1 Introduction

1.1 Overview

This document is the Cerner Direct HISP Practice Statement (HPS) and states the policies and associated practices Cerner Corporation (Cerner) performs as a Health Information Services Provider (HISP) in the exchange of secure 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 goal of this document is to increase confidence in the use of Direct exchange through the Cerner Direct HISP by highlighting policies and practices designed for minimization of risk and liability to participants exchanging Direct messages, promoting an interoperable network of trusted Direct message recipients through transparency in HISP operations, and by providing a structured method to evaluate the HISP practices through accreditation and audit. The intended audiences for this document are Subscribers, Counterparty HISPs, and auditors/certification entities.

This HPS 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). This policy diverges from that framework, at Cerner's sole discretion, to include additional unique aspects of HISP operations and Direct messaging for the secure transport of health information over the internet. It will be updated from time to time to address technical advances, regulatory changes, or other relevant changes in the field. Definitions used within this DirectTrust HISP Policy can be found in § 1.6.

1.1.1 Relationship between the DirectTrust HP and this HPS

This HPS document summarizes how Cerner addresses the specific topics contained within the HISP Policy.

1.1.2 Relationship between this HPS and the DirectTrust CP

Because the Cerner Direct HISP utilizes X.509 Digital Certificates and participates in the DirectTrust community, the DirectTrust Certificate Policy (CP) imposes certain requirements on the Certificate issuer (i.e. Certificate Authority) which are passed through the Cerner Direct HISP and down to the Certificate Subscriber.

1.1.3 Relationship between this HPS and the DirectTrust Accreditation program

This HPS is used to communicate how the Cerner Direct HISP operates in context of the topics contained within the HISP Policy to a DirectTrust accreditation program auditor. Cerner Direct's HISP practices conform to the DirectTrust accreditation requirements, which requirements can be found on the DirectTrust web site.

1.2 Document Name and Identification

This HPS is a controlled document utilizing version control. All versions of this document can be found at www.cerner.com/hps.

This document also references the DirectTrust X.509 Certificate Policy v1.2 (OID 2.16.840.1.41179.0.1.2) and the DirectTrust HISP Policy v1.1.1 (OID 1.3.6.1.4.1.41179.5.1.0).

1.3 Public Key Infrastructure (PKI) Participants

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

1.3.1 PKI Authorities

1.3.1.1 Direct Project

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

1.3.1.2 DirectTrust

DirectTrust is a non-profit, competitively neutral, self-regulatory entity operated by and for participants in the Direct community. DirectTrust has developed and maintains a security and trust framework and operates as a policy authority, and oversees the conformance of HISP practices through the DirectTrust Accreditation program.

1.3.1.3 Certification Authorities (CAs)

A Certification Authority (CA) in this context is an entity that signs Certificate Signing Requests (CSRs) and issues public key X.509 Certificates to Direct exchange or Direct Project organizational or individual Subscribers. Cerner uses a third party to serve as its CA; Cerner makes the CA's Certificate Practice Statement available at www.cerner.com/cps.

1.3.1.4 Registration Authorities (RAs)

Registration Authorities (RA) operate identity management systems (IdMs) and collect and verify Subscriber information on the Issuer CA's behalf. RAs collect and verify identity information from

Direct Subscribers using procedures that implement the identity validation policies set forth in the DirectTrust CP. Policies governing RA services are found in the DirectTrust CP. Cerner uses a third party to serve as its RA.

1.3.2 End Users

An End User is a person or device that uses the Cerner Direct HISP solution to support Direct transactions and communications. End Users are not always the party identified in a Certificate, such as when Group Certificates are issued to an organization for use by its End Users. All End Users are Subscribers of Direct X.509 Certificates, as defined in the DirectTrust Certificate Policy, but not all Subscribers are End Users. The Cerner Direct HISP only issues Certificates for healthcare professionals and not consumers/patients at this time.

1.3.3 Health Information Services Providers (HISPs)

Cerner is the HISP that conducts the exchange of Direct messages to and from Direct Addresses, each of which is bound to a Direct-compliant X.509 digital Certificate for all Cerner Direct HISP End Users in accordance with the Direct Project Applicability Statement. Acting in the capacity of an agent for the Subscriber, Cerner holds and manages the PKI private keys associated with a Direct digital Certificate on behalf of the Subscriber.

1.3.3.1 HISP Boundary Considerations

The “HISP boundary” defines the Cerner Direct HISP, and is specified in order to allow for clear logical and physical borders where Cerner’s HISP ends and other organizational functions and responsibilities begin. The functions below are inside Cerner’s HISP boundary, and are subject to the requirements of the HISP Policy.

- Perform Security/Trust Agent (STA) functions (decrypt inbound messages, validate counterparty signature, ensure outbound messages are properly signed, encrypt outbound messages, send/receive MDNs and confirm receipt of message) [§ 6.9.4]
- Perform trust management functions such as maintaining trust anchor store and trust policy enablement [§ 6.9.3]
- Perform Certificate discovery functions [§ 6.9.4]
- Provide S/MIME inbound and outbound interfaces [§ 6.9.4] to receive messages sent to End User Direct Addresses and transmit messages sent from End User Direct Addresses
- Provide HISP-side of edge protocol connection via an API [§ 6.7.1]
- Maintain End User encryption private key store [§ 6.2]
- Perform End User authentication through EHR technology or dependent application [§ 6.7.1]
- Maintain integrity of security and trust framework, includes review of security logs, etc.
- Maintain privacy of electronic Protected Health Information (ePHI) [§§ 6.7.1, 6.9.2]
- Perform HISP Information Systems Security Officer (ISSO) functions [§ 6.2]
- Maintain End User signing private key store [§ 6.2]
- Provision Direct Addresses
- Generate End User private keys [§ 6.1.1]

- Operate SMTP inbound and outbound servers
- Operate DNS servers hosting Subscriber Certificates for discovery [§ 2.2.1]
- Maintain End User message mailboxes
- Provide and maintain the Cerner Direct Web Inbox and the End User mailboxes associated to that endpoint type, including the user interface for the application
- Provide End User technical support

1.3.4 Counterparties

A Counterparty is either an end entity that either (i) receives a Direct message sent by a Cerner Direct HISP End User or (ii) sends a Direct message to a Cerner Direct HISP End User. If the Cerner Direct HISP End User is the sender of a Direct message, then the recipient is the Counterparty. If the Cerner Direct HISP End User is the recipient of a Direct message, then the sender is the Counterparty. A Counterparty uses an End User's X.509 Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the End User.

1.3.5 Counterparty HISP

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

1.3.6 Intermediate System

An Intermediate System is a healthcare application or other system that communicates directly with the Cerner Direct HISP in order to send and receive Direct messages on behalf of End Users, using the available HISP Application Programming Interfaces (APIs). An example of an Intermediate System is an Electronic Health Record (EHR). For messages sent to Cerner Direct HISP End Users, the HISP boundary starts at the mailserver or secure email gateway and ends at the handoff from the API to the Intermediate System. For messages sent from Cerner Direct HISP End Users, the HISP boundary starts after the handoff from the Intermediate Systems to the HISP API and ends at the mailserver or secure email gateway.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The primary anticipated use for a DirectTrust Community X.509 Certificate is in the exchange of electronic messages grounded in the specifications of the Direct Project as defined in § 1.3.1.1. This includes S/MIME message signature verification and S/MIME message encryption. The Cerner Direct HISP uses Certificates issued under the DirectTrust CP only for purposes permitted by that CP.

1.4.2 Prohibited Certificate Uses

The Cerner Direct HISP does not use Certificates and private keys issued under the DirectTrust CP for any purpose prohibited by that policy.

1.5 Policy Administration

1.5.1 Organization Administering this HPS

Cerner Corporation
2800 Rockcreek Parkway
Kansas City, MO 64117
USA

In the role of providing HISP services, Cerner is a Business Associate under HIPAA.

1.5.2 Contact Person

Cerner Corporation
Attn: Cerner Direct Operations
2800 Rockcreek Parkway
Kansas City, MO 64117
1-866-221-8877
USA

1.5.3 Person Determining HISP Practices Statement Suitability for the Policy

This HPS states how the Cerner Direct HISP implements the policies required by the HISP Policy. Cerner's HISP Policy Cabinet (HPC) approves the content of this HPS. DirectTrust operates an accreditation program which certifies a HISP's compliance to the HISP Policy by analysis and audit of the information contained within an HPS. Outcomes from the DirectTrust compliance analysis and audit can be found here: https://www.directtrust.org/accreditation-status/.

1.5.4 HISP Practices Statement Approval Procedures

This HPS can be updated as needed at any time, but at minimum, it will be reviewed annually. This HPS, and all amendments hereto, must be approved by the HPC. All versions and updates are available at: http://www.cerner.com/hps. The most recent version supersedes all prior versions.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Acronym	Meaning
API	Application Programming Interface
CA	Certification Authority
CCTV	Closed Circuit Television
CP	Certificate Policy
CRL	Certificate Revocation List

CSR	Certificate Signing Request
CTC	Cerner Technology Center
DNS	Domain Name Server
EHR	Electronic Health Record
HISP	Health Information Services Provider or Health Information Service Provider
HPC	HISP Policy Cabinet
HPS	HISP Practices Statement
ID	Identity
IETF	Internet Engineering Task Force
ISO/ITU	International Organization for Standardization/International Telecommunication Union
ISSO	Information Systems Security Officer
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Health Information Technology
MDN	Message Delivery Notification
NTP	Network Time Protocol
PED	Pin Entry Device
PHI	Protected Health Information
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comments
S/MIME	Secure Multipurpose Internet Mail Extensions

1.6.2 Definitions

Term	**Definition**
Accreditation	Accreditation of a HISP through the program operated by DirectTrust. This may be in partnership with another accrediting entity.
Applicability Statement	The Applicability Statement for Secure Health Transport, Version 1.2, dated August 3, 2015, or any subsequent version, published by the Direct Project.
Application Programming Interface	Specifies how software components should interact via a programmatic service contract between one or more components.
Associate	An individual employed by Cerner.

Business Associate	An entity meeting the definition of a business associate under HIPAA at 45 CFR 160.103.
Cerner	Cerner Corporation
Cerner Direct Web Inbox	A solution offered by Cerner which allows End Users to access Direct messages following an initial role based invitation leveraging a shared secret and subsequent authentication.
Certificate	A digital representation of information which at least: (1) identifies the Certification Authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it.
Certificate Discovery IG	Unless otherwise stated, means the then current version of the S&I Framework Certificate Discovery for Direct Implementation Guide, which is available at http://preview.tinyurl.com/y834kkmz.
Certification Authority	An authority trusted by one or more users to create and assign Certificates. Also known as a Certificate Authority.
Certificate Policy	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital Certificates.
Certificate Practice Statement	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing Certificates and providing access to them, in accordance with specific requirements typically provided in a Certificate Policy.
Certificate Revocation List	A list maintained by a Certification Authority identifying the Certificates that it has issued that are revoked prior to their stated expiration date.
Confidential Information	Has the meaning set forth in § 9.3.1.
Counterparty	The end entity on the other side of a Direct transaction with an End User. See § 1.3.4.
Counterparty HISP	The HISP used by a Counterparty. This may be a different HISP than the HISP used by the End User. See § 1.3.5.
Covered Entity	An entity meeting the definition of a covered entity under HIPAA at 45 CFR § 160.103.

Delivery Notification IG	Unless otherwise stated, means the then current version of the Implementation Guide for Delivery Notification in Direct, which is available at http://tinyurl.com/ybmdypg7.
Direct Address	The email address, issued by the Cerner Direct HISP, which is associated with an End User.
Direct Message	An electronic mail message digitally signed and encrypted according to the requirements of the Applicability Statement.
Direct Project	An initiative from the Office of the National Coordinator (ONC) for Health Information Technology that created a set of standards and services that, with a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
DirectTrust CP	The current versions of the DirectTrust Certificate Policy, as further defined in § 1.1.2.
Distinguished Name	A term that describes the identifying name in a Certificate, which becomes part of the Certificate itself.
Electronic PHI	Has the meaning given to *Electronic Protected Health Information* under 45 C.F.R. § 160.103 of HIPAA.
End User	An end entity that uses a HISP's Direct Services. An End User may act in the role of sender or recipient of a Direct message.
Group Certificates	A Certificate where use of the corresponding Private Key is shared by multiple entities/End Users.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, as amended.
HISP	A provider of Direct messaging Security/Trust Agent services to Subscribers.
HISP Policy	A document, written by DirectTrust, defining the requirements to conform to Direct Message standards and industry privacy and security best practices.
HISP Practices Statement	A document written by a HISP to demonstrate how the HISP meets the requirements of this HISP Policy, including both technical and organizational aspects.
Intermediate System	An Intermediate System communicates with a HISP or another Intermediate System to send and/or receive Direct messages on behalf of End Users using an edge protocol supported by both systems. See § 1.3.6.

Internet Engineering Task Force	A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
Information Systems Security Officer (ISSO)	An individual responsible for establishing and maintaining the enterprise vision, strategy and program as it relates to Information Systems Security, to ensure information assets are adequately protected.
Private Key	Means either (i) the key of an asymmetric key pair used to create a digital signature, or (ii) the key of an asymmetric key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	Means either (i) the key of an asymmetric key pair used to validate a digital signature, or (ii) the key of an asymmetric key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital Certificate.
Public Key Infrastructure	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key Certificates.
Registration Authority	The entity responsible for identification and authentication of Certificate subjects.
Relying Party	A person or entity that has received information that includes a Certificate and a digital signature verifiable with reference to a public key listed in the Certificate, and is in a position to rely on them.
Secret Key	The cryptographic key only known by the hardware security module and used to wrap/encrypt Subscriber Private Keys prior to storage as well as decryption of those Private Keys during processing of Direct messages.
Subscriber	A person or entity that: (1) is the subject named or identified in a Certificate issued to that entity, (2) holds, directly or through its designated HISP, a private key that corresponds to the public key listed in the Certificate, and (3) does not itself issue Certificates to another party.
Subscriber Agreement	Subscriber Agreement means the set of agreements entered into between Cerner and a Subscriber under which Cerner agrees to provide Subscriber with the Cerner Direct HISP services.

Subscriber Applicant	A person or entity that submits an application to Cerner to receive Cerner Direct HISP services.
Trust Anchor	See Trust Anchor Certificate.
Trust Anchor Certificate	A Certificate identifying a trusted issuer of Certificates.
Trust Anchor Store	A repository holding a collection of Trust Anchors.
Trust Bundle Distribution IG	Unless otherwise stated, means the then current version of the Implementation Guide for Direct Project Trust Bundle Distribution, which is available at http://preview.tinyurl.com/y834kkmz.
Trusted Roles	Has the meaning set forth in § 5.2.1.

2 Publication and Repository Responsibilities

2.1 Repositories

Cerner is responsible for the repository functions of Subscriber Certificates in its role as a HISP. This includes an internal document repository supporting HISP operations, containing completed Cerner Direct HISP applications, process and procedure documents, and this HPS.

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

The Certificates required for Cerner Direct HISP End Users to receive Direct messages are available for discovery by other HISPs through a DNS service owned and operated by Cerner, as described in the Certificate Discovery IG.

2.2.2 Publication of CA Information

Cerner uses a third party to serve as its CA; Cerner makes the CA's Certificate Practice Statement available at www.cerner.com/cps.

2.2.3 Interoperability

To promote interoperability, Cerner leverages Certificates issued by the CA, which meet the requirements of the DirectTrust CP.

2.3 Frequency of Publication

This HPS is updated and published in accordance with § 9.12. Subscriber Certificate information is published to DNS as soon as possible following issuance.

2.4 Access Controls on Repositories

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized access to repositories and write access, as appropriate.

Subscriber Certificates are stored and protected in accordance with § 6.2.7.

Cerner Direct HISP applications are posted to an internal document repository and are accessible only by individuals those within Trusted Roles.

3 Identification and Authentication

This section pertains only to naming rules and identity validation for initial Certificate issuance and identification and authentication for re-key and revocation requests for existing Certificates. Subsequent identification and authentication of End Users and Intermediate Systems in order to use existing keys for signing or decryption of Direct messages are discussed in § 6.7.2 and § 6.7.3 of this document.

3.1 Naming

No stipulation beyond conformance with the DirectTrust CP.

3.2 Initial Identity Validation

No stipulation beyond conformance with the DirectTrust CP. The Cerner Direct HISP supports the DT.org LoA for identity proofing required by the receiving party and or applicable trust bundle. Private keys are generated and held by the HISP as specified in § 4.5.1. The HISP issues Group Certificates as specified in § 4.3.

3.3 Identification and Authentication for Re-key Requests

No stipulation beyond conformance with the DirectTrust CP.

3.4 Identification and Authentication for Revocation Request

No stipulation beyond conformance with the DirectTrust CP.

4 Certificate Life-Cycle

4.1 Application

All Subscriber Applicants must complete a Cerner Direct HISP application initially and at subsequent intervals as defined by the CA and RA. The application must include:

- Organization information
- Healthcare category indication
- Requested Direct email domain
- Contact information for the authorized representative
- Pass-through obligations required by the CA and RA on use of the issued Certificate

A Subscriber must provide accurate information about him/herself and his/her organization when completing the application.

4.2 Certificate Application Processing

All Subscriber Applicants must first sign a contract with Cerner for Cerner Direct HISP services. Cerner will not process any Subscriber Applications until after such contract is signed.

Cerner will reject Subscriber Applications if:

- Application is incomplete or inaccurate;
- Successful validation of the identity cannot be completed by the RA as set forth in § 3.2;
- Contract for Cerner Direct HISP services has not been signed;
- Cerner, in its sole and exclusive opinion, believes the Subscriber Applicant does not have a legitimate reason to participate in Direct communications;
- Cerner, in its sole and exclusive opinion, believes the Subscriber Applicant represents a risk to the professional reputation of Cerner; or
- For any other reason determined by Cerner, in its sole and exclusive opinion.

Cerner creates the Certificate Signing Request (CSR) for Certificate issuance based on input received from the application. The CA is responsible for verifying the information in a CSR is accurate and reflects the information presented by the Subscriber through its identity proofing activities. Cerner keeps all communication made during the application process confidential.

4.3 Issuance

Upon issuance of a Certificate for the Subscribing Organization, the Subscriber Applicant shall become a Subscriber. The Subscriber will be notified via email once the Certificate has been issued. The Cerner Direct HISP issues Group Certificates to Subscribers and uses single-use Certificates, meaning two Certificates are issued to each Subscriber, one for Direct message signing and the other for Direct message encryption.

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 HISP

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. Cerner maintains Private Key protections in accordance with § 6.1. Certificate usage is described in § 1.4.

The Cerner Direct HISP trust anchor Certificate(s) is available to Relying Parties for download from the DirectTrust website found here: https://bundles.directtrust.org/bundles/accreditedCommunity.p7b, as required by the Trust Bundle Distribution IG.

4.5.2 Relying Party Public Key and Certificate Usage

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

If a Certificate in the Counterparty Certificate chain to be validated lists a CRL distribution point, the HISP will obtain status information to confirm the Certificate has not been revoked before the Certificate is trusted.

1. If the status information is available, either from newly retrieved data or from a non-stale cached version and the CRL does not list the Certificate as revoked, then the HISP will trust the Certificate chain so long as all other local policy trust requirements are met.
2. If the status information is available and the Certificate is marked as revoked, then the HISP will mark the Certificate chain as untrusted.
3. If the status information is not available due to network or other failure, the HISP will base the decision on the non-stale cached version. If found in the Certificate revocation list, it will mark the Certificate chain as untrusted. If a non-stale cached version cannot be located, it will also mark the Certificate chain as untrusted.

If a Certificate in the Counterparty Certificate chain to be validated does not list a CRL distribution point, the HISP will trust the Certificate chain so long as all other local policy trust requirements are met. If a counterparty lists an OCSP location, but not a CRL distribution point, the OCSP service will not be processed by the Cerner Direct HISP. The Cerner Direct HISP only utilizes CRLs to determine Certificate status.

The HISP requires each incoming signed message intended for an End User to contain at least one trusted and valid Certificate meeting local policy requirements prior to sending any message disposition notification back to a Counterparty *sender* and further processing the message. If at least one trusted and valid Certificate is not found, the message is marked as untrusted and the HISP silently drops and deletes the untrusted message in order to reduce the risk of certain types of denial of service attacks. End User *recipients* are not notified of these untrusted messages.

4.6 Certificate Renewal

Cerner requests Certificate renewals prior to Certificate expiry in order to create an overlap in Subscriber Certificates utilized by the HISP, thereby ensuring continuity of communications with Relying Parties during Certificate expiry. Cerner requests Certificate re-key at the time of Certificate renewal.

4.7 Certificate Re-Key

No stipulation beyond conformance with the DirectTrust CP.

4.8 Modification

The Cerner Direct HISP does not support Certificate modification. Any change to the original Certificate results in a new Certificate, including a new private and public keypair.

4.9 Certificate Revocation and Suspension

Cerner may request revocation of a Certificate 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 within the Subscriber Application is false or misleading;
- Reasonable suspicion by Cerner that the Private Key is compromised;
- Request from the Subscriber to revoke his/her Certificate;
- Violation by the Subscriber of the terms of the Subscriber Agreement;
- Termination or expiration of the Subscriber Agreement; or
- Any other reason determined by Cerner, using its sole and exclusive judgment.

4.10 Certificate Status Services

The Cerner Direct HISP utilizes CRL distribution points exclusively to determine Certificate status. Use of OCSP (responders is not supported.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

Cerner does not support key escrow for Certificates.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility Management and Operations Controls

5.1 Physical Controls

Cerner hosted technology necessary for support of this HPS is housed in Cerner's Technology Centers ("CTC"). The CTC is ISO 9001:2008, ISO 27001:2013, SOC 1, SSAE 18 and SOC 2 certified. If Cerner contracts with a third party data center for support of the Cerner Direct HISP, Cerner will make their practices statement available at www.cerner.com/cps.

5.1.1 Site Location and Construction

The CTC is protected by multiple layers of physical security including an off-site alternate CTC, which is designed to reduce 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 within the CTC are controlled by card access, with combination card and biometric readers in high-security areas. Additionally, the CTC uses CCTV cameras and recording devices, along with required photo ID badges and/or escort of personnel. 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. Cerner has established procedures to record and manage maintenance and repair activities and the suppliers who perform maintenance procedures.

Access to CTC facilities are granted and managed on demand by a 24x7 security operations team who follow documented access procedures during normal and disaster situations. Cerner only provides CTC and information to employees and contractors who have a legitimate business need for such privileges. When an Associate no longer has a business need for these privileges, their access is revoked, even if they continue to be an Associate of Cerner. Authorized staff must pass multiple layers of security to access CTC floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

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 are designed to 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 stored in a location separate from the HISP equipment. 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 through the methods described in this § 5.1.

All confidential or sensitive data will be removed from electronic media before movement outside of the data center or redeployment.

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. Cerner maintains a media destruction log which is routinely reviewed to validate accuracy between supplier receipts for media pick up and the corresponding supplier certificate of destruction.

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 5 roles as it relates to the administration of the HPS:

1. Administrator
2. Information Systems Security Officer (ISSO)
3. Operator

The following roles provide support related to the administration of this HPS:

4. Chief Security Officer
5. Chief Privacy Officer

Some roles may be combined, but care has been taken to distribute key functions amongst more than one person. Cerner also has an IT regulatory official responsible for the identification of legal or regulatory requirements relevant to the IT resources and operations. The following subsections provide a detailed description of the responsibilities for each Trusted Role.

5.2.1.1 Administrator

The Administrator is responsible for:

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

5.2.1.2 Information Systems Security Officer

The Information Systems Security Officer is responsible for:

- Configuring End User profiles or templates
- Generating, installing and backing up End User keys
- Managing End User access to private keys stored by HISP
- Managing HISP-wide trust decisions, e.g. addition or deletion of trust anchors, trust bundles, or policy enforcement rules

5.2.1.3 Operator

The Operator role is responsible for the routine operation of the HISP equipment and operations such as system backups and recovery or changing recording media.

5.2.1.4 HIPAA Security Officer

The Chief Security Officer is responsible for duties of the Security Officer under HIPAA and is authorized to make changes about the system security policies. The individual performing this role, and that person's backup, along with a description of the role responsibilities, are documented and communicated internally.

5.2.1.5 HIPAA Privacy Officer

The Privacy Officer is a point of contact for reporting and assisting in the investigation of any data breach that might take place. The individual performing this role, and that person's backup, along with a description of the role responsibilities, are documented and communicated internally.

5.2.2 Number of Persons Required Per Task

Cerner trains at least two Associates for each Cerner Direct HISP 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 HISP, which is used to authenticate the Associate and assign proper authorization to perform HISP activities related to their role.

5.2.4 Separation of Roles

Any individual may assume the Operator role. No one individual shall assume both the Information Systems Security Officer and Administrator roles.

5.2.5 Access to Electronic PHI

Cerner has established policies, procedures, and contractual agreements in place to ensure that its organizational units, business partners, vendors, and Cerner clients protect and maintain the integrity of electronic PHI in accordance with the HIPAA Privacy and Security Rules. Because of the nature of Cerner's business and the potential for exposure to PHI, all Associates receive regular training to enforce the control requirements and guidelines defined in Cerner's corporate policies. Cerner also maintains a list of Business Associates with access to Electronic PHI. All access is audited in accordance with § 5.4.

5.2.6 Policies and Procedures

Cerner maintains policies and procedures implemented to comply with applicable federal and state regulations, including an overall program management and strategy policy for information security. These security policies, procedures and security plans are available to those that need access to them and are reviewed annually and updated as needed.

Policies and procedures are reviewed annually and updated as needed in response to environmental or operational changes affecting the security of the Electronic PHI.

5.2.7 Hybrid Entities

Not applicable.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security 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 Seven Years
- Education Verification (Highest Degree)
- Criminal Search
- Widescreen plus search
- Social Security Number Verification
- Healthcare Sanctions check
- Global Sanctions and Enforcement check

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
- Drug Screen

5.3.3 Training Requirements

Cerner make a significant investment in the recruitment and retention of Associates who possess the skill, knowledge, and ability to automate the process of managing health information. It is imperative that Associates maintain technical and professional training to effectively meet the requirements of their Cerner-defined roles. 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

Cerner conducts annual training to cover breach reporting and notification, privacy, confidentiality, and security. Role-specific 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

Cerner policy provides guidance for resolving a variety of ethical and legal questions for Associates. This policy is designed to deter wrongdoing and to require and promote honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships and defines sanctions for Associates who fail to comply corporate policies and procedures. 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

Cerner reviews the level of access to information that an independent contractor may require to perform its responsibilities and requires the independent contractor sign appropriate agreements such as non-disclosure agreement (NDA), Business Associate Agreements (BAAs) and other contracts binding the independent contractor to compliance with applicable Cerner policies and procedures. Prior to being granted any network connectivity, all third party entities must agree to adhere to the same network access policy requirements as Associates and complete all required corporate training courses including security and privacy topics.

5.3.7.1 Business Associates of HISP

If the Cerner Direct HISP uses the services of a third party to create, receive, maintain, or transmit PHI on behalf of the HISP or its End Users, then Cerner will enter into a downstream Business Associate Agreement (BAA) with the third party, in compliance with HIPAA.

5.3.7.2 Cloud Service Providers as Business Associates of HISP

If Cerner contracts with a cloud service provider for support of the Cerner Direct HISP, Cerner will make their practices statement available at www.cerner.com/cps.

5.3.8 Documentation Supplied to Personnel

Associates are provided a learning plan and the related documentation necessary to perform their job responsibilities competently. All corporate and organizational policies and procedures are made available to all Associates through internal content management systems.

5.4 Audit Logging Procedures

Audit log files are generated for all events occurring within the HISP boundary that relate to the security of the HISP. All security audit logs, both electronic and non-electronic, shall be retained in accordance with § 5.4.3 and made available during an audit.

5.4.1 Types of Events Recorded

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

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

Security audit events captured by the Cerner Direct HISP are listed in the table below.

SECURITY AUDIT • Any changes to the audit parameters, e.g., audit frequency, type of event audited • Any attempt to delete or modify the audit logs
AUTHENTICATION TO HISP STA SYSTEMS • Successful and unsuccessful attempts to assume a role • The value of maximum number of authentication attempts is changed • Maximum number of unsuccessful authentication attempts reached during user login
LOCAL DATA ENTRY

• All security-relevant data that is entered in the system
REMOTE DATA ENTRY • All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT • All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION/REVOCATION/ACCESS • Issue Certificate • Revoke Certificate • Access Certificate
PRIVATE KEY LOAD AND STORAGE • All access to Certificate subject Private Keys retained within the HISP for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE • Any change to the trusted Public Keys, including additions and deletions
SECRET KEY STORAGE • The creation of the Secret Key used for authentication
PRIVATE AND SECRET KEY EXPORT • The export of Private Keys (keys used for a single session or message are excluded)
HISP CONFIGURATION • Any security-relevant changes to the configuration of a HISP system component
ACCOUNT ADMINISTRATION • Roles and users are added or deleted • The access control privileges of a user account or a role are modified
TRUST MANAGEMENT PROFILES • All changes to End User trust management profile, including policy enforcement rules, enabling or disabling trust anchors or trust bundles, manual refreshing of trust bundles, and manual import of Certificates from other parties.
TIME STAMPING • A third party time stamp is obtained (local system time stamps are excluded).
MISCELLANEOUS • Appointment of an individual to a Trusted Role

• Installation of an Operating System • Installation of a HISP Application • Installation of Hardware Security Modules • System Startup • Logon attempts to PKI Application • Attempts to set passwords • Attempts to modify passwords • Backup of the internal HISP database • Restoration from backup of the internal HISP database • All Certificate compromise notification requests • Zeroizing Hardware Security Modules • Re-key of a HISP system component • Access to Directory information (additions, deletions, updates, searches)
CONFIGURATION CHANGES • Hardware • Software • Operating System • Patches
PHYSICAL ACCESS / SITE SECURITY • Known or suspected violations of physical security • ANOMALIES • System crashes and hardware failures • Software error conditions • Software check integrity failures • Network attacks (suspected or confirmed) • Equipment failure • Violations of the HP or HPS • Resetting Operating System clock

5.4.2 Frequency of Processing Log

Cerner reviews access log reports and events generated from system logs and security systems as frequently as daily, with all logs being reviewed on a regular basis and as needed when an issue is suspected. Items that require further investigation are logged as incidents in Cerner’s incident management system and tracked until formal closure occurs.

Audit logs are active at all times and protected from unauthorized access, modification and accidental or deliberate destruction on all audited information resources that contain confidential or restricted information. Activities that are logged include, but are not limited to:

- All successful and unsuccessful login attempts

- All logoff's
- Login attempts using invalid passwords
- Additions, deletions and modifications to user accounts/privileges
- Attempts to perform unauthorized functions
- Activity performed by privileged accounts modifications to system settings (parameters)
- Additions, deletions and modifications to security/audit log parameters
- User account management activities
- System shutdown
- System reboot
- System errors
- Application shutdown
- Application restart
- Application errors
- File creation
- File deletion
- File modification
- Failed and successful log-ons
- Security policy modifications
- Use of administrator privileges

5.4.3 Retention Period for Audit Logs

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

5.4.4 Protection of Audit Logs

Audit logs for the security-related events are protected in accordance to the Cerner 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 HISP events use 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)

All security audit processes are invoked at HISP startup and cease only at shutdown. Redundant systems are utilized to ensure capture and store of audit events occurs in the event the primary security audit system has failed.

5.4.7 Notification to Event-Causing Subject

The subject is not notified of the audit event.

5.4.8 Vulnerability Assessments

Cerner conducts audits and risk assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Electronic PHI based upon NIST and HIPAA standards on a semi-annual basis. Results are reviewed by Cerner's senior management team who implement risk management plans as needed.

Cerner assesses the security of its computing systems and supporting network via a vulnerability management program that utilizes assessment techniques including regular vulnerability scans that measure the vulnerability of systems and networks from multiples layers of the OSI model, to penetration tests that simulate malicious attacks from both an internal and external perspective. Any critical items are promptly addressed. These risk assessment and risk mitigation activities occur, internally, on a quarterly basis and, using an independent third party, at least annually.

5.5 Records Archival

5.5.1 Types of Events Archived

Cerner maintains a record of any action, activity, or assessment that may be required by applicable law or regulation. A sample of HISP-related data being archived is found below:

- Accreditation of the HISP,
- HP and HPS versions,
- Contractual obligations and other agreements concerning the operation of the HISP, notably BAAs,
- System and equipment configurations, modifications, and updates,
- Certificate signing and revocation requests,
- Any documentation related to the receipt or acceptance of a Certificate or token,
- Subscriber Agreements,
- Any data or applications necessary to verify an archive's contents,
- Compliance auditor reports,
- Any changes to the HISP's audit parameters,
- Any attempt to delete or modify audit logs,
- Key generation,
- Access to Private Keys for key recovery purposes,
- Changes to trusted Public Keys,
- Export of Private Keys,
- Appointment of an individual to a Trusted Role,
- Destruction of a cryptographic module,
- Certificate compromise notifications,

- Remedial action taken as a result of violations of physical security, and
- Violations of the HP or HPS.

5.5.2 Retention Period for Archive

Archives of documentation described in §§ 5.2.6 and 5.5.1 are retained for a minimum of six 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. Certificate signing requests, revocation, and related database entries).

5.5.6 Archive Collection System (Internal vs. External)

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

5.5.7 Procedures to Obtain & Verify Archive Information

No stipulation.

5.6 Key Changeover

No stipulation beyond conformance with the DirectTrust CP.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Cerner has an established incident management process to respond to security events that may affect the confidentiality, integrity, or availability of its systems or data. The Cerner incident management process defines specific courses of action and procedures for notification, escalation, mitigation, and documentation as well as an overall lifecycle process to address the operational, tactical, reaction and recovery phases.

Cerner's Incident Response Staff is trained in forensics and evidence handling in preparation for an event, including the use of third party and proprietary tools. The Cerner Security Incident Response Team is available 24x7 to address any incident that may occur.

Cerner's policies, procedures and supporting work instructions define the roles and responsibilities as they apply to breaches of unsecured Electronic PHI and includes, but is not limited to, determination of reporting the incident, evaluation to determine the unauthorized person(s) who received and/or used the Electronic PHI, the extent to which the risk to the Electronic PHI has been mitigated, whether the Electronic PHI was actually used/accessed/viewed, and the type and amount of Electronic PHI involved.

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 CTC's incident handling procedures including system integrity checking. If necessary, the procedures in § 5.7.3 and 5.7.4 will be initiated.

5.7.3 Entity Private Key Compromise Procedures

Subscriber Private Keys are protected from compromise in accordance with § 6.1.1. Should the Private Key of a Subscriber Certificate be identified as compromised, the Certificate will be revoked and a new Subscriber Certificate will be issued in accordance with § 4.9.

5.7.4 Business Continuity Capabilities after a Disaster

Cerner has policies and procedures to cover responding to an emergency or other occurrence such as fire, vandalism, system failure, or natural disasters that impacts systems containing Electronic PHI. Criticality evaluation for system components at the infrastructure, application, and storage layers occurs on an annual basis as specified within this HPS.

The CTC consists of multiple data centers. Each of these data centers has core infrastructure services, including telecommunications, power, and security infrastructure in place. In the event of a disaster, an alternate data center will be invoked, with production systems being recovered first, followed by non-production systems. An emergency response team will be mobilized and will execute an internal and external communication plan to communicate status. System and database backups, as discussed in § 5.9, will be used to recover the production system in an alternate data center. Hardware (e.g., servers, storage) will be provisioned as quickly as possible, followed by data recovery and finally application deployment and configuration. A bill of materials is kept for each of these areas to aide in this process. As soon as the recovery process of production systems is complete, Subscribers will be notified.

5.8 HISP Termination

In the event of HISP termination, Cerner will work with the CA to ensure the CA revokes the CA Certificate for Cerner. Once the CA Certificate is revoked, all Subscriber Certificates become invalid.

5.9 Backup of Electronic PHI

The Cerner Direct HISP does not generally retain any messages sent or received using the Cerner Direct HISP, including any Electronic PHI contained therein, although certain Electronic PHI may be captured as part of the Cerner Direct HISP audit logging process (see § 5.4) and as more fully described below.

In the case of inbound messages for End Users serviced by the Cerner Direct HISP, the HISP does not retain or archive messages beyond receipt of the acceptance or refusal by the Intermediate System, or the sixty minute threshold has been exceeded and at such time a final delivery failure message (message disposition notification with a disposition of "failed") is returned to the sender, whichever comes first.

For outbound messages serviced by the Cerner Direct HISP, the HISP does not retain or archive messages beyond receipt of the acceptance or refusal by the relying party, or the sixty minute threshold has been exceeded and at such time a final delivery failure message (message disposition notification with a disposition of "failed") is returned to the End User, whichever comes first.

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

The Cerner Direct HISP attempts to deliver all trusted Direct messages received on behalf of its End Users and meeting local policy requirements to the intended recipient's HISP-managed mailbox or to an Intermediate System authorized to accept messages on behalf of the End User (e.g. Cerner Millennium). The HISP does not divert, copy, or redistribute incoming messages received on behalf of an End User to any other recipient, destination, application, or database, except as required for routine inline processing of messages for the End User (e.g. message virus scanning) or as required for the HISP to meet any backup, archival, disaster recovery, or other requirement under HIPAA or other regulation.

Cerner does provide mailbox capabilities separate from the HISP services and those mailbox services (such as Cerner Message Center and Cerner Web Inbox) have separate polices and procedures regarding the backup of messages (including Electronic PHI contained therein). Subscribers have full responsibility for ensuring that messages sent through the Cerner Direct HISP are incorporated into a patient's medical record as necessary in accordance with the Record Retention and Classification section of the Cerner Direct terms of use. The Cerner Direct HISP terms of use can be found at: https://cernerdirect.com/inboxes/welcome-terms

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The Cerner Direct HISP generates key pairs for Subscribers only and does so using US FIPS 140-2 Security Level 2 certified hardware security modules which are 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 delivered via a Certificate Signing Request (CSR) to the Certificate Authority using a secure channel (e.g. TLS) and two-factor authentication utilizing username/password and a client digital Certificate.

6.1.4 Public Key Delivery to Relying Parties

6.1.4.1 HISP Trust Anchor Delivery

The Trust Anchor Certificate is delivered to Relying Parties in conformance with the Trust Bundle Distribution IG.

6.1.4.2 End User Subscriber Public Key Delivery

Subscriber Public Keys are delivered within Certificates made available for discovery through DNS as specified in the Certificate Discovery IG.

6.1.5 Key Sizes

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 US FIPS 186-2.

Cerner performs parameter quality checking (including primality testing for prime numbers) in accordance with US FIPS 186-2.

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

Certificates used by the Cerner Direct HISP conform to the DirectTrust CP. Separate signing and encryption Certificates are leveraged for each Subscriber, with each asserting a single key usage bit, respectively:

- digitalSignature
- keyEncipherment

No Certificates will assert the non-repudiation bit. All Certificates assert an extended key usage bit of emailProtection. A Basic Constraint extension is used with the critical flag set to TRUE and CA:FALSE.

The Cerner Direct HISP enforces the permitted key usages when using Certificates if the field or extension is marked as critical, unless the incoming messages are encrypted using the Public Key in a Certificate that asserts the digitalSignature key usage bit but not the keyEncipherment key usage bit in an effort to help preserve interoperability with legacy systems.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

In order to ensure the Private Keys of Subscribers have the strongest protection from unauthorized use, Cerner designates an Information Systems Security Officer (ISSO) who is responsible for: 1) conducting risk assessment and risk mitigation activities on at least a quarterly basis using commercially available third party tools, and 2) recording and tracking specific access to those Private Keys at any given time. Any risks identified as critical are addressed promptly. Cerner captures information on use of Private Keys and obligates its Subscribers to do so as well in accordance with the DirectTrust CP.

6.2.1 Cryptographic Module Standards and Controls

Cryptographic modules used are certified against US FIPS 140-2 Security Level 2.

6.2.2 Private Key (n out of m) Multi-person Control

Not applicable.

6.2.3 Private Key Escrow

No Private Keys are escrowed.

6.2.4 Private Key Backup

Subscriber Private Keys are backed up regularly and stored offsite in order to facilitate disaster recovery.

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 a US FIPS 140-2 Security Level 2 certified hardware security module, then are wrapped with an AES-128 secret key and exported from the hardware security module and stored in a database. Keys are activated by inserting the wrapped key into the hardware security module and decrypted on the module using the AES-128 secret key. Private Keys are never exposed in an unencrypted state outside of the hardware security module, including during the key backup process as defined in § 6.2.4.

6.2.7 Private Key Storage on Cryptographic Module

Cerner generates and encrypts Subscriber Private Keys by means of a US FIPS 140-2 Security Level 2 certified hardware security module using an AES 128 symmetric key which never leaves the hardware security module.

6.2.8 Method of Activating Private Keys

Cerner activates Subscriber Private Keys in accordance with the specifications of the hardware security module manufacturer.

6.2.9 Methods of Deactivating Private Keys

Private Keys are deactivated in accordance with § 4.9. Cerner restricts unauthorized access to all activated cryptographic modules.

6.2.10 Method of Destroying Private Keys

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 Management

6.3.1 Public Key Archival

Public Keys are backup up and archived as part of the media storage process specified in § 5.1.6.

6.3.2 Certificate Operational Periods/Key Usage Periods

Subscriber Certificates and associated key pairs expire three years 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 hardware security module.

Activation data is generated at the time of partition generation on the hardware security module resulting in a random and appropriate length password. The password is stored away from the cryptographic module in an encrypted configuration store. The hardware security module also requires a second factor of authentication via a PED to activate the Private Keys.

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 hardware security module and is not stored with the hardware security module. The activation data is stored away from the cryptographic module in an encrypted configuration store. The hardware security module also requires a second factor of authentication via a PED to activate the private keys.

6.4.3 Other Aspects of Activation Data

The hardware security module also requires a second factor of authentication via a PED to activate the private keys.

6.5 Computer Security Controls

The Cerner Direct HISP operates its infrastructure in accordance with the controls demanded by DirectTrust LoA-3 for identity proofing, DirectTrust LoA-1 for authentication, and FBCA Medium for HISP operations. The corresponding controls to meet these levels are specified in the DirectTrust HISP Policy and incorporated into the development and operational policies and practices of the HISP, which are described or referenced in this document. Adherence to these controls is externally audited at minimum every other year, with some controls being internally audited as frequent as daily. Cerner maintains an active role in shaping industry expectations for these areas to assist in staying current in its implementation and understanding of these controls.

6.5.1 Specific Computer Security Technical Requirements

Cerner configures its systems to:

1. authenticate the identity of HISP personnel before permitting access to the system or applications.
2. manage the privileges of HISP personnel and limit these users to their assigned roles in accordance with the Trusted Roles in § 5.2.1 and personnel controls in § 5.3.
3. generate and archive audit records for all transactions listed in § 5.4.1.
4. enforce domain integrity boundaries for security critical processes.
5. support recovery from key or system failure in accordance with § 5.7.4.

Cerner has policies to:

1. require personnel to memorize and not write down their password or share their passwords with other individuals.
2. temporarily lock access to secure CA processes if a certain number of failed log-in attempts occur.
3. maintain a pictorial diagram or spreadsheet listing all essential HISP function sites including their name, address, relationship to the HISP, and the functions performed.
4. maintain a listing of all hardware and software used to store, transmit or maintain Electronic PHI, including all Primary Domain Controllers (PDCs) and servers.
5. discourage the use of personal software as well as restrict the use of unlicensed and unapproved software and monitoring capabilities to ensure compliance.
6. specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access Electronic PHI.

Cerner implements technology to:

1. authenticate and protect all communications between a Trusted Role and its HISP system.
2. ensure Subscriber Private Keys are protected in accordance with § 6.2.7.
3. guard against, detect, and report malicious software.
4. ensure that internal databases cannot be modified directly through an external web site, unless modified securely by authenticated users.
5. protect any HISP web servers from attack or intrusion through documented web server security configurations.

Cerner maintains documentation to:

1. list all sites that create, receive, maintain, or transmit PHI for the delivery of the services provided.
2. list of all hardware and software used to store, transmit or maintain Electronic PHI, including all Primary Domain Controllers (PDCs) and servers.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

Cerner follows a modern development process that meets ISO 9001:2008. 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 policies which require all changes to be evaluated, documented, and approved before implementation.

Cerner has defined policies and procedures that establish common configuration and patch management standards for systems that store, transmit, and provide access to Electronic PHI. Emergency, non-routine, and other configuration changes to existing Cerner infrastructure are authorized, logged, tested, approved, and documented in accordance with industry norms for similar systems. Updates to the Cerner Direct HISP infrastructure are done to minimize any impact on the Subscriber, its End Users and their use of the Cerner Direct HISP services.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The CTC follows policy designed to comply with the Network System Management requirements of ISO/IEC 27001:2005(E).

Cerner has policies in place which prohibits HISP personnel from storing unencrypted PHI on personal computers, consumer devices, and removable storage media.

Cerner's approach to wireless security is based on implementing current best practices in wireless security, utilizing a layered security approach which focuses on implementing controls securing the following architectural layers:

1. Wireless intrusion protection
2. Authentication
3. Encryption
4. Access control
5. Client security

Cerner employs multiple layers of defense to help protect the network perimeter from external attacks. Only authorized services and protocols that meet Cerner's security requirements are permitted to traverse the company's network. Unauthorized packets are automatically dropped. Cerner's network security strategy is composed of the following elements:

1. Enforcement of network segregation strategies using state-of-the-art firewall and ACL technology.
2. Management of network firewall and ACL rules that employ change management, peer review, and automated testing.
3. Restricting access to networked devices to authorized personnel.
4. Routing of all external traffic through specialized systems that help detect and stop malicious requests.
5. Creating internal aggregation points to support better monitoring.
6. Regular examination of logs for exploitation of programming errors (e.g., cross-site scripting) and generating high priority alerts if an event is found.

Cerner's security monitoring program analyzes information gathered from internal network traffic, end user actions on systems, and outside knowledge of vulnerabilities. At multiple points across Cerner's global network, internal traffic is inspected for suspicious behavior. Information is subsequently sent to a third-party service provider for additional correlation and expert system analysis. Actionable information in the form of alerts is subsequently returned to a Cerner Security Analyst for further investigation or remediation.

6.7.1 End User Data Storage and Edge Protocols

The Cerner Direct HISP adheres to the standard HIPAA privacy and security rules defined at 45 CFR Part 160 and Subparts A and E of Part 164 in storing messages and personal information received from or on behalf of Subscribers and End Users.

The Cerner Direct HISP leverages the Secure Hash Algorithms specified in § 6.1.5 for Direct messages containing Electronic PHI outside of the HISP infrastructure.

The Cerner Direct HISP offers an edge protocol which consists of a set of Restful service APIs. Interaction with the Cerner Direct HISP outbound from the edge client (inbound into the Cerner Direct HISP) using the Restful services is over secure http with OAuth authorization. Final delivery of messages to the edge client (outbound from the Cerner Direct HISP) is via a Restful service which also utilizes secure http with OAuth authorization.

The Cerner Direct HISP also offers a Web inbox application allowing End Users to access messages following an initial role based invitation leveraging a shared secret and subsequent authentication.

The Cerner Direct HISP does not examine the content of messages sent or received through the HISP system for the purpose of clinical document validation or other formatting, but does scan each message for malicious code or content. All activities are performed as permitted by the Business Associate Agreement or other service agreement.

6.7.2 Authentication of End Users

Cerner requires at minimum DT Auth LoA-1in context of accessing End User mailboxes offered by applications using the Cerner Direct HISP. This involves memorized passwords of six characters in length and a throttling mechanism which limits password fails to three per day before invoking CAPTCHA technology.

Password resets involve successfully answering a set of personal knowledge questions (empty answers are prohibited), in addition to proof of control of the email address associated with the account and successful login—all subject to the same throttling mechanism described above. Cerner does not distribute initial passwords.

Cerner utilizes TLS for any connections with Intermediate Systems to help reduce risk of man-in-the-middle attacks.

6.7.3 Authentication of Intermediate Systems

The Cerner Direct HISP requires secure http authentication using OAuth authorization of an Intermediate System (such as an Electronic Health Record) to the HISP system in order to send or receive Direct messages on behalf of an End User.

The Cerner Direct HISP does not require pass-through authentication of an End User by the Intermediate System. The Intermediate System must maintain an accounting of End User access and must make this accounting available when requested by the HISP for auditing purposes. Intermediate Systems must implement End User authentication using at minimum DT Auth LoA-1.

Cerner utilizes TLS for any connections with Intermediate Systems to help reduce risk of man-in-the-middle attacks.

6.7.4 Access Controls (Internal Access)

Cerner has defined policies and procedures established to provide guidance to secure logical access to Cerner's assets, including systems that contain sensitive information including Electronic PHI. Cerner's policies and procedures define specific access methodologies (i.e. individual, role based, business unit access) depending on the general role description of the Associate, and also define how exceptions to the policy are addressed. These policies and procedures extend to vendors, contractors and their employees and incorporate ongoing monitoring to ensure right of access to a workstation, transaction, program or process remains appropriate over time. Associate physical access is performed in accordance with § 5.1.2.

Associates are required to complete a background check and drug screen prior to initial employment in accordance to § 5.3.2.

Cerner has defined policies and procedures describing the process of removing Associate accounts, access and privileges when Associates depart from Cerner or transition from Cerner Technology Services (CTS) or Tech Delivery Services (TDS) to other Cerner organizations. The Cerner Direct HISP also enforces a checklist incorporating the necessary steps taken when a Cerner Direct HISP application development or operations team member departs from Cerner or transitions to a new team within Cerner.

All Associates have unique user names and passwords. Corporate policy dictates no account sharing for any system or application. Access to the Cerner Direct HISP environment is carefully managed to protect the reliability and accuracy of these systems and the privacy and sanctity of the data.

Cerner's password standard operating procedure states that password protected screen savers should be used on end user devices when an Associate is away from their device or the system has been idle for 10 (ten) minutes. Desktop management policies require desktop locking with passwords and servers are configured with standard time-out periods. End User applications accessing mailboxes managed by the Cerner Direct HISP terminate sessions after 60 (sixty) minutes of inactivity.

6.8 Time Stamping

All system clock time for the Cerner Direct HISP is derived from synchronization to a local NTP server cluster with time sources provided by the National Institute of Standards and Technology (NIST) via public internet connectivity using the NTP protocol. The Cerner Direct HISP default accuracy allows for variance up to 128ms before it forces a recalculation.

6.9 Direct Messaging Operations

6.9.1 CA and RA Services

The Cerner Direct HISP only uses accredited CA and accredited RA third party partners to provision and manage Certificates used for Direct messaging.

6.9.2 End User/Subscriber Agreements

Cerner contracts directly with Covered Entities, Business Associates and Healthcare Entities (as each is defined by the DirectTrust CP) utilizing the Cerner Direct HISP. The Business Associate Agreement (BAA) is a standard component of those HISP contracts, as required by law.

All contracts include, but are not limited to, obligations of the Subscriber concerning identity proofing expectations of their End Users, participation in the directory, record retention, incorporation of the privacy policy of the HISP, any permitted uses of Electronic PHI sent by or received for the Subscriber by the HISP, prohibited activities, any obligations of the HISP regarding reporting to the Subscriber of unauthorized use of client PHI or security incidents of which the HISP becomes aware, any terms a

HISP must require of subcontractors that will handle Electronic PHI, and the disposition of Electronic PHI by the HISP upon termination of the contract.

The Cerner Direct HISP terms of use can be found at:
https://cernerdirect.com/inboxes/welcome-terms

The Cerner Direct HISP privacy policy can be found at: https://cernerdirect.com/inboxes/welcome-privacy.

6.9.3 Trust Management

The Cerner Direct HISP manages trust anchor Certificates on behalf of its End Users and Subscribers, and has well-defined, Subscriber-available policies for evaluating the Certificate issuance policies, trustworthiness and selection of those third party trust anchors, including a secure method for obtaining those trust anchor Certificates.

Trust is established at the trust anchor Certificate level, meaning trust decisions are made by matching the Distinguished Name and Public Key of an issuing CA in the Certificate chain, or of the counterparty itself when the Certificate is self-signed, against a local list of explicitly trusted anchors for acceptance, all others are rejected. This is referred to as “whitelisting”. The HISP does not support whitelisting by Direct address or Direct health domain, rather only by trust anchor Certificates for making trust decisions.

Support is provided for bundles of Trust Anchors as described in the Trust Bundle Distribution IG. Bundles are refreshed at 24 hour intervals. Cerner leverages one or more trust bundles as the default trust mechanism for bi-directional and outbound, one-way, Direct exchange.

The HISP enforces permitted key usages for Certificates it controls if the field or extension is marked as critical. It does enforce critical extensions on Counterparty Certificates with the exception of key usage. The HISP is also capable of imposing additional local policy restrictions such as specific content in the Certificate policy extension, or any other field or extension in a Counterparty Certificate or in any of its superior issuing CA Certificates.

6.9.4 Direct Messaging Protocols

The Cerner Direct HISP performs authentication, encryption, trust verification and acknowledgement of responsibility to deliver the message utilizing SMTP transport protocol as specified in the Applicability Statement for Direct Secure Health Transport defined in § 1.6.2 in order to securely route messages from sender’s address to intended recipient’s address.

Support for DNS and LDAP methods for discovering recipient Certificates is implemented as specified in the current Certificate Discovery IG.

The Cerner Direct HISP utilizes components from the *Direct Project Java Reference Implementation* open source, source code to implement core HISP functionality.

6.9.4.1 Message Disposition Notifications (MDNs)

The Cerner Direct HISP implemented the response mechanism for final delivery notification requests received in accordance with the Delivery Notification IG. Specifically, when the HISP receives an incoming Direct message invoking the final delivery notification request mechanism, the HISP responds to the sender with either a Dispatched MDN or failure notification in accordance with the Delivery Notification IG. The HISP also supports the request mechanism for final delivery notification in outgoing messages in accordance with the Delivery Notification IG.

In cases where the HISP is responsible for providing final message storage for the recipient, then a positive delivery notification as defined by the Delivery Notification IG is issued upon delivery to the recipient's inbox. If the HISP delivers received messages to an intermediate system, then a positive delivery notification is issued upon successful handoff of the message to the intermediate system, as defined by the HISP APIs. A positive delivery notification is not a "read receipt" and does not imply that the message was opened, viewed, or acted upon by the recipient.

The HISP will not delay the transmission of processed MDNs in response to incoming Direct messages. Once the HISP has successfully decrypted a message, verified trust and message integrity, a Processed MDN will be transmitted promptly to indicate to the sender that the HISP has received the message and is taking responsibility to attempt delivery to a recipient or endpoint serviced by the HISP. If such delivery attempt subsequently fails, the HISP will transmit a failure notification to the sender.

In the cases where one-way trust is enabled for sending or receiving Direct messages with a Counterparty, the HISP allows for receipt and/or transmission of corresponding message disposition notifications in accordance with the Applicability Statement and, when applicable, the Delivery Notification IG.

The HISP has established time-out intervals for receipt of expected message disposition notifications from Counterparty HISPs and provides failure notifications when those time-out intervals have been exceeded. The time-out interval is one hour for receipt of routine Processed MDNs and one hour for receipt of Dispatched MDNs.

In all cases where the HISP sends a message, yet receives a delayed failure notification message (i.e. failure MDN or failure DSN) after receiving a routine Processed MDN from the Counterparty HISP, the HISP will report those failures to the sender.

In cases where the HISP sends a message with a request for final delivery notification to a Counterparty HISP that does not support the response mechanism for the final delivery notification protocol, no Dispatched MDN will be received and, per the requirements of the Delivery Notification IG, the message will always be reported to the sender as a failure, even if the message was actually received by the Counterparty.

6.9.4.2 Message Wrapping

In order to protect against certain in-transit header re-writing attacks, the Cerner Direct HISP protects the outer, non-content-related message header fields when sending a message on behalf of an End User by wrapping the message as specified in § 3.1 of the "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," RFC 5751, published by the Internet Engineering Task Force and is able to accept and process incoming messages wrapped in this manner. The HISP will validate that sender and recipient information for an incoming message is consistent with the protected headers within the message/rfc822 wrapper and with the signer and encryption Certificates used. The HISP will reject incoming messages as untrusted if inconsistencies are found relating to sender and recipient information.

The Cerner Direct HISP uses the same non-content-related message header fields in both the outer headers and the wrapped headers for consistency, suppresses the "Subject" header field in the outer message to mitigate inadvertent exposure to PHI, and does not allow for Bcc: or blind carbon copy recipients in order to ensure the best opportunity for reconciliation of SMTP envelope data with the protected headers by all Counterparties.

When receiving a message on behalf of an End User, the HISP will allow incoming messages that are not wrapped messages in the interest of supporting interoperability with older systems.

The Cerner Direct HISP processes any message disposition notification requests included in the wrapped headers in accordance with § 6.9.4.1. Message disposition notifications sent in response to a wrapped message will set the value of Original-Message-ID field of the outgoing message disposition report to the value of the Message-ID field within the protected inner headers if this value is different from the outer Message-ID to aide in the sending system reconciliation of original message status and tracking.

6.9.4.3 Case Sensitivity

For incoming messages, the Cerner Direct HISP treats the Direct Addresses that it services in a case-insensitive manner. When address Certificates are used, the HISP will treat Subject Alternative Name rfc822Name entries in a case-insensitive manner when validating the binding between a Direct Address and the rfc822Name. The domain part of any Direct Address and any dnsName included in a domain-bound Certificate is always treated in a case-insensitive manner.

6.9.4.4 Message Canonicalization

The Cerner Direct HISP prepares the message content for signing in accordance with § 3.1 of RFC 5751. The Cerner Direct HISP requires all edge systems to properly canonicalize messages.

The HISP treats the received content as if it were properly canonicalized by the sender (i.e. perform no further canonicalization) when computing the message digest on an incoming message to validate digital signature.

6.9.5 Directory Services

Cerner provides directory services for the purpose of identifying the Direct Addresses of Counterparties in addition to offering the Cerner Direct HISP. Cerner's directory usage policy can be found here: http://www.cerner.com/health_care_directory_policy/?langtype=1033.

7 Certificate, CRL, and OCSP Profiles Format

7.1 Certificate Profile

The Cerner Direct HISP is able to process and use Certificates issued in conformance with the Certificate profiles defined in the DirectTrust CP.

Independent audit demonstrating compliance to these capabilities occurs at minimum annually.

7.1.1 Version Numbers

No stipulation beyond conformance with the DirectTrust CP.

7.1.2 Certificate Extensions

No stipulation beyond conformance with the DirectTrust CP.

7.1.3 Algorithm Object Identifiers

No stipulation beyond conformance with the DirectTrust CP.

7.1.4 Name Forms

No stipulation beyond conformance with the DirectTrust CP.

7.1.5 Name Constraints

No stipulation beyond conformance with the DirectTrust CP.

7.1.6 Certificate Policy Object Identifier

No stipulation beyond conformance with the DirectTrust CP.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The Cerner Direct HISP processes Certificate extensions in accordance with § 6.9.3.

The HISP may reject a Certificate if it encounters an extension it does not recognize or a critical extension that contains information that it cannot process following review of the full context of the message.

7.2 CRL Profile

The Cerner Direct HISP processes and uses CRLs issued in conformance with the CRL profile defined in the DirectTrust CP.

7.2.1 Version Numbers

No stipulation beyond conformance with the DirectTrust CP.

7.2.2 CRL and CRL Entry Extensions

No stipulation beyond conformance with the DirectTrust CP.

7.3 OCSP Profile

No stipulation beyond conformance with the DirectTrust CP.

8 Compliance Audits and Other Assessments

The HPC is comprised of representatives from the applicable organizations within Cerner responsible for operation of the HISP. It is the responsibility of the each HPC representative to ensure their organization is following the policies and procedures in this HPS.

8.1 Frequency and Circumstances of Assessment

Independent audits are performed annually and cover the controls specific to the CTC remote hosted and system management services. The facility, management, and operational controls within the CTCs are reviewed on an annual basis as per SOC 1 (SSAE18) and SOC 2 reports. Cerner leverages the DirectTrust Accreditation program with the additional DirectTrust-sanctioned HIPAA Privacy and Security audits to certify compliance of the HISP to the requirements of the DirectTrust HP.

In years where an independent audit is not performed, DirectTrust requires proof that the Cerner Direct HISP adheres to a set of DirectTrust CP requirements.

8.2 Identity/Qualifications of Assessor

Due to the nature of Cerner's business, Cerner's internal auditors possess experience gained through regular audit participation in internal and external audit, certification and accreditation programs such as ISO27001 (UK Hosting) Certification, ISO9001, SOC 1 (SSAE18), SOC 2, and PCI attestation.

An external audit of the CTC is done in accordance with § 8.1.

8.3 Assessor's Relationship to Assessed Entity

Cerner leverages independent compliance auditors with respect to determining conformance to the requirements contained within the Direct Trust HP. Results of the assessment are communicated in accordance with § 8.6.

8.4 Topics Covered by Assessment

The Cerner Direct HISP assessment occurs in accordance with § 8.1 and covers the topics outlined within this HPS.

8.5 Actions Taken as a Result of Deficiency

Any material deficiencies identified as a result of reviews included in § 8.1 are remediated through an action plan.

8.6 Communication of Results

The Cerner Direct HISP conformance to the DirectTrust HP and related accreditation compliance assessment and audit process can be found on the DirectTrust web site.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fee

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

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

9.1.5 Refund Policy

Cerner does not issue refunds for fees related to Cerner Direct HISP 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/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;
- Subscriber Agreements;
- Audit logs for types specified in § 5.4;
- Cerner policies and procedures related to this HPS; and
- Audit reports and related documentation.

Except as expressly permitted by this HPS, neither Subscriber nor Cerner will disclose, use, copy, distribute, sell, license, publish, reproduce or otherwise make available Confidential Information of others.

9.3.2 Information not within the scope of Confidential Information

Confidential Information will not include any information (i) that is publicly available through no breach of this HPS, (ii) that is independently developed by Subscriber or Cerner, (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, or (iv) that is published as part of the directory services described in § 6.9.5.

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 in accordance with § 5.3.3.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

See § 9.3.1. Information included in Certificates and information described under § 9.3.2 is not deemed private.

9.4.4 Responsibility to Protect Private Information

See § 9.3.3. 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 HPS, the privacy policy referenced in § 9.4.1, and applicable Subscriber Agreements.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Notwithstanding the foregoing, Cerner may disclose confidential 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 HISP. Cerner hereby reserves all rights not expressly granted hereunder. Cerner will not knowingly violate the intellectual property rights held by others.

9.6 Representations and Warranties

9.6.1 HISP Representations and Warranties

Except as expressly set forth herein or in a Subscriber Agreement or other agreement with an impacted party, Cerner makes no warranties related to the Cerner Direct HISP. However, Cerner represents that it will (i) perform its functions under this HPS in a professional manner, and (ii) comply, in all material respects, with applicable laws, regulations and this HPS when performing its functions set forth in this HPS.

9.6.2 CA/RA Representations and Warranties

Cerner uses a third party to perform the CA and RA functions. Their Certificate Practice Statement, inclusive of any applicable representations and warranties, can be found at www.cerner.com/cps.

9.6.3 End User Representations and Warranties

No stipulation beyond conformance with the DirectTrust CP. Subscriber Agreements may include additional representations and warranties.

9.6.4 Counterparty Representations and Warranties

Counterparty 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 HPS, (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. Counterparties are solely responsible for any representations they make to third parties and for all transactions using their Certificates.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations have the same representations and warranties as Subscribers in accordance with § 9.6.6.

9.6.6 Representations and Warranties of Other Participants

Subscriber warrants that (i) the information provided by the Subscriber within the Certificate is true, accurate and complete, (ii) it has completed required identity verification as set forth in § 3, (iii) the Certificate will be used in conformance with this HPS 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.

9.7 Disclaimers of Warranties

THE CERNER DIRECT HISP IS PROVIDED ON AN AS-IS AND AS-AVAILABLE BASIS. CERNER EXPRESSLY DISCLAIMS ALL WARRANTIES, BOTH EXPRESS AND IMPLIED. SPECIFICALLY, AND WITHOUT LIMITATION, CERNER DOES NOT WARRANT THAT THE

CERNER DIRECT HISP WILL BE ERROR-FREE OR UNINTERRUPTED OR THAT ANY DEFECTS WILL BE CORRECTED.

9.8 Limitations of Liabilities

UNLESS OTHERWISE SET FORTH IN A SUBSCRIBER AGREEMENT OR OTHER APPLICABLE AGREEMENT WITH AN IMPACTED PARTY, CERNER WILL NOT BE LIABLE UNDER THIS HPS FOR 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. THIS LIMITATION SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY LAW.

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 HPS, and (ii) its use of the Cerner Direct HISP, other than those Claims arising out of or related to Cerner’s negligence or willful misconduct in providing the Cerner Direct HISP. Additional indemnities may be found in the Subscriber Agreement.

9.10 Term and Termination

9.10.1 Term

The HPS is effective immediately upon publication and has no specified term. 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 HPS may occur if approved by the HPC.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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 HPS may be amended by the HPC in accordance with § 1.5.4.

9.12.2 Notification Mechanism and Period

Cerner may provide notification of a change to this HPS in its sole and exclusive judgment.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

This HPS 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.

Cerner's Corporate Policy Board is responsible for initiating an annual review of the Information Security policy and sponsoring a working group to perform the policy review. The scope of the annual review should be focused on major areas of improvement as identified through IT quality monitoring or as required by the business. The review should include the following:

- An analysis of the general information security practices applicable to current technology, business and process requirements.
- A gap analysis of general information security practices against current industry standards such as those published by the International Standards Organization (ISO), major regulatory bodies or other similar organizations.
- An open "Request for Comments" from business units, groups or departments to allow for any requests for changes or reviews of specific sections of the practice such that the CTS Enterprise

Security Organization can address requests based upon an risk analysis of the comments and suggestions.

- A review of any impacting legal changes to ensure practice compliance with the local laws where the organization has a point of presence

Cerner's policy review process is an automated process that is managed via its online document management system.

In context of the Cerner Direct HISP, Cerner's status under HIPAA is Business Associate.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This HPS constitutes the entire agreement related to the subject matter of this HPS and supersedes all prior or contemporaneous agreements, representations and proposals, written or oral, if any, regarding such subjects. If Cerner has entered into an agreement with an impacted party hereto (such as a Subscriber Agreement) then such agreement controls but only with respect to that impacted party.

9.16.2 Assignment

Unless otherwise set forth in the Subscriber Agreement or other applicable agreement with an impacted party, Cerner may assign its rights and obligations under this HPS in its sole discretion, with or without notice. No other entity operating under this HPS may assign its rights or obligations without Cerner's prior written consent.

9.16.3 Severability

This HPS obligates the parties only to the extent that its provisions are lawful. Any provision prohibited by law will be ineffective (but only to the extent that, and in the locations where, the prohibition is applicable). The remainder of the HPS will remain in full force and effect if the HPS can continue to be performed in furtherance of its objectives.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

Cerner will be not responsible for failing to perform under this HPS due to causes beyond its reasonable control, including, but not limited to, failures by Cerner's suppliers or subcontractors, war, sabotage, riots, civil disobedience, acts of governments and government agencies, labor disputes, accidents, fires, acts of terrorism, or natural disasters. Cerner will perform its obligations within a reasonable time after the cause of the failure has been remedied.

9.17 Other Provisions

No stipulation.