the Certificate by checking the appropriate Certificate status information defined in § 2.1.

1.3.5 Other participants

No stipulation.

1.4 Certificate Usage

1.4.1. Appropriate Certificate uses

The CA Certificates are used for the sole purpose of issuing Certificates to Cerner Direct Subscribers. The Certificates issued by the CA Certificates will be used in the exchange of electronic messages as defined in the specification of the Direct Project. This includes S/MIME message signature verification and S/MIME message encryption.

1.4.2 Prohibited Certificate uses

Any use not for the purposes of Directed exchange is prohibited.

1.5 Policy administration

1.5.1 Organization administering the CPS

Cerner Corporation
2800 Rockcreek Parkway
Kansas City, MO 64117
USA

1.5.2 Contact person

Cerner Corporation
Attn: Cerner Direct Operations

2800 Rockcreek Parkway
Kansas City, MO 64117
1-816-201-1024
USA

1.5.3 Person determining CPS suitability for the policy

The Certificate Policy Cabinet (CPC) approves the content of this CPS.

1.5.4 CPS approval procedures

CPS approval and subsequent amendments shall be approved by the CPC. All versions and updates shall be linked to the CPS page of the Cerner web site located at: http://www.cerner.com/cps. The most recent version or update supersedes all prior versions.

1.6 Definitions and acronyms

Term	Definition
Associate	An individual employed by Cerner.
Cerner Direct	Cerner-owned and operated HISP which provides the management of security and transport as it relates to information exchange using Direct Project standards.
Cerner Direct Administrator	The Professional person who is tasked with responsibility for distribution and use of Cerner Direct capabilities within their respective organization.
Certificate Policy Cabinet or CPC	A group of Associates tasked with (1) management and oversight of the Certificate practices and procedures used in Cerner Direct communications, and (2) the review and approval of this CPS and updates thereto.
Cerner Technology Centers or CTC	The ISO 9001:2008 and SSAE-16 certified data center facilities which host the Certificate infrastructure.
Certificate	A digital representation of information which (1) identifies the Certification Authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it. Unless otherwise qualified, the term “Certificate” refers to Certificates issued to a Subscriber.
Certificate Class	A classification of Certificates by type as defined in § 3.2.3.1.
Certification Authority or CA	An authority trusted by one or more users to create and assign Certificates.
Certificate Policy or CP	A specialized form of administrative policy for electronic transactions performed during Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of Certificates. The Direct Ecosystem Community X.509 Certificate Policy is the governing policy on which this CPS is based in accordance with § 1.
Certification Practice Statement or CPS	A statement of the practices that Cerner employs in issuing, suspending, revoking, renewing and use of Certificates, in accordance with specific requirements provided in the CP, as defined by this document.
Certification Practice Statement (CPS) Policy	Identifies a pointer to a URI that contains the CPS defined by the Certification Authority.

Qualifier	
Certificate Revocation List or CRL	A list of Certificates that are revoked prior to their stated expiration date that is maintained by the CA that issued them.
Certificate Signing Request or CSR	A communication sent from an applicant requesting a digital signature.
Citizen	An individual participating in their own health care.
Compromise	The unauthorized disclosure of, loss of, loss of control over, or use of a Private Key associated with the Certificate or a reasonable suspicion thereof.
Direct Project	An initiative from the ONC that created a set of standards and services that, with a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
Distinguished Name or DN	A name given to an individual or organization which uniquely identifies it in the respective system.
Domain Name System or DNS	The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network.
Health Information Service Provider or HISP	A separate business organization that provides the management of security and transport as it relates to information exchange using Direct Project standards on behalf of the sending or receiving organization or individual. For purposes of this CPS, the HISP is Cerner.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, as amended.
Identity or ID	Information used to establish or prove a person's individuality.
Internet Engineering Task Force or IETF	A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
Object Identifier or OID	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.
ONC	Office of the National Coordinator for Health Information Technology
Online Certificate Status Protocol or OCSP	An internet protocol used for obtaining Certificate Revocation Lists.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Professional	An individual who acts on behalf of an organization which is a covered entity or business associate under HIPAA, or is a healthcare related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a Certificate.
Public Key Infrastructure or PKI	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the

	ability to issue, maintain, and revoke Public Key Certificates.
Registration Authority or RA	Entity responsible for identification and authentication of Certificate subjects, but that does not sign or issue certificates (i.e. a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Relying Party	An individual or entity who has received information that includes a Certificate and a digital signature verifiable with reference to a Public Key listed in the Certificate, and is in a position to rely on them. Responsibilities of the Relying Party are outlined in http://wiki.directproject.org/Best+Practices+for+HISP-HISP+Agreements.
Repository	The Certificate storage mechanism.
Secure Multipurpose Internet Mail Extensions or S/MIME	A standard for public key encryption and digital signing of email messages.
Subscriber or Cerner Direct Subscriber	An individual or organization that (1) is the subject named or identified in a Certificate issued to that individual or organization, (2) uses the Private Key corresponding to the Public Key listed in the Certificate for purposes of Direct Project message encryption, and (3) does not itself issue Certificates to another party.
Subscriber Applicant	An individual that requests Cerner Direct enabled communication on behalf of their organization.
Subscriber Agreements	Documents which set forth legal responsibilities and expectations concerning use of Cerner Direct.
Trusted Agent	An organization authorized to act as a representative of a Subscriber in confirming the Subscriber Applicant identification during the registration process.
Uniform Resource Identifier (URI)	A string of characters used to identify a name or a resource on the Internet.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Cerner is responsible for the repository functions for all Certificates generated from its role as CA. This includes the CA Certificate and the corresponding Certificates issued by the CA Certificate. Publishing of these Certificates into this repository is done in accordance with § 2.2.

The CA leverages the repository to publish notices of revocation in a CRL when a Subscriber's Certificate has been revoked. This list for Professional Class Certificates can be found at http://cernerdirect.com/professional/crl.

Additionally, the CA offers Relying Parties access to its Online Certificate Status Protocol (OCSP) services in accordance with the provisions of this CPS.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The CA maintains a CRL and exposes its location via URI in the CRL Distribution Points X.509v3 extension, conforming to RFC 5280 § 5, and hosted on redundant/highly available servers. The CA also maintains an equivalent Online Certificate Status Protocol (OCSP) Responder and publicly exposes its location in the Authority Information Access X.509 extension, conforming to RFC 5280 § 5.2, and hosted on redundant/highly available servers.

2.2.2 Publication of CA Information

This CPS is publicly accessible at the location specified in § 1.2 per the procedure defined in §1.5.4.

2.2.3 Interoperability

No stipulation.

2.3 Time or frequency of publication

This CPS is updated and published in accordance with § 9.12. Certificates are published to DNS upon issuance. The Cerner Direct CRL is issued every 5 minutes and is posted immediately.

2.4 Access controls on repositories

Read only access to this CPS document and the Cerner Direct repository are provided on the publicly-accessible web sites specified in § 1.5.4 and § 2.1. Unauthorized persons are prevented from creating, deleting, or modifying entries in the Certificate Repository through logical and physical security measures.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

As specified in the Direct Project Applicability Statement for Secure Health Transport, Professional Organization Certificates contain the domain name in the following:

1. The *subjectAltName* extension formatted as a dNSName, and
2. The Common Name (CN) of the Subject Distinguished Name (DN).

A listing of the CA Certificate DN attributes can be found in the table below.

Attribute	Value
Country (C) =	US
Organization (O) =	Cerner Corporation
Organizational Unit (OU) =	CernerDirect
State or Province (S) =	Missouri
Locality (L) =	Kansas City
Common Name (CN) =	CernerDirect Professional Community CA (Professional Class Certificate Use Only)

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

A listing of the Certificate DN attributes can be found in the table below and attributes have been authenticated according to § 3.2.

Attribute	**Value**
Country (C) =	US
Organization (O) =	Subscriber Organization Name on file.
Organizational Unit (OU) =	Not used.
State or Province (S) =	Subscriber Organization State.
Locality (L) =	Subscriber Organization Locality.
Common Name (CN) =	Subscriber Organization Direct Email Domain Name (Professional Organization Class Certificate Use Only)
E-Mail Address (E) =	Not used. Information stored in subjectAltName extension.

Table 2: x.501 Distinguished Name Attributes in Cerner Direct Certificates

3.1.2 Need for names to be meaningful

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

Names in the CA Certificate uniquely identify Cerner Direct as the CA and the applicable Certificate Class.

3.1.3 Anonymity or pseudonymity of Subscribers

The CA does not issue anonymous or pseudonymous Certificates.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The CA enforces name uniqueness within the X.500 namespace of the Certificate subject DN across all Cerner Direct Subscribers in that Certificate Class; however, a Subscriber can be issued multiple Certificates with the same subject DN.

3.1.6 Recognition, authentication, and role of trademarks

The CA will not knowingly use trademarks in names unless the subject of the Certificate possesses the rights to use that name.

3.2 Initial identity validation

3.2.1 Method to prove possession of Private Key

The CA generates the Private Key on behalf of the Subscriber; therefore no proof of Private Key possession is required.

3.2.2 Authentication of Organization Identity

The following is required from a Professional Subscriber Applicant who is submitting an application on behalf of an organization:

- Organization Name;
- Organization NPI (National Provider Identifier) or Organization EIN (Employer Identification Number);
- Organization Mailing Address;
- Requested Direct Domain Name;
- Documentation of the existence of the organization if not already known to the RA; and
- Acknowledgment and acceptance of the responsibilities for proper use of communications leveraging the Certificate, which are set forth in § 1.4.

The identity of the organization and other enrollment information provided by the Subscriber Applicant is confirmed in accordance with Cerner Direct's Identity Validation procedures.

At a minimum the RA shall:

- Verify the organization is a legal entity with valid reason to participate in Directed exchange through an existing contractual relationship to the RA, by using at least one third party database such as the National Plan and Provider Enumeration System (NPPES), or through a comparable procedure; and
- Confirm by telephone or comparable procedure certain information provided by the Subscriber Applicant and verify the applicant is authorized to act on behalf of the organization.

3.2.3 Authentication of individual identity

3.2.3.1 Authentication of Human Subscribers

The minimum authentication standard for each certificate class is specified in the table below.

Certificate Class	**Authentication of Individual Identity**
Professional Individual	A Professional Individual Certificate Class is a Professional seeking a Certificate representing themselves as an individual. This class is currently not supported.
Professional Organization	A Professional Organization Certificate Class is defined as a Professional seeking a Certificate on behalf of the organization they are representing. Identity for this class shall be established by in-person identify proofing before the RA, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities (e.g., notary public). Information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the Subscriber Applicant which is based on an in-person

	antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are a state or federally issued picture I.D. and an additional form of identification (non-picture I.D. is acceptable). Credentials presented must be unexpired.
Citizen	Citizen Certificate Class is defined as an individual participating in their own health care. This class is currently not supported.

Table 3: Authentication of Human Subscribers

3.2.3.2 Authentication of Subscribers for Role-based Certificates

No stipulation.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

A Professional Organization Class Certificate is considered a Group Certificate. Professional Organization Certificates are issued to an organization and allow its employees and agents to use Cerner Direct. Identity validation of the organization and its representative is covered in § 3.2.2 and 3.2.3.1.

3.2.3.4 Authentication of Devices

No stipulation.

3.2.4 Non-verified Subscriber information

All Subscriber information included in the Certificate is verified. A list of the Subscriber information specified in the Subject DN is outlined in § 3.1.1. The Certificate is issued within the timeframe specified in § 4.3.2.

3.2.5 Validation of authority

The RA verifies the association between an organization requesting a Professional Organization Class Certificate and the individual representing the organization under the procedures outlined in § 3.2.2.

3.2.6 Criteria for interoperation

Professional Organization Class Certificates issued by the CA conform to the Direct Ecosystem Community X.509 Certificate Policy. Cerner intends to conform to the Direct Citizen Community Certificate Policy when finalized.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

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

3.3.2 Identification and authentication for re-key after revocation

Associates manage this entire process for the Subscribers as it relates to their use of the Cerner Direct HISP.

3.4 Identification and authentication for revocation request

The CA reviews every revocation request for validity and authenticity. The CA Certificate Officer will complete approved revocation requests.

4. CERTIFICATE LIFE-CYCLE

4.1 Application

4.1.1 Submission of Certificate application

The RA creates the official Certificate signing request based on input received from the Subscriber application during the identity validation process.

4.1.2 Enrollment process and responsibilities

As part of the identity validation steps outlined in § 3.2, the Subscriber Applicant is responsible for providing accurate information, and the RA is responsible for archiving the Subscriber application and documentation of the application validation.

4.2 Certificate application processing

The CA and the RA verify the Certificate signing request for completeness and accuracy.

4.2.1 Performing identification and authentication functions

The identity validation of Subscribers shall be done by the RA as specified in § 3.2.

4.2.2 Approval or rejection of Certificate applications

The CA or the RA will approve a Certificate application upon:

- Successful validation of the identity as set forth in § 3.2;
- Successful validation of the Subscriber application; and
- Signed contract for Cerner Direct services.

The CA or the RA will reject a Certificate application if:

- Successful validation of the identity cannot be completed as set forth in § 3.2;
- Certificate signing request is incomplete or inaccurate;
- Contract for Cerner Direct services has not been signed;
- The CA or the RA, in their sole and exclusive judgment, believes the Subscriber Organization does not have a legitimate reason to participate in Direct communications;
- The CA or the RA, in their sole and exclusive judgment, believes the Subscriber Organization represents a risk to the professional reputation of Cerner; or
- For any other reason determined by Cerner in Cerner's sole and exclusive judgment.

4.2.3 Time to process Certificate applications

The CA issues a Certificate within 30 days of the completion of identity validation and verification of all Subscriber information placed in the Certificate.

4.3 Issuance

4.3.1 CA actions during Certificate issuance

The CA creates, issues, and publishes Certificates in its repository following validation of the credentials provided by the Subscriber to the RA as outlined in § 3.2. Information provided by the Subscriber is included in the fields described in § 3.1.

4.3.2 Notification to Subscriber of Certificate issuance

The CA notifies the Subscriber Applicant via physical mail or email when a Certificate has been issued for the Subscribing Organization, at which time the Subscriber Applicant shall become a Subscriber.

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

Use by the Subscriber of any application using the Certificate is considered acceptance of the Certificate.

4.4.2 Publication of the Certificate by the CA

The CA publishes Certificates in a directory specified in § 2.2.1.

4.4.3 Notification of Certificate issuance by the CA to other entities

If the RA is not Cerner, the CA notifies the RA when a Certificate has been issued for a Subscriber they verified.

4.5 Key pair and Certificate usage

4.5.1 Subscriber Private Key and Certificate usage

The CA does not allow a Subscriber to take possession of their Private Key. Certificate usage is described in § 1.4.

4.5.2 Relying Party Public Key and Certificate usage

Certificates conform to the policies provided by the Direct Ecosystem Community X.509 Certificate Policy. The CA publishes a certificate revocation list (CRL) and maintains an OCSP Responder as described in § 2.2.1.

4.6 Certificate renewal

The CA does not support Certificate renewal, rather, relies on Certificate re-key and posting of Certificate information via the methods described in § 2.2.

4.6.1 Circumstance for Certificate renewal

N/A

4.6.2 Who may request renewal

N/A

4.6.3 Processing Certificate renewal requests

N/A

4.6.4 Notification of new Certificate issuance to Subscriber

N/A

4.6.5 Conduct constituting acceptance of a renewal Certificate

N/A

4.6.6 Publication of the renewal Certificate by the CA

N/A

4.6.7 Notification of Certificate issuance by the CA to other entities

N/A

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 may be assigned a different validity period, key identifiers, specify a different CRL distribution point 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 may or may not be revoked in the CA's sole and exclusive judgment, but shall not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate re-key

To avoid interruption in service due to expiry, the CA must re-key the Certificate before expiration; however, the CA could re-key a Certificate after expiration. The CA could also execute a Certificate re-key at the request of an authorized party as specified in § 4.7.2. The CA will not re-key a revoked Certificate.

4.7.2 Who may request Certification of a new Public Key

An RA or the Subscriber may request the re-key of a Certificate.

4.7.3 Processing Certificate re-keying requests

The CA approves or rejects Certificate re-keying requests in their sole and exclusive judgment. Identity validation of the Subscriber will rely on identity validation completed before Certificate issuance or shall be equivalent to the initial identity validation steps found in § 3.2.

4.7.4 Notification of new Certificate issuance to subscriber

Notification of Certificate issuance to the Subscriber is in accordance with § 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

Conduct constituting acceptance of a Certificate is set forth in § 4.4.1.

4.7.6 Publication of the re-keyed Certificate by the CA

The CA publishes the Certificates in the repository specified in § 2.2.1.

4.7.7 Notification of Certificate issuance by the CA to other entities

If an RA submitted the re-key request, the CA notifies the RA in accordance with § 4.4.3.

4.8 Modification

The CA does not support Certificate modification, rather, relies on Certificate issuance or re-key and posting of Certificate information via the methods described in § 2.2.

4.8.1 Circumstance for Certificate modification

N/A

4.8.2 Who may request Certificate modification

N/A

4.8.3 Processing Certificate modification requests

N/A

4.8.4 Notification of new Certificate issuance to Subscriber

N/A

4.8.5 Conduct constituting acceptance of modified Certificate

N/A

4.8.6 Publication of the modified Certificate by the CA

N/A

4.8.7 Notification of Certificate issuance by the CA to other entities

N/A

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The CA will revoke a Certificate and publish the status in accordance with § 2.2 in its sole and exclusive judgment, for any reason, including but not limited to:

- The identifying information or affiliation components of any names in the Certificate become invalid;
- Reason to believe information provided by the Subscriber during application for the Certificate is false or misleading;
- Reasonable suspicion by the CA that the Private Key is Compromised;
- Request from the Subscriber to revoke his/her Certificate;
- The Subscriber violates the terms of the Subscriber Agreement; or
- Termination or expiration of the Subscriber Agreement with the Subscriber.

4.9.2 Who can request revocation

The following can request a Certificate to be revoked:

- An authorized representative (e.g. Cerner Direct Administrator) of the Subscriber;

- An authorized representative of the RA when the RA performed the initial identity validation; or
- An Associate, on behalf of the CA.

4.9.3 Procedure for revocation request

Revocation requests for Subscribers within the Professional Organization classes shall be in accordance with § 3.4. The Certificate Officer (as defined in § 5.2) will review the request and reason to ensure that the Certificate revocation request is not malicious and will verify that the reason for revocation is valid.

Approved revocation requests will be posted to the repository in accordance with § 2.2.

4.9.4 Revocation request grace period

Authorized parties outlined in § 4.9.2 shall request the revocation of a Certificate within a commercially reasonable amount of time from the time the need for revocation comes to their attention.

4.9.5 Time within which CA must process the revocation request

The CA takes commercially reasonable steps to process revocation requests within 8 hours of receipt. CRL issuance frequency is addressed in § 4.9.7.

4.9.6 Revocation checking requirement for relying parties

The Relying Party shall determine how often new revocation data should be obtained and reviewed. Information on how to access these resources is set forth in § 2.2.1.

4.9.7 CRL issuance frequency

The CA issues and posts the CRL to the repository listed in § 2.1 per the frequency specified in § 2.3. The CA removes all superseded CRLs from the repository upon posting of the latest CRL.

4.9.8 Maximum latency for CRLs

The CA makes commercially reasonable efforts to post the CRL promptly.

4.9.9 On-line revocation/status checking availability

Relying Parties can utilize the OCSP Responder referenced in § 2.2.1.

4.9.10 On-line revocation checking requirements

On-line revocation checking requirements are in accordance with § 4.9.6.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements related to key Compromise

The CA uses commercially reasonable efforts to notify known Relying Parties if it discovers, or has reason to believe, that there has been a Compromise of the CA’s Private Key.

4.9.13 Circumstances for suspension

The CA does not support suspension of 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 CRL and an OCSP responder. The location of both the CRL and the OCSP responder are published in each Certificate using the appropriate x509v3 extension in accordance with § 2.2.1.

4.10.2 Service availability

Certificate status services are hosted on highly available and redundant servers.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

The CA will revoke any unexpired Certificate of a Subscriber upon termination or expiration of their Subscriber Agreement. Certificates that expired during the term of a Subscriber Agreement will not be revoked.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

The CA does not support key escrow and recovery for Certificates.

4.12.2 Session key encapsulation and recovery policy and practices

The CA does not support key escrow and recovery for Certificates.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Cerner, as the CA, hosts all technology necessary for support of this CPS in Cerner's Technology Centers (CTC). The CTC is ISO 9001:2008 and SSAE-16 certified to show Cerner is executing on its stated policies.

5.1.1 Site location and construction

The CTC is protected by multiple layers of physical security including an off-site alternate CTC, which greatly reduces the probability of a single security or disastrous event causing a significant degradation or cessation of service.

5.1.2 Physical access

All primary doors are controlled by card access, with combination card and biometric readers in high-security areas. Cerner adheres to the concept of least-privileged access using NIST best practices. Access is logged for auditing purposes.

5.1.3 Power and air conditioning

The CTC has a fully redundant power and air conditioning environment. Uninterrupted power is achieved through redundant infrastructure, including a dedicated utility substation, dual carriers, routers, switches and LAN, dedicated power transformers, and battery backup plus multiple industrial-grade generators. The CTC is supplied with redundant precision cooling units fed from redundant building piping systems, to protect against a single leak affecting any cooling abilities. All related systems are monitored continuously and inspected regularly.

5.1.4 Water exposures

The CTC's "building within a building" design and redundant building piping system virtually eliminate the risk of water exposure to any hosted systems.

5.1.5 Fire prevention and protection

Fire protection systems are monitored at multiple command and control rooms within the CTC and from Cerner's Security Operations Center. The local city fire departments inspect the fire system annually, as does a contracted third party supplier. All fire systems are connected to emergency backup power sources.

5.1.6 Media storage

The backup and restore architecture is based on short-term backups on disk and long-term backups on tape. This allows for two copies of the backups to be available during the critical time period, providing redundancy and data corruption protection. All media storage is both physically and logically secured and protected from accidental damage via methods described in this § 5.1.

5.1.7 Waste disposal

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

5.1.8 Off-site backup

Cerner conducts regularly scheduled backups of critical system data. Copies of backups are kept off-site at a secure CTC location.

The Cerner Root CA, used to generate the CA Certificate, is backed up on dedicated removable media but is not stored off-site.

5.2 Procedural controls

5.2.1 Trusted roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The CA has processes for screening and training these individuals. Details of these processes can be found in § 5.3.

Cerner leverages four roles as it relates to administration of the CA.

1. Administrator
2. Officer
3. Auditor
4. Operator

Some roles may be combined. The following subsections provide a detailed description of the responsibilities for each role.

5.2.1.1 Administrator

The administrators of the CA are Associates assigned to the CTC. They are responsible for:

- Installing, configuring, and generally maintaining the CA technology;
- Establishing and maintaining CA technology system accounts;
- Configuring Certificate profiles or templates and audit parameters; and
- Generating and backing up the CA Certificate.

Administrators do not issue Certificates to Subscribers.

5.2.1.2 Officer

The officers of the CA and RA are Associates dedicated to Cerner Direct and they are responsible for:

- Registering new Subscribers;
- Reviewing the Subscriber application and accuracy of information included in Certificates;
- Approving and executing the issuance of Certificates; and
- Requesting, approving and executing the revocation of Certificates.

5.2.1.3 Auditor

The auditor is responsible for:

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

5.2.1.4 Operator

The operators of the CA are Associates assigned to the CTC. They are responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.2 Number of persons required per task

Cerner trains at least two Associates for each task, but only one Associate is required to execute each task.

5.2.3 Identification and authentication for each role

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

5.2.4 Roles requiring separation of duties

Any properly trained individual may assume the operator, administrator, and/or officer role. An Associate may not assume the auditor role in conjunction with any of these roles.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Associates have been subject to the background check procedures outlined in the subsequent section.

5.3.2 Background check procedures

As part of Cerner's hiring process, offer-stage candidates have been subject to a background check. The background check for U.S. applicants is comprised of the following components, as applicable to each candidate:

- Employment History Dating Back Ten Years
- Education Verification (Highest Degree)
- Criminal Search
- Social Security Number Verification
- FACIS (Fraud & Abuse Control Information System) List
- U.S. Government Terrorist List

Additional checks may be deemed appropriate according to the offer-stage candidate's role and may include, but are not limited to, the following:

- Professional License Check
- Credit Check
- Office of Inspector General (OIG) Check
- Drug Screen

5.3.3 Training requirements

Initial training plans are assigned based on role and organization placement. For all trusted roles this includes, but is not limited to, information on Cerner, quality systems, regulatory overview, information privacy and security requirements, and process and procedure. Ongoing training is based on the Associate's role and is a continual part of each Associate's development.

5.3.4 Retraining frequency and requirements

Retraining is on an as-needed basis to ensure personnel meet the training requirements and level of proficiency necessary to perform their job responsibilities competently. Documentation of training requirements is maintained by Cerner's centralized online training solution.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

Independent contractors are required to sign a non-disclosure agreement (NDA) and contract that defines CTC security requirements. Prior to being granted any network connectivity, all third party entities must agree to adhere to the same network access policy requirements as Cerner personnel.

5.3.8 Documentation supplied to personnel

Associates are provided a learning plan and the related documentation necessary to perform their job responsibilities competently.

5.4 Audit logging procedures

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

5.4.1 Types of events recorded

The following significant events are logged automatically:

- Certificate Management Events:
  - o Authentication into the certificate management application(s);
  - o Certificate request generation;
  - o Certificate issuance;
  - o Read access to the Certificate repository;
  - o Certificate revocation; and
  - o Access to machine(s) and file system hosting the certificate services and repositories.
- Security-related events including:
  - Successful and unsuccessful user authentication;
  - Creation and modifications to user accounts; and
  - Successful and unsuccessful user data access.

Log entries include the following elements:

- Date and time of the entry;
- Type of significant event;
- Identity of the entity (ie. solution or service) recording the entry; and
- User information of person performing the significant event, if applicable.

5.4.2 Frequency of processing log

Audit logs are reviewed when an issue is suspected.

5.4.3 Retention period for audit log

Audit logs are kept for a period of no less than 2 months.

5.4.4 Protection of audit log

Audit logs for the security-related events are protected in accordance to the CernerWorks Logging Policy designed to meet objective A.10.10 of ISO/IEC 27001:2005(E). Full access to the log data is limited to the CTC Security Team. Audit logs for certificate management events utilize the same centralized auditing architecture as other HIPAA covered services hosted within CTC.

5.4.5 Audit log backup procedures

A backup of the audit data is performed daily and stored off-site in another CTC facility.

5.4.6 Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level at all times while the CA is in operation. Audit events related to the issuance and maintenance of Certificates are designed to retain the audit events for replay in the event that the audit system fails.

5.4.7 Notification to event-causing subject

The subject is not notified of the audit event.

5.4.8 Vulnerability assessments

Standard CTC vulnerability scans have been completed on the Intermediate CA system. Findings were addressed within 30 days of the scan results per CTC standards. Additional vulnerability scans will be scheduled in Cerner’s sole and exclusive judgment.

5.5 Records archival

5.5.1 Types of records archived

Records related to the Certificate Life-cycle detailed in § 4 are archived. This includes:

- CPS;
- Documentation related to Certificate Applications;
- Audit logs detailed in § 5.4; and
- Issued Certificates;

5.5.2 Retention period for archive

Archives are retained for a minimum of three years.

5.5.3 Protection of archive

Archives are protected according to the same requirements as § 5.4.4.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

Artifacts related to the Certificate Life-cycle contain time and date information (i.e. Certificates, CRLs, related database entries). Manual documentation related to Certificate Applications contains date information.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

The CA will not issue Certificates if the issuing CA Certificate expires in less than one year. The time period is set in accordance with the operational period for Certificates documented in § 6.3.2.

To minimize risk to the PKI through compromise of the CA Private Key, the CA will generate a new private signing key for the CA Certificate at a minimum every 5 years or earlier based on Cerner's sole and exclusive judgment.

The CA Certificate is valid for no more than 20 years.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

If a potential compromise of the CA Certificate becomes known, the CPC and/or appropriate Associates in trusted roles will investigate in order to determine the nature and the degree of damage. The scope of potential damage shall be assessed in order to determine if the CA Certificate needs to be rebuilt, only some certificates need to be revoked, and/or the CA Certificate key needs to be declared compromised.

5.7.2 Computing resources, software, and/or data are corrupted

In the event of the corruption of computing resources, software, and/or data, the CTC's 24x7x365 support staff is notified manually or by automated alerts. The support staff follows the CTCs incident handling procedures. If necessary, the procedures in § 5.7.3 and 5.7.4 will be initiated.

5.7.3 Entity private key compromise procedures

If the Root Cerner CA or Intermediate Cerner Direct CA Certificates are compromised, they will be revoked and a new Intermediate Cerner Direct CA Certificate will be issued. Until the new CA Certificate is distributed in accordance with § 6.1.4, Relying Parties will no longer trust the CA Certificate or any Certificates issued by that CA Certificate. There is no security risk to the CA or Relying Parties following Direct Project best practices in having a revoked Certificate in their trust store.

5.7.4 Business continuity capabilities after a disaster

In the case of a disaster involving any aspect of the CTC, the CTC Associates will implement the CTC Business Continuity and Disaster Recovery plan. If CA operations are affected, Associates will implement the supplemental BCDR plan for the CA to restore operations as quickly and safely as possible. The CPC will be involved to make the determination if a compromise has occurred and the appropriate way to resume operations of the CA.

5.8 CA or RA termination

In the event of CA termination, the CA will revoke the CA Certificate and can revoke non-expired Certificates if necessary.

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 is generated on physical hardware that is well protected according to the physical controls in § 5.1.

6.1.1.2 Subscriber Key Pair Generation

The CA cryptographic keying material generated for Certificates is created on physical hardware that is well protected according to the physical controls in § 5.1.

6.1.2 Private Key delivery to Subscriber

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

6.1.3 Public Key delivery to Certificate Issuer

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

6.1.4 CA Public Key delivery to relying parties

The CA Certificate Public Key is delivered to Replying Parties within a self-signed Certificate using secure FTP.

6.1.5 Key sizes

The CA utilizes the SHA-256 algorithm for all Certificate signatures. Key size is at least 2048 bits (RSA).

6.1.6 Public key parameters generation and quality checking

The CA generates the Public key parameters prescribed in the Digital Signature Standard (DSS) in accordance with FIPS 186-2.

The CA performs parameter quality checking (including primality testing for prime numbers) in accordance with FIPS 186.

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

Certificates assert the following key usage bits:

- digitalSignature
- keyEncipherment

Certificates also assert an extended key usage bit of *emailProtection*. No Basic Constraint extension is used therefore the relying party must assume *CA:FALSE*.

The CA Certificate asserts the following key usage bits:

- cRLSign
- keyCertSign

The CA Certificate 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

Cryptographic modules are compliant with US FIPS 140-2 Level 1.

6.2.2 Private Key (n out of m) multi-person control

No stipulation.

6.2.3 Private Key escrow

No Private Keys (CA Certificate or Subscriber Certificate) are escrowed.

6.2.4 Private Key backup

The Cerner Root CA Certificate is backed up on dedicated removable media but is not stored off-site. Subscriber Private Keys are backed up regularly and stored offsite at one of the other CTC facilities.

6.2.5 Private Key archival

No stipulation.

6.2.6 Private Key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private Key storage on cryptographic module

No stipulation.

6.2.8 Method of activating Private Key

No stipulation.

6.2.9 Method of deactivating Private Key

No stipulation.

6.2.10 Method of destroying Private Key

Private Key signatures are not destroyed in conformance with the Certificate Policy referenced in § 1; however, it is expected that by end of 2012 Cerner will be in conformance with this requirement.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are archived as part of the certificate archival process specified in § 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The CA Certificate Private Key is used for a maximum of 5 years in accordance with § 5.6. The CA Certificate expires after a maximum of 20 years.

Certificates expire one year from date of issuance. A new key pair is generated when a new Certificate is issued.

6.4 Activation data

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All CA hardware requires authenticated logins. All logins are audited in accordance with § 5.4. Access control measures are in place in accordance with personnel controls in § 5.3.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

Cerner follows a modern development process that meets ISO 9001:2008. All CA hardware and software are dedicated to Cerner Direct CA functions. Hardware and software updates are performed in accordance to the change control policy in § 6.6.2.

6.6.2 Security management controls

The CTC follows the CernerWorks Change Management Policy which requires all changes to be evaluated, documented, and approved before implementation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

Information transferred from the CA is done through dedicated removable media or secure networks. The CTC follows the CernerWorks Managed Services Network Security Policy designed to comply with the Network System Management requirements of ISO/IEC 27001:2005(E).

6.8 Time-stamping

CA servers with network access have Network Time Protocol enabled in accordance with Cerner Works Managed Services Network Security Policy. A manual process ensures the time is accurate to within three minutes on the off-network root CA hardware.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Cerner Direct uses Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 (“RFC 5280”) as a basis for the Certificate profiles. Additionally, Cerner Direct uses X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 1999 (“RFC 2560”).

A listing of the Certificates basic profile fields and associated values are:

Field	**Expected Value or Value Constraint**
Serial Number	Unique value per Issuer DN
Signature Algorithm	Object Identifier (OID) of the certificate signing algorithm indicated in § 7.1.3.
Issuer DN	Reference §7.1.4.
Valid From	UTCTime (Universal Time Type) as per RFC 5280.
Valid To	UTCTime (Universal Time Type) as per RFC 5280.
Subject DN	Reference §7.1.4.
Subject Public Key	Encoded as per RFC 5280.
Signature	Generated and encoded as per RFC 5280.

Table 4: Cerner Direct Certificate Basic Profile Fields

7.1.1 Version number(s)

The CA issues X.509 v3 Certificates, indicated by the version field containing the integer 2.

7.1.2 Certificate extensions

Certificates leverage the following extensions in compliance with RFC 5280:

- The Key Usage, Extended Key Usage, and Basic Constraints extensions are populated as specified in § 6.1.7;
- The CRL Distribution Points extension is populated with a CRL URI as specified in § 2.2.1;
- The Authority Information Access extension is populated with an OCSP Responder location as specified in § 2.2.1;
- The Subject Alternative Name extension is populated as specified in § 3.1.1; and
- The Certificate Policies extension is populated as defined in § 7.1.6.

7.1.3 Algorithm object identifiers

Certificates are signed with the following algorithm:

sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates 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

Reference § 3.1.1.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

Reference § 1.2

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

The Certificate Policy Extension field is populated for CA Certificates as specified in § 1.2. The Subscriber Certificates do not contain any policy qualifiers.

7.1.9 Processing semantics for the critical Certificate Policies extension

The *certificatePolicies* extension is a non-critical extension, but Relying Parties whose client software does not process this extension risk using Certificates inappropriately.

7.2 CRL profile

7.2.1 Version number(s)

The CA issues X.509 version 2 CRLs, indicated by the version field containing the integer 1.

7.2.2 CRL and CRL entry extensions

The CA conforms to the CRL and CRL Extensions profile defined in RFC 5280 with non-critical extensions listed in the table below, and 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}

Delta CRLs are leveraged using the critical delta CRL indicator extension.

Extensions/Entry Extensions	**Expected Value or Value Constraint**
CRL Number	Monotonically increasing sequence number up to 20 octets.
Authority Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
Reason Code	unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5),

Table 5: Cerner Direct CRL Non-Critical Extensions/Entry Extensions

The CRL will contain a CRL Reason Code entry extension for each entry.

7.3 OCSP profile

7.3.1 Version number(s)

The CA leverages X.509 Version 1 of the OCSP specification as defined by RFC 2560.

7.3.2 OCSP extensions

Certificates use the Authority Information Access extension to specify the location of the OCSP Responder as specified in § 2.2.1.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CPC is comprised of representatives from the significant organizations within Cerner responsible for operation of the CA. Currently, it is the responsibility of the each CPC representative to ensure their organization is following the policies and procedures in this document.

8.1 Frequency or circumstances of assessment

The facility, management, and operational controls within the CTCs are reviewed on an annual basis as per SSAE 16 recommendations. Although no additional review has been implemented by the CA, a compliance review will be conducted at least every 2 years after the initial publication of this CPS document.

8.2 Identity/qualifications of assessor

The CTC employs an external assessor to perform a semi-annual review of its internal controls and publishes an SSAE 16 which is an attestation or report on those controls. For the CA assessment, it is expected Cerner's Quality Management organization will provide assessors with initial review by an external assessor. Assessors within the organization have experience with ISO, SSAE 16, FDA, and other industry standard reviews.

8.3 Assessor's relationship to assessed entity

The Declaration of Conformance has not been made available by DirectTrust.org as specified in CP § 8.

8.4 Topics covered by assessment

The SSAE 16 includes but is not limited to the following:

- Site Description;
- Network Security;
- Physical Security;
- Commitment to Quality;
- Risk Management;
- Control Activities;
- Monitoring; and
- Information and Communication

8.5 Actions taken as a result of deficiency

Any deficiencies identified as a result of the CTC's SSAE 16 semi-annual review are remediated via a formal action plan.

8.6 Communication of results

The CTC's most recent SSAE 16 is available for review by any CTC client that requests to review the report.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees set forth in the Subscriber Agreement include Certificate issuance and renewal fees.

9.1.2 Certificate access fees

The CA does not charge for access and use of the Certificates by Relying Parties. The fees set forth in the Subscriber Agreement include fees for access to a Certificate by a Subscriber.

9.1.3 Revocation or status information access fees

The CA does not charge a fee for access to revocation or status information using the methods indicated in § 2.2.

9.1.4 Fees for other services

Not applicable.

9.1.5 Refund policy

The CA does not issue refunds.

9.2 Financial responsibility

9.2.1 Insurance coverage

The CA maintains commercial general liability insurance of not less than $5,000,000 per occurrence and in aggregate, errors and omissions liability insurance of not less than $5,000,000 per occurrence and in aggregate, and worker's compensation insurance at or greater than the minimum levels required by applicable law. The CA maintains a minimum of $1,000,000 per occurrence and in aggregate for network security, privacy protection and notification coverage. Policies shall be maintained by a carrier rated A or higher by AM Best.

The RA shall maintain commercial general liability insurance of not less than $5,000,000 per occurrence and in aggregate, errors and omissions liability insurance of not less than $5,000,000 per occurrence and in aggregate, and worker's compensation insurance at or greater than the minimum levels required by applicable law. The RA is encouraged to maintain a minimum of $1,000,000 per occurrence and in aggregate for network security, privacy protection and notification coverage. Policies shall be maintained by a carrier rated A or higher by AM Best.

The Subscriber is encouraged to maintain commercially reasonable levels of the following types of insurance: (i) commercial general liability, (ii) errors and omissions liability, (iii) worker's compensation, and (iv) network security, privacy protection and notification coverage.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential Information means any information that (a) is clearly marked as confidential, (b) that by its nature or context should reasonably be understood to be confidential, and (c) the information specifically set forth in the list below.

- Subscriber applications;
- Audit logs for types specified in § 5.4.1;

- Cerner policies and procedures related to this CPS; and
- Audit reports and related documentation

9.3.2 Information not within the scope of confidential information

Confidential Information will not include any information (i) that is publicly available through no breach of this CPS, (ii) that is independently developed by Subscriber, RA, or CA, or (iii) that is rightfully acquired by Subscriber, RA, or CA from a third party who is not in breach of an agreement to keep such information confidential. Except as expressly permitted by this CPS, neither Subscriber, RA nor CA will disclose, use, copy, distribute, sell, license, publish, reproduce or otherwise make available confidential information of others.

9.3.3 Responsibility to protect confidential information

CA, RA, and Subscriber will each (i) secure and protect confidential information by using the same or greater level of care that it uses to protect its own confidential and proprietary information of like kind, but in no event less than a reasonable degree of care, and (ii) require that each of their respective employees, agents, attorneys and independent contractors who have access to such confidential information are bound to at least as restrictive confidentiality terms as this § 9.3. Notwithstanding the foregoing, any party may disclose another party's confidential information to the extent required by applicable law or regulation or by order of a court or other governmental entity, in which case, if permitted, such party will notify the other disclosing party as soon as practicable prior to such party making such required disclosure.

9.4 Privacy of personal information

9.4.1 Privacy plan

CA protects the privacy of the information sent through Cerner Direct in accordance with its privacy policy which can be found at https://cernerdirect.com.

9.4.2 Information treated as private

See §9.3.1.

9.4.3 Information not deemed private

See §9.3.2.

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

Private information may be used by CA in accordance with this CPS, the privacy policy referenced in § 9.4.1, and applicable Subscriber Agreements.

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

Cerner has and shall retain sole and exclusive right, title and interest, including copyright and all other rights, in and for the Cerner Direct services. Cerner hereby reserves all rights not expressly granted hereunder.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The CA warrants that it will perform the functions outlined in this CPS in accordance with applicable laws and regulations and in a professional manner in accordance with this CPS. Subscriber Agreements may include additional representations and warranties.

9.6.2 RA representations and warranties

The RA warrants that (i) the information provided by the RA within the Certificate is true and correct, (ii) it has completed required identity verification as set forth in § 3, and (iii) it perform the functions of an RA in a professional manner and in accordance with applicable laws and regulations and this CPS.

9.6.3 Subscriber representations and warranties

Subscriber warrants that (i) the information provided by the Subscriber within the Certificate is true and correct, (ii) it has completed required identity verification as set forth in § 3, (iii) the Certificate will be used in conformance with this CPS and all applicable laws and regulations. Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying party representations and warranties

Relying Party warrants that (i) it will only use Certificates for the purpose for which they were intended, and for no other purposes whatsoever, and in compliance with all applicable laws and regulations and this CPS, (ii) it will check each Certificate for validity and authenticity, (iii) it will promptly notify CA of any issues or problems with a Certificate of which it becomes aware, and (iv) Relying Party's decision to rely on the information within a Certificate is solely its responsibility.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

To the maximum extent permitted by law, the CA will not be liable under this CSP for lost revenues or direct, indirect, special, incidental, consequential, exemplary, or punitive damages, even if the claimant knew or should have known that such damages were possible and even if direct damages do not satisfy a remedy.

9.9 Indemnities

To the extent permitted by applicable law, the RA agrees to indemnify, defend and hold the CA harmless from and against all claims, damages, costs and expenses ("Claims") brought by a third party against the CA which arise out of or are related to RA's breach of its obligations under or the terms of this CPS. The terms of the preceding sentence shall not apply in the event that both the CA and the RA are Cerner.

To the extent permitted by applicable law, the Subscriber agrees to indemnify, defend and hold the CA harmless from and against all Claims brought by a third party against the CA which arise out of or are related to (i) Subscriber's breach of its obligations under or the terms of this CPS, and (ii) its use of Cerner Direct, other than those claims arising out of or related to the CA's negligence or willful misconduct in providing Cerner Direct. Additional indemnities may be found in the Subscriber Agreement.

9.10 Term and termination

9.10.1 Term

The CPS is effective immediately upon publication. Subsequent revisions approved and published in accordance with § 1.5.4 will supersede all prior versions and become effective immediately upon publication.

9.10.2 Termination

Termination of this CPS may occur if approved by the CPC.

9.10.3 Effect of termination and survival

The requirements of this CPS shall remain in effect until the end of the validity period for all Certificates issued by the CA Certificate governed by this CPS.

9.11 Individual notices and communications with participants

Notices will be given in commercially reasonable manner, as dictated by the circumstance.

9.12 Amendments

9.12.1 Procedure for amendment

This CPS may be amended by the CPC in accordance with § 1.5.4.

9.12.2 Notification mechanism and period

The CA may provide notification of a change to this CPS in its sole and exclusive judgment.

9.12.3 Circumstances under which OID must be changed

The CPS Pointer qualifier defined in § 1.2 is subject to change during the amendment approval process in Cerner's sole and exclusive judgment.

9.13 Dispute resolution provisions

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

9.14 Governing law

This CPS shall be governed by the laws of the state Missouri, excluding Missouri's conflicts of laws rules.

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CPS constitutes the entire agreement related to the subjects herein and supersedes all prior or contemporaneous agreements, representations and proposals, written or oral, if any, regarding such subjects.

9.16.2 Assignment

No Certificate issued under this CPS may be assigned without prior written approval of the CA. The CA may assign its rights and obligations under this CPS in its sole discretion.

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other provisions

No stipulation.