Cerner Direct

Certification Practice Statement

Version 2.0

Effective Date: January 16, 2014

Cerner Corporation

2800 Rockcreek Parkway

Kansas City, MO 64117

1-816-201-1024

www.cerner.com

Table of Contents

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) and Registration Authority (RA) 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 Trust Community X.509 Certificate Policy[1] (CP) is the governing policy on which this CPS is based. The CP provides specific requirements necessary to ensure integrity of Directed exchanges within this community intended to be fully consistent with the Federal Bridge Certificate Authority (FBCA) Certificate Policy at the Basic assurance level and the Identity Vetting requirements of NIST Special Publication 800-63-1. 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.

This 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).

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 Health Information Service Provider (HISP) called Cerner Direct which includes the CA and RA functions for the HISP.

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 for Level of Assurance 3 (DT.org LoA 3).

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 the 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

[1] This CPS is governed by the then current version of the Direct Trust Community X.509 Certificate Policy. At the time of publication of this CPS, the current CP version is 1.2.

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)

Cerner is the Registration Authority (RA) that collects and verifies identity information from Subscribers using procedures that implement the identity validation policies set forth in this document. This CPS also serves as the Registration Authority Practice Statement (RPS).

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.

1.3.3.1 Health Information Service Providers (HISPs)

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

1.3.4 Relying Party

A Relying Party 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 Relying Party 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
This CPS can be updated as needed at any time, but at minimum, it will be reviewed annually. 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 certified data center facilities which host the Certificate infrastructure. The CTC undergoes a bi-annual SSAE No. 16, Type II, assessment.
Certificate	A digital representation of information which (1) identifies the Certification Authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it. Unless otherwise qualified, the term “Certificate” refers to Certificates issued to a Subscriber.
Certificate Class	A classification of Certificates by type as defined in § 3.2.3.1.
Certification Authority or CA	An authority trusted by one or more users to create and assign Certificates.
Certificate Policy or CP	A specialized form of administrative policy for electronic transactions performed during Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of Certificates. The DirectTrust Ecosystem Community X.509 Certificate Policy is the governing policy on which this CPS is based in

	accordance with § 1.
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 Qualifier	Identifies a pointer to a URI that contains the CPS defined by the Certification Authority.
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	An entity that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital certificate. Acting in the capacity of an agent for the Subscriber, the HISP may hold and manage PKI private keys associated with a Direct digital certificate on behalf of the Subscriber. For purposes of this 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.
Information Systems Security Officer or ISSO	An individual responsible for establishing and maintaining the enterprise vision, strategy and program as it relates to information systems security, to ensure information assets are adequately protected.
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.
Trust Bundle	A collection of trust anchors that comply with a common set of policies and represent trust communities.
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 and RA. This includes Subscriber Agreements, 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.

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

2.1.1 Repository Obligations

All repositories mentioned in § 2.1 are located within the CTC on redundant/highly available servers.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

Cerner maintains a CRL and exposes its location via URI in the CRL Distribution Points X.509v3 extension, conforming to RFC 5280 § 5. Cerner 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.

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. Subscriber Agreements are posted to an internal document repository, and accessible only by those within the Trusted Roles defined in § 5.2.1. Certificates are published to DNS upon issuance. The Cerner Direct CRL is issued every 2 minutes and is posted immediately.

2.4 Access controls on repositories

Read only access to this CPS document and the certificate status repositories 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 Subscriber Agreement, Intermediate CA Certificate and Subscriber Certificate repositories 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

Cerner does not issue anonymous or pseudonymous Certificates.

3.1.4 Rules for interpreting various name forms

Certificate DNs are interpreted using X.500 standards.

3.1.5 Uniqueness of names

Cerner 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

Subscribers may not request certificates with any content that infringes the intellectual property rights of another entity. Cerner may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2 Initial identity validation

3.2.1 Method to prove possession of Private Key

Cerner 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;
- Organization Healthcare Category which must be one of the following:
  - HIPAA Covered Entity;
  - HIPAA Business Associate; or
  - Healthcare-related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA. Each organizational certificate must represent a legally distinct entity.
- Requested Direct Domain Name;
- Documentation of the existence of the organization if not already known to the RA;
- Self attestation that the organization is either a (i) HIPAA covered entity or business associate, or (ii) healthcare related organization which treat protected health information with privacy and security protections that are equivalent to those required by HIPAA; and
- Acknowledgment and acceptance of the responsibilities including, but not limited to 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 Cerner shall verify the organization is a legal entity with valid reason to participate in Directed exchange through an existing contractual relationship with Cerner, by

using at least one third party database such as the National Plan and Provider Enumeration System (NPPES), or through a comparable procedure.

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 of the Professional and the HISP ISSO shall be established by in-person identify proofing before Cerner, 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 identification. Credentials presented must be unexpired. Identity vetting process is performed in compliance with DirectTrust.org Level of Assurance (LoA) 3.
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 Human Subscribers for Role-based Certificates

Not applicable.

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 representatives is covered in § 3.2.2 and 3.2.3.1.

3.2.3.4 Authentication of Devices
Not applicable.

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

3.2.5 Validation of authority
Cerner 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 Cerner conform to the DirectTrust Ecosystem Community X.509 Certificate Policy.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key
Cerner manages this process on behalf of the Subscriber as it relates to their use of the Cerner Direct HISP. Cerner 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
If a Certificate is revoked, the Subscriber shall go through the initial identity verification process described in section 3.2 to obtain a new certificate.

3.4 Identification and authentication for revocation request
Cerner reviews every revocation request for validity and authenticity. A Certificate Officer will complete approved revocation requests.

4. CERTIFICATE LIFE-CYCLE

4.1 Application

4.1.1 Submission of Certificate application
Cerner 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, a Subscriber is responsible for providing accurate information about him/herself and his/her organization during identity verification. Cerner is responsible for ensuring that the identity of each Subscriber Applicant is verified in accordance with this CPS prior to the issuance of a Certificate. Cerner authenticates and keeps confidential all communication made during the certificate application process.

4.2 Certificate application processing

Cerner verifies 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 Cerner as specified in § 3.2.

4.2.2 Approval or rejection of Certificate applications

Cerner 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.

Cerner 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;
- Cerner, in their sole and exclusive judgment, believes the Subscriber Organization does not have a legitimate reason to participate in Direct communications;
- Cerner, 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

Cerner 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

Cerner creates, issues, and publishes Certificates in its repository following validation of the credentials provided by the Subscriber 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

Cerner 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

Cerner publishes Certificates in a directory specified in § 2.2.1.

4.4.3 Notification of Certificate issuance by the CA to other entities
No stipulation.

4.5 Key pair and Certificate usage

4.5.1 Subscriber Private Key and Certificate usage
Cerner 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 Trust Community X.509 Certificate Policy. Cerner publishes a certificate revocation list (CRL) and maintains an OCSP Responder as described in § 2.2.1. Relying Parties should process the CRL on a regular basis and reject Certificates found on the CRL or respect the Certificate status reflected in an OCSP response.

4.6 Certificate renewal

Cerner 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
Not applicable.

4.6.2 Who may request renewal
Not applicable.

4.6.3 Processing Certificate renewal requests
Not applicable.

4.6.4 Notification of new Certificate issuance to Subscriber
Not applicable.

4.6.5 Conduct constituting acceptance of a renewal Certificate
Not applicable.

4.6.6 Publication of the renewal Certificate by the CA
Not applicable.

4.6.7 Notification of Certificate issuance by the CA to other entities
Not applicable.

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 Cerner'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, Cerner must re-key the Certificate before expiration; however, Cerner could re-key a Certificate after expiration. Cerner could also execute a Certificate re-key at the request of an authorized party as specified in § 4.7.2. Cerner will not re-key a revoked Certificate.

4.7.2 Who may request Certification of a new Public Key

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

4.7.3 Processing Certificate re-keying requests

Cerner 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

If the Certificate is re-keyed to prevent disruption of service due to expiry, no notification is sent to the Subscriber. If the Certificate is re-keyed for any other reason and it is relevant to the Subscriber's use of the Certificate, Cerner will notify the Subscriber of the Certificate issuance via physical mail or email.

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

Cerner publishes the Certificates in the repository specified in § 2.2.1.

4.7.7 Notification of Certificate issuance by the CA to other entities

No stipulation.

4.8 Modification

Cerner 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

Not applicable.

4.8.2 Who may request Certificate modification

Not applicable.

4.8.3 Processing Certificate modification requests
Not applicable.

4.8.4 Notification of new Certificate issuance to Subscriber
Not applicable.

4.8.5 Conduct constituting acceptance of modified Certificate
Not applicable.

4.8.6 Publication of the modified Certificate by the CA
Not applicable.

4.8.7 Notification of Certificate issuance by the CA to other entities
Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Cerner 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 Cerner 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; or
- An Associate.

4.9.3 Procedure for revocation request

Revocation requests for Certificates within the Professional Organization Certificate Class shall be in accordance with § 3.4. The Certificate Officer (as defined in § 5.2) will process the request if it is approved by an Associate authorized to approve revocation requests. The authorized Associate reviews the request 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
Cerner 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
Cerner issues and posts the CRL to the repository listed in § 2.1 per the frequency specified in § 2.3. Cerner removes all superseded CRLs from the repository upon posting of the latest CRL.

4.9.8 Maximum latency for CRLs
Cerner 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
Cerner does not offer other forms of revocation advertisements.

4.9.12 Special requirements related to key Compromise
Cerner 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
Cerner does not support suspension of Certificates.

4.9.14 Who can request suspension
Not applicable.

4.9.15 Procedure for suspension request
Not applicable.

4.9.16 Limits on suspension period
Not applicable.

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

Not applicable.

4.11 End of subscription

Cerner 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

Cerner does not support key escrow and recovery for Certificates.

4.12.2 Session key encapsulation and recovery policy and practices

Cerner does not support key escrow and recovery for Certificates.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Cerner 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. This includes both data center operations and support or registration workstations.

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. Cerner 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 Cerner 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 individual may assume the Operator role. No one individual shall assume both the Officer and Administrator 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 security of the CA. All security audit logs will be retained and made available during an audit.

5.4.1 Types of events recorded

All applicable auditable events specified in CP § 5.4.1 are logged including but not limited to the following:

- Certificate Management Events:
    - Authentication into the certificate management application(s);
    - Certificate request generation;
    - Certificate issuance;
    - Read access to the Certificate repository;
    - Certificate revocation; and
    - 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;
- A success or failure indicator, where appropriate;
- 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 related to Certificate management events defined in § 5.4.1 are reviewed regularly for irregularities. Other 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. Should it become apparent that an automated security audit system has failed, Cerner will cease all CA operations except for revocation processing until the security audit capability can be restored.

5.4.7 Notification to event-causing subject

The subject is not notified of the audit event.

5.4.8 Vulnerability assessments

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 and applicable data referenced in CP § 5.5.1 including but not limited to the following:

- 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 5 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

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

5.5.5 Requirements for time-stamping of records

Artifacts related to the Certificate Life-cycle contain time and date information from a trusted time service (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)

Archived data is generated and recorded at the application, network and operating system level while the CA is in operation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

Cerner 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, Cerner 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 Cerner 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, Cerner 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 Cerner creates, stores, and manages the key pairs.

6.1.3 Public Key delivery to Certificate Issuer

Public Keys are not delivered to Cerner; rather Cerner generates the Public Keys.

6.1.4 CA Public Key delivery to relying parties

Relying Parties could have access to the CA Certificate Public Key through either of the following:

1. Cerner delivered the CA Certificate Public Key to Replying Parties within a self-signed Certificate; or
2. Cerner delivered the CA Certificate Public Key to a Trust Bundle for distribution to Relying Parties.

6.1.5 Key sizes

Cerner generates and uses 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 1 (SHA-1)
- 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)

Cerner utilizes at minimum 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256) for all Subscriber Certificate keys.

6.1.6 Public key parameters generation and quality checking
Cerner generates the Public key parameters prescribed in the Digital Signature Standard (DSS) in accordance with FIPS 186-2.

Cerner 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 will not assert the non-repudiation bit. 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
Not applicable.

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 and Subscriber Private Keys are backed up regularly and stored offsite at one of the other CTC facilities.

6.2.5 Private Key archival
Not applicable.

6.2.6 Private Key transfer into or from a cryptographic module

Private Keys are generated by and in a US FIPS 140-2 Level 1 compliant cryptographic module. Cerner exports Private Keys only for the purpose of backups as defined in § 5.4.

6.2.7 Private Key storage on cryptographic module
Cerner stores and protects the CA and Subscriber Private Keys in a FIPS 140-2 Level 1 software based module.

6.2.8 Method of activating Private Key
Cerner activates the CA and Subscriber Private Keys in accordance with the specifications of the cryptographic module manufacturer.

6.2.9 Method of deactivating Private Key
Private Keys are deactivated in accordance with § 4.9. Cerner prevents unauthorized access to all activated cryptographic modules.

6.2.10 Method of destroying Private Key
Private Key signatures that are no longer needed are destroyed quarterly by Associates in trusted roles.

6.2.11 Cryptographic Module Rating
See § 6.2.1.

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
Cerner generates activation data that has sufficient strength to protect the Private Keys. Since Cerner uses passwords as activation data for a signing key, the activation data is changed upon rekey of the respective Certificate. Cerner only transmits activation data through an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

6.4.2 Activation data protection
Cerner protects data used to unlock Private Keys from disclosure using a combination of cryptographic 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.

Cerner requires personnel to memorize and not write down their password or share their passwords with other individuals. Cerner has 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
All CA hardware requires authenticated logins. All logins and CA transactions are audited in accordance with § 5.4. Access control measures are in place in accordance with personnel controls in § 5.3. Archival processes are completed in accordance with § 5.5 to support recovery from key or system failure.

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)

Cerner 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
Not applicable.

7.1.8 Policy qualifiers syntax and semantics
The c*ertificatePolicies* extension 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 c*ertificatePolicies* 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)
Cerner issues X.509 version 2 CRLs, indicated by the version field containing the integer 1.

7.2.2 CRL and CRL entry extensions
Cerner 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)

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

7.3.2 OCSP extensions

The OCSP server returns a single extension as defined by OID 1.3.6.1.4.1.311.21.4 that indicates the next time the CRL is expected to be published.

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 Cerner, 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

Cerner 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

Cerner 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

Cerner does not issue refunds for fees related to Cerner Direct services.

9.2 Financial responsibility

9.2.1 Insurance coverage

Cerner 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. Cerner 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 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 or Cerner, or (iii) that is rightfully acquired by Subscriber or Cerner 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 nor Cerner 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

Cerner 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. Cerner provides training to employees on how to handle confidential information.

9.4 Privacy of personal information

9.4.1 Privacy plan

Cerner 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 Cerner 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, Cerner 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, Cerner 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
Cerner 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
Cerner warrants that (i) the information provided by Cerner 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, and (iv) it will promptly cease using the Certificate and notify Cerner if: (a) any information that was submitted to Cerner or is included in a certificate changes or becomes misleading, or (b) there is

any actual or suspected misuse or compromise of the Private Key associated with the certificate. Subscriber Agreements may include additional representations and warranties.

9.6.3.1 Health Information Service Providers (HISPs)
Cerner warrants that (i) it will take commercially reasonable measures to protect the Subscriber Private Keys from compromise in according with this CPS, (ii) it will promptly cease using the Certificate and related Private Key after the Certificate's expiration.

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 Cerner of any issues or problems with a Certificate of which it becomes aware, and (iv) its 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, Cerner will not be liable under this CPS 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 Subscriber agrees to indemnify, defend and hold Cerner harmless from and against all claims, damages, costs and expenses ("Claims") brought by a third party against Cerner 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 Cerner'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 to and communications with PKI participants will be conducted in a 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

Cerner 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 Cerner 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"). Cerner, each Subscriber, and Relying Parties 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 Cerner. Cerner 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

Cerner 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.