phiCert™ Certificate Policy and Certification Practices Statement

Version 1.5

Effective Date: January 31, 2021

[Trademark Notices]
phiCert is a trademark of EMR Direct.

Revision History

Version	Effective Date	Details
1.5	January 31, 2021	Updated §§ 1.1-3, 1.6, 3.1-2, 6.2-3, and subsections thereof, for mapping to version 2.0 of the DirectTrust CP and miscellaneous corrections and clarifications.
1.4.3	September 16, 2019	Updated §§ 1.1-2, 3.1-2, 4.1, 5.6, 6.2 and subsections thereof, for addition of IAL1 and IAL2 proofing levels and miscellaneous corrections and clarifications.
1.4.2	June 26, 2019	Updated §§ 1.1-4, 1.6, 2.4, 3.1-2, 4.1-4, 4.6-9, 5.2, 6.1-2 and subsections thereof, for mapping to version 1.4 of the DirectTrust CP and miscellaneous corrections and clarifications.
1.4.1	December 20, 2018	Removed “Direct” from title of document; updated: §§1.1-4, 1.6, 3.1-2, 4.2, 5.2, 4.9, 7.1, 9.6 and subsections thereof, clarifying requirements unique to Direct Messaging uses, and miscellaneous corrections and clarifications.
1.4	July 3, 2017	Updated: §§1.1-4, 1.6, 3.1-3, 4.3, 4.5, 4.7-4.9, 5.1, 6.1-6.2, 7.1, 9.6, 9.9, 9.12-14, 9.16 and subsections thereof, for mapping to version 1.3 of the DirectTrust CP and miscellaneous corrections and clarifications.
1.3	March 29, 2016	Updates to §§ 1.2, 3.1.1.4-6 and 3.2.2; miscellaneous corrections and clarifications.
1.2	February 8, 2016	Updates for policy mapping and for new versions of NIST 800-63, ONC Applicability Statement, and DirectTrust CP; miscellaneous corrections and clarifications.
1.1	March 31, 2014	Updated: §§1.1, 1.1.4, 1.2, 1.3.2, 1.3.4, 1.4.1, 1.4.2, 3.1 & subsections, 3.2 & subsections, 4.2, 4.8 & subsections, 5.1.2, 5.5.2, 6.1.2, 6.3.1, 6.3.2, 7.1.2 & subsections
1.01	January 28, 2014	Updated: §§1.1.4, 1.2, 1.6.1, 1.6.2, 5.5.1, 6.2.1
1.0	April 23, 2013	Initial version

Table of Contents

1 Introduction

1.1 Overview

This document is the phiCert Certificate Policy Certification Practices Statement ("this CP/CPS", "the phiCert CP/CPS") and is issued by EMR Direct ("the Company", "us", "we", "our"). This CP/CPS describes the overall business, legal, and technical infrastructure that we employ in maintaining the phiCert public key infrastructure ("our PKI"), including the policies and procedures we use in approving, issuing and managing X.509 digital certificates, and defines the assurance that can be placed in these certificate. The effective date of this document can be found on the title page.

This CP/CPS assumes that the reader is familiar with the general concepts of digital signatures, certificates, encryption, and public key infrastructure. If not, EMR Direct advises that the reader obtain training in the use of public key cryptography and public key infrastructure as implemented in our PKI sufficient to understand this document.

This phiCert CP/CPS generally conforms to the policy framework described in RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, issued by the Internet Engineering Task Force. In order to preserve the framework of RFC 3647, some sections of this CP/CPS will include the statement "No stipulation" or "Not applicable." We reserve the right to vary from this framework in our sole discretion.

Our PKI is intended to enable the secure electronic exchange of information between PKI participants, in uses cases where authentication, content integrity, and/or confidentiality is required.

X.509 digital certificates ("Certificates") issued by our Certification Authorities ("CAs") to our Subscribers for use within our PKI contain one or more registered certificate policy object identifiers ("OIDs"). The OIDs are asserted in the certificate policies extension of the Certificate and corresponds to the specific levels of assurance defined by this CP, as discussed further in §§ 3 and 7 of this CP/CPS. At this time, we define the "phiCert Certificate Policy" at six levels of assurance: "LOA-1" through "LOA-3", generally conforming to the identity proofing requirements of NIST 800-63-2 levels of assurance 1 through 3, respectively, but specifically defined below; "IAL1" and "IAL2", intended to provide equivalent identity assurance to the identity proofing requirements of NIST SP 800-63-3A; and "Basic", generally conforming to the requirements of the Federal Bridge CA certificate policy of the same name, and included to facilitate policy mapping.

1.1.1 Role of the phiCert CP/CPS and Ancillary Agreements

In addition to this CP/CPS, there are ancillary agreements between us and other PKI Participants. These agreements bind Customers, Subscribers, and Relying Parties of EMR Direct. Among other things, these agreements flow down requirements listed in this CP/CPS to these

PKI Participants and, in some cases, state specific practices for how they must meet these requirements.

1.1.2 Background concerning Direct Messaging and the phiCert PKI

Our Certificates are intended for use in applications related to the secure electronic exchange of information over the Internet. This includes the transport of health information as described in the document entitled Applicability Statement for Secure Health Transport, Version 1.2, August 3, 2015, by the Direct Project, and referred to in this CP/CPS as "the Direct Project Applicability Statement". The Direct Project began as an initiative of the Office of the National Coordinator for Health Information Technology ("the ONC"), U.S. Department of Health & Human Services. This CP/CPS assumes that the reader is familiar with the Direct Project Applicability Statement.

Secure transport of health information over the Internet as described by the Direct Project Applicability Statement is based on S/MIME, and is known variously as Directed exchange, Direct exchange, Direct secure messaging, and Direct messaging, among other names, and is referred to in this CP/CPS as "Direct Messaging." Messages with content secured in conformance with the requirements of the Direct Project Applicability Statement are referred to in this CP/CPS as "Direct messages". The terms "Direct Address", "Health Domain Name" and "Health Endpoint Name", as used in this document, are defined in the Direct Project Applicability Statement, §§ 1.0, 1.1, and 1.2, respectively.

1.1.3 Relationship between the phiCert CP/CPS and other certificate policies

From time to time, we may determine that one or more of our certificate policies map to a certificate policy of another PKI ("Foreign PKI") sufficiently to deem the two policies substantially equivalent. Such determination shall be made by the Director of Certification Practices only after a formal mapping of the two policies is performed. Where we also determine that cross-certification with a CA issuing certificates in that Foreign PKI would enhance overall interoperability for our Subscribers, we may choose to exchange cross-certificates with that CA. The decision to exchange cross-certificates is also made by the Director of Certification Practices. In those cases, the relationship between the Foreign CP and the phiCert CP will be asserted in the *policyMappings* extension of the respective cross-certificates.

In cases where we determine that substantial equivalence with a CP from another PKI ("Foreign CP") exists but cross-certificates are not exchanged, we may choose to assert one or more Foreign CP object identifiers in the certificate policies extension of our CA Certificates and/or end-user Certificates, when permitted by the Foreign CP, if we determine that doing so would enhance overall interoperability for our Subscribers. The decision to permit assertion of Foreign CP OIDs is also made by the Director of Certification Practices.

1.1.4 Relationship between the phiCert CP/CPS and DirectTrust.org CP

DirectTrust.org is an independent non-profit trade association that publishes bundles of CA certificates for use by relying parties. In this document, we refer to the CAs we operate whose certificates are included (or may be considered for inclusion) in a DirectTrust.org bundle, and their subordinate CAs, as "DirectTrust Bundle CAs". DirectTrust.org requires DirectTrust Bundle CAs to assert certain policy OIDs defined in the DirectTrust CP in their respective end entity certificates. We have determined that substantial equivalence exists between the provisions of our CP/CPS and the DirectTrust Community X.509 Certificate Policy, Version 2.0, dated October 7, 2020, ("the DirectTrust CP", identified by OID 1.3.6.1.4.1.41179.0.2.0). As such, we will assert the DirectTrust CP OID in all end entity Certificates issued by one of our DirectTrust Bundle CAs. Should we determine that our policies and practices continue to conform substantively to any future version of the DirectTrust CP, we may choose to begin asserting the updated DirectTrust CP OID or OIDs in our CA and/or Subscriber Certificates instead.

We have also determined that sufficient equivalence exists between our Certificate Policy requirements and certain other policy OIDs defined in the DirectTrust CP to justify their use in our Certificates issued by one of our DirectTrust Bundle CAs when such use is required by the DirectTrust CP. Specifically, our CP/CPS is intended to assign equivalent meaning to the OIDs defined in the DirectTrust CP to identify entity type in OID arc 1.3.6.1.4.1.41179.2, and to identify certificates issued to devices with DirectTrust Device OID 1.3.6.1.4.1.41179.3.1. Additionally, we follow substantively equivalent requirements for level of assurance for identity proofing for phiCert levels LoA-1 through 3 and IAL1 through 2 defined in this CP/CPS as compared to the corresponding DirectTrust levels in OID arc 1.3.6.1.4.1.41179.1. Therefore, we have concluded that the overall meaning of the level of assurance is sufficiently equivalent that we may assert the supported DirectTrust OIDs in our Certificates.

1.2 Document Name and Identification

This document is the "phiCert Certificate Policy and Certification Practices Statement, Version 1.5" which was approved by EMR Direct management on 1/30/2021. There are six certificate policies specified in the phiCert CP/CPS, identified in the table below and defined in subsequent sections of this CP/CPS. Where not otherwise specified, the requirements defined in this CP/CPS shall apply to all policies.

Name	Short Name	Object Identifier (OID)
Base OID of phiCert arc	id-phicert	::= { joint-iso-itu-t(2) country(16) us(840) organization(1) hl7(113883) externalUseRoots(3) emrdirect(2681) phicert(1) }
phiCert Certificate Policies	id-phicert-cp	::= { id-phicert 1 }
phiCert LOA-1		::= { id-phicert-cp 6 }
phiCert LOA-2		::= { id-phicert-cp 7 }
phiCert LOA-3		::= { id-phicert-cp 8 }
phiCert Basic Assurance		::= { id-phicert-cp 9 }
phiCert IAL1		::= { id-phicert-cp 10 }
phiCert IAL2		::= { id-phicert-cp 11 }

1.3 PKI Participants

The community governed by this CP/CPS is our PKI. Our PKI accommodates a large, public, and widely distributed community of individuals and organizations with a need to securely exchange information over the Internet. Participants in our PKI are located primarily within the United States of America, and include us, Customers, Subscribers, Relying Parties, Certification Authorities, Registration Authorities, Resellers, and Referrers. This CP/CPS applies to all Participants in our PKI.

1.3.1 EMR Direct Management

The management team of EMR Direct has established this PKI, oversees its operation, and is responsible for governing and promoting its use. This CP/CPS was established under the authority of and with the approval of the EMR Direct management.

1.3.2 Certification Authorities

The term Certification Authority (“CA”) is an umbrella term that refers to any entity which creates, signs, and issues X.509 public key certificates within our PKI. We operate all CAs within our PKI. Our CAs also perform other certificate management functions, including approval, renewal, re-keying, modification, and revocation of certificates and publication of certificate status information within our PKI. Each CA performs its functions in accordance with the requirements of this CP/CPS.

A CA is the Issuing CA with respect to the Certificates it issues and is the Subject CA with respect to the Certificates issued to it. A Root CA is both the Subject CA and Issuing CA of its own Root Certificate.

Our PKI operates as a hierarchical PKI. Each CA may issue Certificates to one or more Subordinate CAs. Only Subordinate CAs issue Certificates to end-user Subscribers. Root CAs do not issue Subscriber Certificates. This restriction is enforced through defined certificate profiles for each Issuing CA.

To facilitate management of trust for our Subscribers, our CAs may assert one or more specific certificate policies or levels of assurance in Certificates issued to Subordinate CAs. Such assertion will be made in the certificate policies extension. In these cases, these policy terms limit the set of policies for certification paths that include this Subordinate CA. However, if our CA does not intend to limit the set of policies, the special *anyPolicy* OID (2.5.29.32.0) may be asserted in the certificate policies extension.

1.3.3 Registration Authorities

A Registration Authority (RA) collects and verifies information from applicants, performs identification and authentication of applicants, initiates or passes along revocation requests for Certificates, and approves applications for renewal or re-keying Certificates on behalf of a CA. We operate our own RA, which performs all RA functions for all Certificates issued by our CAs in accordance with this CP/CPS.

1.3.4 Trusted Agents

A Trusted Agent is an entity that acts on behalf of our RA to collect and/or verify information regarding Subscribers, and, where applicable, to provide support regarding those activities to Subscribers. Trusted Agents have a direct contractual relationship with us obligating the Trusted Agent and, where applicable, the Trusted Agent's employees and/or agents, to perform these functions in accordance with this CP/CPS, and to provide any proofing artifacts to our RA upon request, including any artifacts from historical proofing events at the Trusted Agent's organization.

1.3.5 Subscribers

A Certificate is issued to a Subscriber. A Subscriber may be either (a) a natural person or other legal entity, or (b) a single Device with a designated human sponsor, as defined in CP/CPS § 3.2.3.4. Prior to issuance of a Certificate, a Subscriber is known as an Applicant. The Subscriber is identified in the subject field of a Certificate.

If the Subscriber authorizes any other entity to control or use the associated private key, such as when a HISP Security Officer is appointed to manage the associated private key, then the Certificate is a "Group Certificate" as discussed in CP/CPS § 3.2.3.3.

As a technical matter, our CAs are themselves also Subscribers, either as a subordinate CA issued a Certificate by a superior CA, or as a Root CA issuing a self-signed Certificate to itself. In this CP, however, "Subscriber" refers only to end-user Subscribers, unless otherwise specified.

1.3.6 Affiliates

An Affiliate is an individual or other entity legally distinct from the Subscriber who is authorized by the Subscriber to use Direct Addresses bound to the Subscriber's Certificate, provided that the Affiliate is performing its work, duties or activities on behalf of the Subscriber when using that Direct Address. When the Subscriber is a patient, an individual authorized by the patient to access the patient's Direct account is also considered an Affiliate.

1.3.7 Sponsoring Organizations

A Sponsoring Organization sponsors an individual or Device to be a Subscriber of a Certificate that indicates an affiliation between the Subscriber and the Sponsoring Organization. An authenticated and authorized representative of the Sponsoring Organization shall confirm the affiliation between an individual or Device and the organization. When an organization has sponsored an individual or Device as a Subscriber of a Certificate, the individual or Device is acting on behalf of and as an agent of the Sponsoring Organization when using the Certificate and/or the corresponding keys.

1.3.8 Relying parties

Relying parties are entities that rely on our Certificates in order to exchange information with Subscribers. Each Relying Party is solely responsible for determining the suitability of a Certificate for a particular use in accordance with this CP/CPS. Subscribers may also be Relying Parties.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Our Subscriber Certificates are intended for use in securing the electronic exchange of information, and related applications, in a manner compliant with the security and privacy rules of HIPAA and HITECH and any other applicable law or regulation. Examples include, but are not limited to, the secure transport of health information over the Internet as described in the Direct Project Applicability Statement and applications enabling access to data by consumers. Our Subscriber Agreements require Subscribers to acknowledge that they are solely responsible for obtaining any necessary consents or approvals, or executing any other agreements, when required by HIPAA, HITECH, or any other governmental statute or regulation, as applicable, prior to each use of their Certificate or initiation of any transmission of data with a digital signature that may be verified by a Relying Party by using their Certificate.

Notwithstanding the above, Certificates may also be used for other authenticated communications, including communications with us that are incidental to certificate renewal, re-keying, and modification, as detailed in CP/CPS §§ 4.6.3, 4.7.3, and 4.8.3, respectively. We may maintain one or more Direct Addresses and associated Certificates for the purposes of such communications, or for purposes of interoperability testing and troubleshooting. We may also issue Certificates to Subscribers for the purposes of communicating with us, or for the purposes of interoperability testing and troubleshooting. CA Certificates are used only to support the use of Subscriber Certificates.

Our Subscriber Agreements and Relying Party Agreements specify appropriate certificate uses consistent with the terms of this CP/CPS § 1.4.1. If we determine that a Subscriber is using a Certificate issued by us for purposes other than those allowed in this section, we may, at our sole discretion, revoke the Subscriber's Certificate. Such determination may be made by our Registration Authority or Certification Authority.

1.4.2 Restricted and Prohibited certificate uses

A Subscriber Certificate only establishes that the information in the Certificate was reasonably verified to a specified level of assurance prior to issuance of the Certificate. It does not establish the trustworthiness of a Subscriber. In determining the level of assurance required in any particular application or transaction, Relying Parties must evaluate the threats and vulnerabilities they are willing to accept based on the sensitivity or significance of the information to be exchanged. This evaluation must be performed by each Relying Party and is not controlled by this CP/CPS.

The following restrictions on use apply to the Certificates that we issue:

a. Certificates shall be used only to the extent permitted by applicable law, including but not limited to HIPAA, HITECH, and any applicable import or export laws;
b. Certificates shall not be used for purposes other than those described in CP/CPS § 1.4.1;
c. Certificates shall not be used for purposes that are inconsistent with the permitted key usage(s) and, when applicable, the extended key usage(s) asserted in each Certificate; and
d. Certificates shall not be used for any application whose failure could lead to injury or death, examples including, but not limited to, any application used as a substitute for direct verbal communication with clinicians in life-threatening situations or for communication of critical medical results.

Use of a Direct Messaging Certificate by an Affiliate is subject to the following additional restrictions:

e. A HIPAA Covered Entity may only be an Affiliate of a Subscriber who is also a HIPAA Covered Entity and may not be an Affiliate of a Subscriber who is a Business Associate under HIPAA, except when the Covered Entity is providing services to or on behalf of the Business Associate; and
f. A Subscriber may only authorize a health care provider or health care organization as an Affiliate if (a) the Affiliate provides care on behalf of the Subscriber, and (b) the Subscriber is a HIPAA Covered Entity.

Subscribers or Sponsoring Organizations using Certificates within their own environment may place additional restrictions on the use of Certificates within their environment. However, neither we nor other PKI participants are responsible for monitoring or enforcing any such restrictions within these environments.

CA Certificates shall not be used for any function except CA functions. End-user Subscriber Certificates shall not be used as CA Certificates. This use restriction is enforced by setting appropriate values in the *basicConstraints* extension in issued Certificates as per CP/CPS § 7.1.2.3.

The above restrictions on use flow down into our Subscriber Agreements and Relying Party Agreements, as applicable. If we determine that a Subscriber is using a Certificate issued by us for a restricted or prohibited purpose, we may, at our sole discretion, revoke the Subscriber's Certificate. Such determination may be made by our Registration Authority or Certification Authority.

1.5 Policy Administration

1.5.1 Organization administering the document

EMR Direct is responsible for all aspects of this CP/CPS. EMR Direct means California Mediterranean, LLC, a California limited liability company, dba EMR Direct.

1.5.2 Contact person

EMR Direct designates our Director of Certification Practices as the contact Person for inquiries about this CP/CPS. Only the Director of Certification Practices and his or her appointees are authorized to respond to inquiries about this CP/CPS. Inquiries may be directed to:

Director of Certification Practices
EMR Direct
PO Box 676011
Rancho Santa Fe, CA 92067
(858) 367-0770
cps@emrdirect.com

1.5.3 Person determining suitability of documents under our CP/CPS

The Director of Certification Practices is responsible for determining suitability of all documents under this CP/CPS. The determination of suitability shall be based on an independent compliance auditor's results and recommendations. See § 8 for further details.

1.5.4 CPS approval procedures

The Director of Certification Practices is responsible for approving this CP/CPS and any future changes, updates, or modifications to it. Such approval will be made only after review of any completed compliance audits and resolution of any identified discrepancies.

1.6 Definitions and Acronyms

1.6.1 Acronyms as used in this CP/CPS

CA	Certification Authority or, equivalently, Certificate Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
DN	Distinguished name; additional abbreviations for Distinguished Name attributes can be found in CP/CPS § 3.1.1
FIPS	Federal Information Processing Standard
HIPAA	The Health Insurance Portability and Accountability Act of 1996
HISP	Health Information Service Provider
HITECH	The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009.
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Identifier
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union

ITU-T	ITU Telecommunication Standardization Sector
LOA	Level of assurance
NIST	National Institute of Standards and Technology
NPI	National Provider Identifier
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Health Information Technology
OS	Operating system
PDF	Portable document format
PHI	Protected Health Information, as defined by HIPAA
PKCS#12	Public-Key Cryptography Standards number 12
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
RP	Relying Party
RPA	Relying Party Agreement
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
UPS	Uninterruptible power supply
URI	Uniform resource identifier
US or USA	United States of America
X.500	ISO/IEC Standard 9594-1: “The Directory: Overview of concepts, models and services”
X.509	ISO/IEC Standard 9594-8: “The Directory: Public-key and attribute certificate frameworks”

1.6.2 Definitions as used in this CP/CPS

Applicant	An individual or entity applying for a Certificate. Following issuance of a Certificate, the Applicant becomes a Subscriber.
Certificate	A digital instrument issued by a Certification Authority that conforms to the requirements of the Certificate Profile defined in the document entitled “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 5280, published by the Internet Engineering Task Force, May 2008.
Certification Authority	Also known as a Certificate Authority. An entity that issues Certificates.
Device	A hardware and/or software system or system component that generally operates without the direct intervention of a human Subscriber. Examples include a medical monitoring device attached to a patient that automatically transmits medical data to a healthcare provider as a Direct message, client or server infrastructure equipment, and an electronic health record system that transmits encounter data to a billing company as Direct messages or receives and processes medical data transmitted as Direct messages.
Direct Address	An endpoint for Direct Messaging, as defined in the Direct Project Applicability Statement § 1.0.
Direct Message	An Internet mail message constructed according to the requirements of the Direct Project Applicability Statement.
Direct Messaging	Sending and/or receiving of Direct Messages, including encryption, decryption, digital signing, and/or signature verification according to the requirements of the Direct Project Applicability Statement.
Direct Messaging Certificate	A Subscriber Certificate used for Direct Messaging purposes, i.e. containing public keys used to encrypt a Direct Message or to validate a digital signature in a Direct Message.
Direct Project	Publisher of the Direct Project Applicability Statement. Originally an initiative of the Office of the National Coordinator for Health Information Technology, U.S. Department of Health & Human Services.
Direct Project Applicability Statement	The document entitled “Applicability Statement for Secure Health Transport, Version 1.2”, August 3, 2015, by the Direct Project.

DirectTrust.org	An independent non-profit trade association operating the website www.directtrust.org.
DirectTrust Bundle CA	A CA operated by us whose certificate is included (or may be considered for inclusion) in a bundle of CA certificates published by DirectTrust.org, or any of its subordinate CAs.
DirectTrust CP	The document entitled "DirectTrust Community X.509 Certificate Policy, Version 1.4" dated June 27, 2018, published by DirectTrust.org.
Group Certificate	A Certificate where more than one entity can make use of the associated private key, as described further in CP/CPS § 3.2.3.3.
Health Domain Name	A fully qualified domain name used for Direct Messaging, as defined in the Direct Project Applicability Statement § 1.1.
Health Endpoint Name	The local part of a Direct Address, as defined in the Direct Project Applicability Statement § 1.2.
Participant	An entity that participates in our Public Key Infrastructure by using Certificates and/or providing supporting functions.
Registration Authority	An entity responsible for establishing and executing the enrollment procedures for end-user Certificate applicants, including identification and authentication of applicants.
Relying Party	An individual or organization who relies upon the information contained in a Certificate issued to a Subscriber in order to exchange information with that Subscriber.
Relying Party Agreement	A legal agreement which must be read and accepted by a Relying Party prior to validating, relying on a Certificate, or accessing information contained in our repositories.
Security Officer	The individual responsible for managing Group Certificates as described further in CP/CPS § 3.2.3.3.
Subscriber	Also known as End-user Subscriber. An end-entity to whom a Certificate is issued by a Certification Authority as described further in CP/CPS § 1.3.5.
Subscriber Agreement	A legal agreement that must be read and accepted by the Applicant prior to issuance of a Certificate.
Subscriber Certificate	A Certificate issued to a Subscriber.

Sponsoring Organization	An organization that sponsors an Applicant seeking Subscriber status by affirming an ongoing affiliation between the organization and the Applicant. Subscribers act on behalf of and as agents of a Sponsoring Organization when using Certificates sponsored by that organization and/or the corresponding keys.
User	A natural person or Device authorized by a Subscriber to access or make use of a private key corresponding to a Direct Messaging Certificate.

2 Publication and Repository Responsibilities

2.1 Repositories

EMR Direct operates and maintains repositories of information to support the operation of our PKI as detailed below. EMR Direct operates all public repositories specified in this CP/CPS. We may, in our sole discretion, perform operations of one or more of these repositories in a consolidated or distributed manner. The repositories shall operate 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year (excluding network outages), and scheduled down-time not to exceed 0.5% annually. Where repository systems are distributed, the availability figures shall apply to the system as a whole.

We achieve the above availability by operating our repository at one or more high availability datacenters or co-location facilities with redundant network access and power.

We operate a public document repository within our PKI, wherein we publish this CP/CPS and certain other documents related to our PKI. This repository is accessible through our public website: www.phicert.com. The published documents are made available in a widely adopted document format such as PDF.

We may choose to exclude or remove certain documents related to our PKI from our repository, including, but not limited to, sensitive documents related to internal security matters or trade secrets. We may do so at our sole discretion, even if the excluded or removed documents are referenced by other materials which remain within the repository, such as this CP/CPS. We may publish a CP/CPS summary in place of the complete EMR Direct CP/CPS, should we determine that publication of the complete CP/CPS would constitute a security risk to our PKI. However, the complete CP/CPS shall be made available to auditors for the purposes described in CP/CPS § 8.

2.2 Publication of certification information

Each of our CAs maintains a public repository within our PKI, wherein it publishes its own Certificate Revocation Lists (CRLs) and its CA Certificate. These are made available on our public

website: www.phicert.com. Each CA may also maintain an optional Online Certificate Status Protocol (OCSP) Responder containing equivalent revocation information. Each of our CAs also operates an internal CA database serving as a private repository, wherein it publishes the Subscriber Certificates that it issues. Multiple CAs may share the same OCSP Responder.

Every Certificate issued by one of our CAs, excluding self-signed Root Certificates, contains URIs specifying the location of its Issuing CA's current CRL and its Issuing CA's Certificates within this public repository. If the Issuing CA also operates an OCSP Responder, the Certificate may also contain a URI specifying the location of this Responder. These URIs can be found in the corresponding Certificate extension fields, as detailed further in CP/CPS §§ 7.1.2.8 and 7.1.2.9. This requirement is enforced by use of defined certificate profiles for each CA.

We expect, but do not require, that Subscribers will publish their own public Certificates in a suitable manner such that these Certificates are discoverable using one or more of the methods recommended in the Direct Project Applicability Statement § 5. Each of our CAs may choose to publish Subscriber Certificates to one or more optional directory servers, but is not required to do so.

2.3 Time or frequency of publication

We will publish updates or other changes to the documents published in the public repository within 30 days of approval.

CRL issuance frequency and latency are detailed in §§ 4.9.7 and 4.9.8.

Each of our CAs will publish a new or re-keyed CA Certificate prior to issuing any Certificates signed with the respective private Key. We have policies and procedures in place (1) to publish the new or re-keyed CA Certificate on our public website before the corresponding CA is authorized to sign Certificates, (2) to publish Renewal CA Certificates on our public website prior to expiration of the CA Certificate that was renewed, but not prior to the time listed in the *notValidBefore* field of the renewal CA Certificate, and (3) to publish modified CA Certificates on our public website within 3 business days of issuance.

2.4 Access controls on repositories

The documents in our public document repository are available on our public Internet website for download by current and potential Subscribers, Relying Parties, and other parties with a legitimate reason to view these materials.

Repository materials are stored in read-only directories on our public web server with file access controls configured such that the materials may not be modified, except by authorized personnel who have properly authenticated themselves to the public web server system.

The CA Certificates and CRLs published by our CAs are available for download by Relying Parties at the URIs specified within the Certificates issued by each of our CAs. These URIs provide specific valid URLs on our public website that are accessible over the Internet by Relying Parties.

The corresponding materials are also stored in suitable read-only directories that may not be modified, except by authorized personnel who have properly authenticated themselves to the public web server system. Additionally, the CA software may be configured for automated authenticated publication of CA data to the web server over a secure TLS channel.

The public document repository and the public CA Certificate and CRL repositories are operated on servers separate from any CA or RA system used for approval or issuance of Certificates or CRLs, as required by our internal policies and procedures.

Any access or use of any public repository materials by a Subscriber or Relying Party shall be deemed acceptance of the terms of this CP/CPS and any applicable Subscriber Agreements and/or Relying Party Agreements. At our sole discretion, we may require any party to provide their legitimate reason for viewing these materials prior to releasing them, or we may terminate access to repository materials by any party who we determine is not acting in accordance with this CP/CPS, including, but not limited to, engaging in any activities which we deem may result in denial of service to legitimate users.

The private repository of Subscriber Certificates issued by each CA is accessible only by authorized and authenticated CA personnel. However, a subscriber may request a copy of their Certificate at any time through an authenticated TLS session on our Subscriber website. If we choose to operate an optional directory server as described in CP/CPS § 2.2, this will be made available to Relying Parties for queries, but the information in any directory record may only be modified by authorized personnel who have properly authenticated themselves to the directory server. Additionally, the CA software may be configured for automated authenticated publication of CA data to a directory server over a secure TLS channel.

3 Identification and Authentication

3.1 Naming

This section and its subsections describe the rules relating to acceptable names in Certificates we issue. The RA is responsible for enforcing these rules during the verification process, prior to submitting a completed application to the CA for approval.

3.1.1 Types of names

Our CAs will only issue Certificates that have non-null Distinguished Name (DN) name forms for the issuer and subject names. This is enforced through defined certificate profiles used by each CA. Additional requirements are listed below.

The subject alternative name extension in Direct Messaging Certificates issued by our CAs will be populated with either an *rfc822Name* entry matching the Direct Address in the Subscriber database for address-bound Certificates or a *dnsName* entry matching the Health Domain

Name in the Subscriber database for domain-bound Certificates, as detailed further in CP/CPS § 7.1.2.6.

Support for the following Subject Distinguished Name attributes in our Subscriber Certificates is implemented through defined certificate profiles and end entity profiles for each of our CAs:

Atrribute	**Abbreviation**	**Object Identifier (OID)**
commonName	CN	2.5.4.3
organizationName	O	2.5.4.10
organizationalUnitName	OU	2.5.4.11
streetAddress	STREET	2.5.4.9
localityName	L	2.5.4.7
stateOrProvinceName	ST	2.5.4.8
postalCode	ZIP	2.5.4.17
countryName	C	2.5.4.6
telephoneNumber	TEL	2.5.4.20

Support for the following UTF8String encoded *otherName* entry in the Subject Alternative Name extension in our Subscriber Certificates is also enabled in our CA Systems:

Atrribute	**Abbreviation**	**Object Identifier (OID)**
nationalProviderIndex	NPI	2.16.840.1.113883.4.6

CA Certificate Distinguished Names will contain CN, O, and C attributes. Additionally, we may optionally include an OU attribute. The CN value will be of the general form “<identifier> CA <#>” where <identifier> is a name relating to the purpose of the CA and <#> is an optional numeric value for use when more than one CA has the same identifier.

Distinguished Name attribute values may be abbreviated at the discretion of our RA, such as when the value would otherwise exceed length limits. The additional requirements of CP/CPS §§ 3.1.1.1-3.1.1.6 pertain only to Subscriber Certificates.

3.1.1.1 CN attribute

For Direct Messaging Certificates issued to organizations and all Direct Messaging Certificates requested with LOA-1 or IAL1 identity proofing, the CN attribute value shall be set to the Direct

Address associated with the Certificate for address-bound Certificates or to the Health Domain Name for domain-bound Certificates. For Direct Messaging Certificates issued to a natural person at LOA-2 or higher, the CN attribute value shall be set to either the Direct Address associated with the Certificate or the Applicant's name.

When a human Applicant's name is used, the CN attribute value shall be set to match the provider name field in the individual's NPI record (where applicable) or the government issued identification provided by the individual during identity-proofing. It is expected, but not required, that the CN attribute value match one of the following forms:

a. The full legal name of the Applicant, with or without any generational modifier preceded by an optional comma;
b. As in (a), but with one or more given names abbreviated to its first letter followed by a period, so long as at least one of the given names is not abbreviated (for example: J. Frances Smith or John W. Jones, III);
c. As in (a), but with one or more given names other than the first legal given name omitted or abbreviated to its first letter followed by a period (for example: Eric A. Jones or Eric Jones);
d. As in (a), (b), or (c), followed by the generally accepted acronym or abbreviation of one or more educational degrees or professional designations held by the Applicant, optionally with all periods (".") removed, optionally separated by commas (for example, John Doe, R.N., M.B.A. or Mary A. Wilson MD PhD FACP); or
e. As in (a), (b), (c), or (d), preceded by Mr., Ms., Mrs., or Dr., with the use of Dr. also requiring that Applicant hold at least one doctoral degree and also included in the CN field as per (d) (for example, Mr. Alfred Bux or Dr. Alex Smith, MD)

A person may request any of the forms (a)-(e) above so long as (1) all included substantive data is also present in one or both of the individual's NPI record (where applicable) or the Applicant's government issued identification, and (2) a generational modifier cannot be removed unless it is also absent in either the individual's NPI record (where applicable) or the Applicant's government issued identification. For example, an additional middle name or degree cannot be added unless it appears on one or both of the above.

3.1.1.2 O attribute

For all Subscriber Certificates, the O attribute shall list the verified name of the Sponsoring Organization or the Applicant organization, if any. An entity's fictitious business name (FBN) or other doing business as (DBA) name may be used when verified by our RA. For jurisdictions where registration of such names is not required, a fictitious business name claimed by the organization may be used together with the organization's verified name by indicating "dba" before such a name.

3.1.1.3 OU attribute

The OU attribute is optional and when used, shall list the name of a department or organizational unit of the organization listed in the O attribute. A Sponsoring Organization or Organizational Applicant may request an OU attribute value in Certificates issued to it or to individuals whom they are sponsoring, subject to verification and approval by our RA, in which case listing of the department or organizational unit on the application or other assertion by the organization as to the accuracy of the requested OU may be deemed sufficient verification by our RA.

3.1.1.4 STREET, L, ST, ZIP and C attributes

The STREET, L, ST, and ZIP attributes are optional. If requested by the Applicant, one or more of these attributes shall be set to values corresponding to an address verified and approved by our RA for the Applicant or Sponsoring Organization, if applicable. If STREET is used, then both L and ST will also be used. If L is used, then ST will also be used. ST will be set to the full name of the state, province, or other subdivision type as defined in ISO 3166-2. C will be set to the two-letter ISO 3166-1 country code of the verified address, e.g. “US” for addresses in the United States of America.

3.1.1.5 TEL attribute

The TEL attribute value is optional. When used, the TEL value shall be a verified voice or fax telephone number for the Applicant or Sponsoring Organization, if applicable. At most one voice and one fax number may be included in a Certificate. The Applicant shall identify each number as either a voice or fax number.

Telephone and Fax numbers shall be formatted according to ITU-T Recommendation E.123 Notation for national telephone numbers within the North American zone, with the following modifications: (a) an additional hyphen shall be inserted between the third and fourth digits of the local seven-digit part of the number, for example (212)345-6789 ext. 344, and (b) fax numbers shall be identified by adding the postfix (fax) preceded by a space.

3.1.1.6 NPI subject alternative name

An NPI value is optional and is permitted only for Applicants requesting Certificates identifying the Applicant or Sponsoring Organization as a Covered Entity as per CP/CPS § 3.2.2. When used, it shall be set to a numeric 10-digit National Provider Identifier associated with the Applicant or Sponsoring Organization. The RA will verify the NPI value by retrieving the corresponding record from the NPI Registry provided by the Centers for Medicare & Medicaid Services (CMS) and confirming that the data elements returned are consistent with the application. When more than one NPI number is associated with the Applicant or Sponsoring Organization, the RA shall determine which, if any, NPI values may be included in the Certificate.

The NPI shall be encoded in the Certificate as an *otherName* entry in the subject alternative names extension, as an OID:value pair, with the OID listed in CP/CPS § 3.1.1 and the NPI value encoded as a UTF8String.

3.1.2 Need for names to be meaningful

Subject names used in Certificates must identify the organization, individual, or Device to which they are assigned, must not be misleading, and must be easily understood by humans. The RA and CA Officers are responsible for verifying that these conditions are met prior to Certificate issuance.

In order to prevent potential confusion by Relying Parties evaluating a Certificate issued by us, Subject names shall not contain email addresses, Internet domain names, or string of digits resembling a phone number other than those corresponding to the Applicant's Direct Address or Health Domain Name, unless said email address or Internet domain name is an integral part of applicant's legal name or verified telephone or fax number. The RA representative is responsible for verifying that these conditions are met.

3.1.3 Anonymity or pseudonymity of subscribers

We do not issue anonymous Certificates. Our CAs may issue pseudonymous Certificates to internal Subscribers to support CA operations, or to other end entities, subject to the namespace uniqueness requirements of § 3.1.5.

3.1.4 Rules for interpreting various name forms

Name forms are interpreted according the rules specified in CP/CPS § 3.1.1.

3.1.5 Uniqueness of names

The proposed Subject DN listed by an Applicant must be unique within the X.500 namespace of our PKI. This means that the proposed Subject DN must be substantially different from all other DNs associated with other Participants in our PKI holding valid Certificates. This requirement is not violated when multiple Certificates with the same Subject DN are issued to the same Subscriber. Our CA Systems are configured to confirm that the requirements for unique Subject DN values for different end entities are met before allowing a Certificate to be issued.

Subject names within our PKI are issued on a "first come, first served" basis based on the time of final approval of an application. The Applicant will be informed if the proposed DN does not meet these requirements and will be provided an opportunity to change the proposed DN, so long as the new proposed name still meets all naming requirements. Should all Certificates for a single Participant bearing the same DN become invalid due to expiration or revocation, we may, in our sole discretion, continue to treat the associated DN as unavailable to different Applicants.

In the circumstance that an Applicant's proposed DN for a Direct Messaging Certificate is identical to that of a different Subscriber in our PKI, and no other changes to the DN attributes that are acceptable to the Applicant are permitted by this CP, the Applicant may append their Direct Address to the CN field within parentheses, in order to distinguish the Applicant's proposed DN from that of the existing Subscriber (for example, Applicant proposed CN "John Doe" would become "John Doe (jdoe@direct.example.com)", if this change would result in a DN meeting the naming requirements of this CP/CPS.

3.1.6 Recognition, authentication, and role of trademarks

Our Application forms require an Applicant to represent and warrant that they have not included trademarks in their proposed names unless the Applicant also possesses the rights to use the respective names. It is the sole obligation of the Applicant to verify that the names requested are not trademarked names in any jurisdiction in which their Certificates may be used or viewed. EMR Direct, in its sole discretion, shall resolve any name collisions or disputes brought to our attention. Such resolution may include revocation or modification of any Certificate that is part of a trademark dispute. See also CP/CPS § 9.9.1.

3.1.7 Subscriber Entity Type identifiers

The DirectTrust CP defines the following OIDs for entity types, which are defined in full in the DirectTrust CP §§ 1.2, 3.2.2, and 3.2.3.1, and may be expressed by our CAs in the certificate policies extension of Subscriber Certificates as per CP/CPS §§ 1.1.4 and 7.1.2.5:

Name	OID	Summary Use
DirectTrust CE	1.3.6.1.4.1.41179.2.1	Entity represents that it is a Covered Entity as defined by HIPAA at 45 CFR 160.103
DirectTrust BA	1.3.6.1.4.1.41179.2.2	Entity represents that it is a Business Associate as defined by HIPAA at 45 CFR 160.103
DirectTrust HE	1.3.6.1.4.1.41179.2.3	Entity represents that it is not covered by HIPAA, but provides equivalent protection to PHI

Name	OID	Summary Use
DirectTrust Patient	1.3.6.1.4.1.41179.2.4	Entity represents that the requested Certificate will be used for health information exchange purposes other than as a health care professional, Business Associate, or individual associated with a HIPAA Covered Entity.
DirectTrust Non-Declared	1.3.6.1.4.1.41179.2.5	Entity has not asserted that it will protect PHI with privacy and security protections equivalent to those required by HIPAA and has not asserted that it is a Patient as defined by DirectTrust CP.

All Applicant organizations and Sponsoring Organizations may classify themselves into one of the categories in the above table on their Application or other signed statement. Entities that do not classify themselves will be classified as “Non-Declared”.

For entities classifying themselves in the “CE”, “BA”, and “HE” categories, our RA shall verify that the signed Application or other signed statement or agreement includes the following representations, as applicable:

For the “CE” category: Applicant is a HIPAA Covered Entity. For the “BA” category: Applicant is a Business Associate under HIPAA. For the “HE” category: Applicant is not covered by HIPAA and handles Protected Health Information with privacy and security protections meeting or exceeding those required by HIPAA.

For the “Patient” category, our Subscriber Agreements require the Subscriber to represent that the Certificate will be used for their personal healthcare Direct message exchange purposes, or for healthcare Direct message exchange purposes on behalf of a patient for which they are a representative. When the Applicant for a Certificate bound to a Direct Address and asserting the “Patient” category is a patient representative, then the Direct Address requested by the representative shall correspond to the representative and not to the patient.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

For all private keys generated by our RA for Subscribers, no proof of private key possession by the Applicant is required as part of initial identity validation. For private keys generated by

Subscribers, the Subscriber must prove possession of the private key to our RA or CA. This can be done by (a) signing a known piece of data provided by the RA or CA and returning it to us for verification with the associated public key, or (b) submitting a PKCS #10 Certificate Signing Request to us through our Subscriber website in a secure and authenticated session containing a digital signature matching the public key in the CSR.

3.2.2 Authentication of organization identity

Organizations shall be authenticated for the following purposes: (1) The organization is an Applicant for a Certificate; and (2) The organization is sponsoring an Application by an individual or a Device for a Certificate. In both cases, the organization will be listed in any corresponding Certificates issued by us as per CP/CPS § 3.1.1.2.

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

Otherwise, the Applicant Organization's existence, name, and address shall be verified either (1) by matching to National Provider Identifier records provided by the US Department of Health and Human Services and associated with the Applicant, or (2) by matching to Federal, state, county, or other governmental records made freely available to the general public through the corresponding governmental agency's public website, or other publically available records or databases. An organizational mailing address may also be verified by confirming the ability of the Applicant or Applicant's organizational representative to receive mail at the address.

Our RA will confirm, based on the records in the previous paragraph, that the organizational Applicant or Sponsoring Organization exists as a legal entity. We may utilize the services of a third party to obtain or confirm any required information. We may also request additional supporting evidence from the organization or use data from multiple sources to assist in verifying this information or in resolving discrepancies, as we deem appropriate.

If the Certificate will assert an organizational affiliation between the Applicant and a Sponsoring Organization, our RA will obtain documentation from the Sponsoring Organization authorizing the affiliation and an agreement obligating the Sponsoring Organization to request modification or revocation of the Certificate, as applicable, if information in the Certificate subject identifying the Sponsoring Organization is no longer accurate or if the organizational affiliation ends.

3.2.3 Authentication of individual identity

3.2.3.1 Authentication of Human Subscribers

Validation of the identity of an individual is required for: (1) Individuals who are Applicants for a Certificate; (2) Individuals who are acting as an authorized representative of an Applicant; (3) the Security Officer who will be responsible for a Group Certificate, as defined in CP/CPS § 3.2.3.3; and (4) Individuals who are applying as the sponsor for a Device as described further in CP/CPS § 3.2.3.4. This requirement applies for all Subscriber entity types defined in CP/CPS § 3.1.7, including patients and patient representatives.

The DirectTrust CP defines the following OIDs for level of assurance with respect to identity proofing of human Subscribers, which are defined in the DirectTrust CP §§ 1.2 and 3.2.3.1 and may also be expressed by our CAs in in the certificate policies extension of Subscriber Certificates as per CP/CPS §§ 1.1.4 and 7.1.2.5:

Name	OID	Summary Use
DirectTrust ID LoA 1	1.3.6.1.4.1.41179.1.1	Level LoA 1 identity proofing
DirectTrust ID LoA 2	1.3.6.1.4.1.41179.1.2	Level LoA 2 identity proofing
DirectTrust ID LoA 3	1.3.6.1.4.1.41179.1.3	Level LoA 3 identity proofing
DirectTrust ID IAL1	1.3.6.1.4.1.41179.1.1	Level IAL1 identity proofing
DirectTrust ID IAL2	1.3.6.1.4.1.41179.1.5	Level IAL2 identity proofing

The identity proofing requirements described below are intended to be consistent with the requirements for the equivalent levels of assurance as defined in the DirectTrust CP. Specifically, the DirectTrust levels of assurance in the table above correspond to the phiCert LOA-1, LOA-2, LOA-3, IAL1, and IAL2 policies identified in CP/CPS § 1.2, respectively.

An individual's identity may be considered authenticated for the purposes of an Application if the same individual's identity has been previously authenticated in conjunction with another Certificate issued by us at the same or higher level of assurance, that Certificate is valid at the time of Application approval, the individual is still a subscriber to the previous Certificate, the information relating to the individual on the previous Application matches the information in the current Application, and the individual can demonstrate control of the corresponding

private key in a manner specified by our RA, such as by transmitting a Direct message signed with this key to us at a Direct Address specified by the RA.

Otherwise, the following authentication procedures shall be followed:

For an Applicant requesting a Certificate issued at LOA-1 or IAL1, the RA shall verify the Applicant's control over an email address by requiring the Applicant to demonstrate possession of an authentication code sent by the RA to the email address listed on the Application.

For LOA-2 and above, each Applicant shall supply his or her full legal name, an address of record, and date of birth on our Application materials. The Applicant will also specify (1) the desired level of assurance, and (2) whether they wish to be authenticated in person or remotely.

For in person proofing at LOA-2 or LOA-3, the Applicant completes an identity proofing form supplied by our RA. The Applicant then presents themselves in person to one of the following who may act as an "ID Verifier": an authorized RA representative, Trusted Agent, or Notary Public. The Applicant shall sign the identity proofing form in the presence of the ID Verifier. The ID Verifier will inspect the Applicant's valid government issued photo ID, compare the picture to the Applicant, record the ID number, and sign the identity proofing form. A Notary Public may alternatively provide their own signature on a Notary Acknowledgement suitable for this purpose in their jurisdiction.

For in person identity proofing at LOA-2, the CA shall either (a) send notice to an address of record after Certificate issuance; (b) issue credentials in a manner that confirms the Applicant's ability to receive mail at a claimed address; or (c) if personal information in records includes a telephone number or e-mail address, issue credentials in a manner that confirms the ability of the Applicant to receive telephone or fax communications or text messages at the telephone number or e-mail address associated with the Applicant in records. For (c), any secret sent over an unprotected session shall be reset upon first use.

For in person identity proofing at LOA-3, the RA or a Trusted Agent shall also verify the information provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases to confirm that the name, date of birth, address, and other personal information in records are consistent with the application. The CA shall either (a) send notice to a confirmed address of record after Certificate issuance; (b) issue credentials in a manner that confirms the Applicant's ability to receive mail at a claimed address; or (c) if personal information in records includes a telephone number, issue credentials in a manner that confirms the ability of the Applicant to receive telephone or fax communications at a number associated with the Applicant in records, while recording the Applicant's voice or using alternative means that establish an equivalent level of non-repudiation.

If the Applicant requests remote identity proofing at LOA-2, then he or she shall supply the ID number of a valid government issued ID and a utility or financial account identifier, along with

appropriate metadata sufficient to identify and verify the respective ID or account. The RA must inspect the two numbers supplied (e.g. for the correct number of digits, if known) and verify either the ID number or the account number information provided through records checks either with the applicable agency or institution or through credit bureaus or similar databases, to confirm that the name, date of birth, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. Confirmation of utility or financial account numbers may be performed by verifying knowledge of recent account activity, when applicable. The CA shall either (a) send notice to an address of record confirmed in the records check after Certificate issuance; (b) issue credentials in a manner that confirms the Applicant's ability to receive mail at a physical address; or (c) if personal information in records includes a telephone number or e-mail address, issue credentials in a manner that confirms the ability of the Applicant to receive telephone or fax communications or text messages at a telephone number or e-mail address associated with the Applicant in records. For (c) any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days.

If the Applicant requests remote identity proofing at LOA-3, then he or she shall supply the ID number of a valid government issued ID and a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID or account. The RA or a Trusted Agent must verify both the ID number and the account number provided through records checks either with the applicable agency or institution or through credit bureaus or similar databases, to confirm that the name, date of birth, address, and other personal information in records are consistent with the application. Confirmation of utility or financial account numbers may be performed by verifying knowledge of recent account activity, when applicable. Prior to Certificate issuance, the RA or a Trusted Agent shall either (a) confirm the ability of the Applicant to receive mail at a physical address associated with Applicant in records; or (b) if personal information in records includes both an electronic address and a physical address that are linked together with the Applicant's name, and are consistent with the information provided by the applicant, confirm the ability of the Applicant to receive messages (e.g. SMS, voice, fax, or e-mail) sent to the electronic address. For (b), any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days. The CA may send notice to an address of record confirmed in the records check after Certificate issuance.

If the Applicant requests identity proofing at IAL2, then he or she shall supply a valid government issued photo ID. If the supplied photo ID is not a United States passport, REAL ID, or Enhanced ID, then the Applicant shall also supply and the RA or a Trusted Agent shall validate two of the following: a telephone number, email address, his or her individual NPI number, or other identity evidence approved by our RA. The RA or a Trusted Agent shall (a) confirm a visual match between the applicant and the photo provided on the photo ID, (b) confirm that the supplied evidence appears to be genuine and unmodified, and (c) confirm that the personal details and evidence details are consistent with information held or published by

the issuing source or authoritative source(s). The RA shall confirm an address of record associated with the Applicant through (a) validation of an address contained on any supplied, valid piece of evidence, (b) validation of an address supplied by the applicant through authoritative source(s), or (c) confirmation of the ability of the Applicant to receive mail at a postal address. The RA or CA shall send a notification of proofing to a confirmed address of record. If remote proofing at IAL2 is requested, then prior to Certificate issuance, the RA or a Trusted Agent shall also confirm the ability of the Applicant to present a secret sent to a different confirmed address of record. This secret shall consist of at least six random alphanumeric characters or equivalent entropy and shall be valid for a maximum lifetime of 10 days if sent to a postal address, 24 hours if sent to an email address, or 10 minutes if sent to a telephone number.

The requirements listed above for a higher LOA can also be used to satisfy the authentication requirements of a lower LOA. LOA-1 and IAL1 are deemed equivalent LOAs. The ordering of LOAs from lowest to highest is as follows: LOA-1/IAL1, LOA-2, LOA-3, IAL2. All government-issued identification documents presented which bear an expiration date must be unexpired. The requirement for confirmation of a financial account or utility account number for remote identity proofing at LOA-2 or LOA-3 may be satisfied by a cellular or landline telephone service account when the phone is associated in records with the Applicant's name and an address of record and the applicant demonstrates that they are able to send or receive messages at the phone number.

The ID Verifier will record the required information on one of our approved identity verification forms. If this form is not completed at one of our RA offices, the form may be sent by US Mail or delivered by Courier to an RA address by the ID Verifier for processing in a tamper-evident mailer, or transmitted electronically to our RA via a secure channel approved by our RA. The ID Verifier may send several forms together in a single mailer. We utilize a third party service specializing in identity verification to perform required record checks through credit bureaus, public records, or similar databases. For individual healthcare providers, an individual NPI number may be used as the financial account.

In addition to the identity proofing methods described above, our RA or a Trusted Agent may verify an Applicant’s identity based upon evidence from one or more historical identity proofing events, such as events that occurred at the Applicant organization or Sponsoring Organization, when that evidence demonstrates that an equivalent identity proofing process to that outlined above for the LOA requested has been successfully performed. The organization may submit either (a) sufficient artifacts from the previous proofing events or (b) an attestation from a Trusted Agent at the organization that sufficient artifacts exist at the organization to meet the above requirements.

For phiCert Basic Assurance: Applicant must be authenticated following procedures in this section meeting the requirements for LOA-2, LOA-3, or IAL2.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

We do not offer role-based Certificates.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

A Group Certificate is a Certificate where more than one entity has access to use the corresponding private key. Examples are provided in CP/CPS § 1.3.5. Every Group Certificate must have a designated Security Officer. The Security Officer may be affiliated with a third party hosting the Certificate and act on behalf of the Subscriber. The Security Officer is designated by the Applicant on the Application.

The Security Officer is responsible for managing the private key corresponding to a Group Certificate on behalf of the Subscriber. For Direct Messaging Certificates, the Security Officer is also responsible for maintaining a list of any Users with access to or use of the private key, and accounting for which User had control of the key at a given time. A list of those holding the shared private key must be provided to, and retained by, the CA or the CA's designated representative. These lists may be updated through our Subscriber website in a secure authenticated session.

The value of the subject distinguished name of a Group Certificate must indicate the group nature of the Certificate and must not imply that the subject is a single individual. When necessary to meet this requirement, our RA may add "Group Cert", "HISP-Managed Cert", or other similar text to the proposed subject distinguished name.

For Direct Messaging Certificates that are also Group Certificates, each User as well as the Security Officer must be authenticated according to the requirements of CP/CPS § 3.2.3.1, at a level of assurance equal to or greater than the level of assurance asserted in the Group Certificate.

3.2.3.4 Authentication of Devices

Every Device must have a designated human sponsor who is responsible for carrying out Subscriber duties, including managing the Device's use of private keys. The human sponsor must be authenticated by our RA according to the requirements of CP/CPS § 3.2.3.1, at a level of assurance equal to or greater than the level of assurance sought for the Device. The human sponsor must provide identification of the Device (e.g. serial number or DNS name), the Device public key, any specific authorizations or attributes permitted by this CP to be included in the Certificate, and contact information. Our Subscriber Agreements for Devices require that, if the Device sponsor changes: (1) the new sponsor shall review the status of each Device to ensure that it is still authorized to use the issued Certificates, (2) the new sponsor is authenticated according to CP/CPS § 3.2.3.1, and (3) the new sponsor enters into a new Subscriber Agreement for the Device. If the above conditions are not met within 14 days of the change of sponsorship, the Device Certificate will be revoked.

A Device may be the sole Subscriber of a Certificate. A Device may also use a Group Certificate, such as when the keys corresponding to a Direct Messaging Certificate that is also a Group Certificate issued to a medical practice are used both by human Users for messages initiated by providers and by an electronic health record system for messages initiated by other triggering events.

3.2.4 Non-verified subscriber information

Only information verified by our RA or by a Trusted Agent will be included in our Certificates.

3.2.5 Validation of authority

An Applicant for a Certificate who is a natural person, or the authorized representative submitting an Application on behalf of an individual or organizational Applicant, must attest to his or her authority to submit the Application and to the accuracy and completeness of the contents of the Application. The Subscriber is responsible for any information provided by their agent to us and must promptly notify us of any misrepresentations or omissions made by their agent. The RA or a Trusted Agent will verify that a representative is authorized to act on behalf of and as an agent of the Applicant. Acceptable artifacts include a signed authorization submitted by the Applicant. For organizations, this authorization may be signed by an officer, owner, or other authorized official of the organization. We may use any means of communication at our disposal to ascertain the identity and authority of an organizational or individual Applicant or their representative.

3.2.6 Criteria for interoperation

Our Direct Messaging Certificates are intended to conform to the requirements specified in the Direct Project Applicability Statement. As such, when using suitable Direct Messaging software or services, participants in our PKI should be able to interoperate within our PKI and may be able to interoperate with participants in other similar PKIs. However, we make no warranty that any other participant does or will allow the use of any Certificate issued by our CAs, as this determination is made in the sole discretion of these other participants.

3.2.7 Right to use a Health Domain Name or Direct Address

An Applicant must have the right to use any email address or domain name listed on the Application for inclusion in a Certificate, unless the email address or domain name is assigned by us at a domain controlled by us. Our Subscriber Agreements shall require the Subscriber to warrant that the Subscriber has these rights. The RA will also verify that the domain name exists if this is not already known to the RA, and we may request that the Applicant demonstrate control of this domain using a method we specify. For Direct Messaging Certificates, we shall treat Direct Addresses and Health Domain Names in a case-insensitive manner when determining equivalence, i.e. two Direct Addresses that differ only in the capitalization of one or more of the component characters shall both represent the same Direct Address.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication for routine re-key

See CP/CPS § 4.7.3.

3.3.2 Identification and authentication for re-key after revocation

If a Subscriber's Certificate is revoked other than during a renewal or update action, the Subscriber must repeat the initial identity verification process described in CP/CPS § 3.2 to obtain a replacement Certificate.

3.4 Identification and Authentication for Revocation Requests

All Certificate revocation requests must be authenticated. Acceptable means of authentication include submission of the revocation request through our Subscriber website in a secure authenticated session or by demonstrating control of the corresponding private key. See also CP/CPS § 4.9.3.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

An individual or organization meeting the requirements of this CP/CPS may submit an application for a Certificate to our RA, together with any required supporting documents (collectively, "the Application"). Applications are reviewed by one of more of our RA staff.

4.1.2 Enrollment process and responsibilities

Our Registration Authority is responsible for establishing the enrollment process, under the management of the Director of Certification Practices, who is responsible for approving all elements of the enrollment process including any Application materials. Our RA will request the minimum personally identifiable information necessary to meet all applicable requirements for certificate issuance defined in this CP/CPS. Applicants may request an Application from our RA. We may make necessary applications or portions thereof available on our website as downloadable materials or as an online application form. Registration may be initiated by the Applicant through our Subscriber website through a secure TLS session or as a paper-based Application or facsimile thereof submitted to our RA. The Applicant must attest to the accuracy and completeness of information provided on our application materials as part of the Application process, and is required to submit any applicable application processing fees required prior to processing of the Application. Our RA is responsible for archiving Applicant data for audit purposes.

4.2 Certificate Application Processing

Once an application and any requisite application fees are received, our RA is responsible for verifying information on the Application according to the requirements of CP/CPS §§ 3.1 and 3.2.

We may use automated systems for authentication of Applicants or verification of information submitted by an Applicant where such use conforms to the authentication and verification requirements of this CP/CPS. This includes automated transmission of authentication codes by email, fax, telephone, or short messaging service (SMS) to verify control of an email address, fax number, mobile number or other telephone number, automated inspection or evaluation of submitted documents or identity artifacts, and automated printing or mailing of documents. We may also permit Applicants and Subscribers to accept certain agreements and make certain attestations electronically through our Subscriber website in a secured and authenticated session.

4.2.1 Performing identification and authentication functions

The identity verification of Applicants shall be performed by our RA as specified in CP/CPS § 3.2. During the identity verification, the Applicant is responsible for submitting any required supplementary documentation required by our RA. If any information is missing, incomplete, or cannot be verified, the Applicant or organizational representative will be notified either by email, postal mail, through our Subscriber website, or by telephone, fax, or other contact method provided by the Applicant. Once the verification process is completed by our RA, our RA will submit the completed Application and all verified information to one of our CAs.

4.2.2 Approval or rejection of certificate applications

A Certificate Application will be rejected by our CAs due to missing or inaccurate information, or if any of the information in the Application that would appear in the resulting Certificate is not consistent with the requirements of our CP/CPS. Each CA retains the right to reject a Certificate Application if, in the sole judgment of its CA Officer, the Applicant represents a risk to the professional reputation of the Company, or for any other reason determined by us, in our sole discretion. Once an application is approved, the Applicant must accept the Subscriber Agreement and pay any required issuance fees prior to Certificate issuance.

4.2.3 Time to process certificate applications

All Certificates will be issued within 30 days of the completion of the verification process by the RA. We have policies and procedures in place to enforce these requirements wherein the date and time that the verification step is successfully completed by the RA is reviewed by the assigned CA Officer before approving issuance of the corresponding Certificate. If 30 days has passed, the Certificate is not issued and the Application is returned to the RA to repeat the verification process.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

After an Application has been approved by the CA Officer, the verified Application information is entered into the CA Subscriber database by the CA Officer or the RA representative in a secured and authenticated session. Prior to electronically approving issuance of a Certificate, the CA Officer will verify that (a) the certificate request originated from the Applicant or the Applicant's authorized representative, (b) the information entered into the CA Subscriber database matches the verified Application information, and (c) all information needed to properly populate the fields and extensions that will be asserted in the Certificate has been entered. If the above conditions are not met, the RA is notified to correct and resubmit the Applicant information.

A CSR may be provided by the Subscriber or generated by us.

4.3.1.1 Actions when a CSR is generated by us

When a CSR is not supplied by the Subscriber, following electronic approval of Certificate issuance by the CA Officer, the RA Officer initiates generation of a new cryptographic key pair and a CSR by the CA system for the Subscriber. The CA software ensures that the newly generated public key is bound to the correct Subscriber and immediately generates the corresponding Certificate. The CA software then generates a password-protected secure digital file containing the newly issued Certificate and the encrypted private key which is delivered to the RA. The CA software archives the newly issued Certificate in the CA repository, but does not archive the temporary CSR or the private key. All interactions between the RA representative and the CA system in this paragraph occur in the setting of a secured and authenticated TLS session.

4.3.1.2 Additional CA actions when a CSR is provided by the Subscriber

Our CA software is configured such that only the public key component of a CSR supplied by a Subscriber is propagated into the Subscriber Certificate during Certificate generation. For CA Certificates, the requested Subject Key Identifier extension, if present, will also be retained. Any other information in the CSR, including any requested extensions, is ignored by the CA Software and is, therefore, not inspected or reviewed by the RA or CA. It is the sole responsibility of the Subscriber to provide the correct public key in the CSR. All other Subscriber information is taken from the CA Subscriber database, which contains only Subscriber information that has been verified by our RA. Our RA verifies that the CSR originated from the Subscriber by requiring the Subscriber to upload the CSR content through our Subscriber website in a secured and authenticated TLS session. If the CSR data is a valid CSR file, the CSR data is then uploaded to the CA system by the RA representative and associated with the Subscriber, to ensure correct binding between the included public key and the Subscriber who uploaded the CSR data. The CA software then generates the new Subscriber Certificate which is archived in the CA

repository and delivered to the RA representative as a public certificate file. All interactions between the RA representative and the CA system in this paragraph occur in the setting of a secured and authenticated TLS session.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Our RA will notify the Subscriber that a new Certificate has been issued via physical mail, email, or an equivalent means. The Subject information included in the Certificate is available for review by the Subscriber on our secure Subscriber website. The file containing the Certificate and, when applicable, the encrypted private key, may be downloaded in a secured and authenticated TLS session from this site by the Subscriber after acceptance of the Certificate contents. When applicable, the activation code to unlock the private key is mailed to the Subscriber by US mail.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

Upon Certificate issuance, the Applicant becomes a Subscriber. Following issuance of the Certificate, the Subscriber will have 7 business days to accept or reject the Certificate. Use by the Subscriber of any application using the issued Certificate or any private key generated by us shall be considered acceptance of the Certificate. If the Subscriber does not reject the Certificate within 7 days, the Certificate will be deemed to have been accepted by the Subscriber.

The Subscriber may reject the Certificate only if the Certificate contains fields which are incorrect or incomplete when compared with the information accepted by the Subscriber in CP/CPS § 4.3.2. Rejection of a Certificate must be done by the Applicant through our secure Subscriber website.

The above terms and requirements are included in our Subscriber Agreements.

Rejected Certificates will be revoked by the CA. We have policies and procedures in place so that the CA Officer is alerted when a Subscriber has rejected a Certificate and revokes the rejected Certificate.

4.4.2 Publication of the certificate by the CA

Subscribers shall publish their own Certificates for discovery as in CP/CPS § 2.2. The Issuing CA shall not be required to publish end-user Subscriber Certificates. If the Issuing CA operates an optional directory server as described in CP/CPS § 2.2, then the Issuing CA may generate a directory record with the Subscriber Certificate and corresponding Direct Address on this server. We may implement this through automated publishing of newly issued Certificates to a directory server by the CA software over a secured and authenticated channel. If the Issuing CA operates one or more OCSP Responders, then the status of the newly issued Certificate will be

published to those Responders immediately following issuance. The CA software will be configured to automatically publish the status information required by this paragraph to any OCSP Responders that are serving the corresponding CA over a secured and authenticated channel.

4.4.3 Notification of certificate issuance by the CA to other entities

The RA will be notified upon Certificate issuance. Our Issuing CAs are not required to notify any other entities upon the issuance of a Certificate. A cross-certified Issuing CA shall notify us upon issuance of a Subject CA Certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Subscribers shall protect their private key from access by unauthorized parties and use their private keys only as specified through certificate extensions, including the key usage, extended key usage, and certificate policies extensions, in the corresponding Certificate. These requirements flow down into our Subscriber Agreements.

4.5.2 Relying party public key and certificate usage

Relying Parties shall use public keys only for purposes for which the corresponding Certificate was intended, and not for a restricted or prohibited purpose. These requirements flow down into our Relying Party Agreements.

4.6 Certificate Renewal

Certificate renewal means the issuance of a new Certificate (the “Renewal Certificate”) to a Participant certifying the same public key as the original. Renewal Certificates will contain a new serial number, will generally contain a new validity period, and may contain new issuer-related attributes, but all attributes which identify the Participant will remain the same. The renewal Certificate may be issued by the same CA or a different CA in our PKI. Following renewal, the Subscriber may still use the Original Certificate, if the conditions of CP/CPS § 4.6.1 are met. The original Certificate may not be further renewed, re-keyed, or modified.

4.6.1 Circumstance for certificate renewal

Our Subscriber Agreements permit renewal of Subscriber Certificates only if all of the following conditions exist:

a. at the time of the request, the original Certificate has not expired and is not revoked,
b. the original Certificate has not been previously renewed, re-keyed, or modified,
c. the original private key has not been compromised,
d. the original private key has not reached the end of its usage period (see CP/CPS § 6.3.2),

e. the Subscriber remains in possession of the original private key,
f. the Subscriber name and attributes are unchanged, and,
g. the Subscriber's account with us is in good standing.

Notwithstanding the above, Original Certificates may be automatically renewed by the Issuing CA if circumstances arise where we deem it necessary to re-key the Issuing CA Certificate. If the Issuing CA Certificate is re-keyed, the Subscriber's Renewal Certificate will contain a new serial number and CA signature, but all other attributes, including the validity period, will be the same as those of the Original Certificate.

CA Certificates may be renewed if conditions (a)-(d) of this section are met as applied to the CA Certificate, the CA remains in possession of the original private key, and the CA name and attributes are unchanged.

4.6.2 Who may request renewal

A Subscriber Certificate may be renewed by request of the Subscriber, the Subscriber's authorized representative, or our Registration Authority. A Subscriber Certificate may also be renewed by the Issuing CA under the circumstances described in CP/CPS § 4.6.1. For Group Certificates, the Security Officer is the only Subscriber who may request renewal.

Our CAs may request renewal of their own Certificates.

4.6.3 Processing certificate renewal requests

A CA Officer will review each renewal request and approve it only upon successful re-authentication of the Subscriber to the CA Officer, and only after the CA Officer has verified conditions (a), (b), (d) and (g) of CP/CPS § 4.6.1 by reviewing the relevant records in the CA and billing department databases. The remaining conditions of CP/CPS § 4.6.1 shall be considered verified following attestation by the Subscriber that these conditions are met.

The Subscriber will re-authenticate to the CA Officer by submitting the renewal request either (1) in a secured and authenticated session or (2) as a Direct message to us at the Direct Address specified by the CA Officer during the renewal process. If a CSR cannot be submitted because the original private key is no longer available, then the Subscriber will not qualify for a renewal under CP/CPS § 4.6. In this circumstance, a new Application must be filed and initial identity verification must be repeated as per CP/CPS §§ 4.1 and 4.2.

Once the renewal request has been approved, the new Certificate will be issued as per CP/CPS § 4.3.1.2 using the CSR transmitted by the Subscriber.

4.6.4 Notification of renewal certificate issuance to subscriber

See CP/CPS § 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

See CP/CPS § 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

See CP/CPS § 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

See CP/CPS § 4.4.3.

4.7 Certificate Re-key

Certificate re-keying means that a Subscriber requests issuance of a new Certificate (the "Re-keyed Certificate") wherein the Issuing CA certifies a new public key. Either the Subscriber or the RA may generate the new key-pair. The Re-keyed Certificate will contain a new serial number and public key, but the Certificate attributes specific to the identity of the Participant will not be changed. The Re-keyed Certificate may be issued by the same CA or a different CA in our PKI that conforms to this CP/CPS. Following re-keying, the Participant may still use the old Certificate, provided it is not expired or revoked, and provided that the old private key has not been compromised and its valid usage period has not ended. The old Certificate may not be further renewed, re-keyed, or modified.

4.7.1 Circumstances for certificate re-key

Subscriber Certificates can be re-keyed only if:

a. conditions (a)-(c) and (e)-(g) for renewal in CP/CPS § 4.6.1 are met;
b. (i) the usage period of the associated key pair as defined in CP/CPS § 6.3.2 has expired or is nearing its expiration or (ii) re-keying has been requested by an authorized party listed in CP/CPS § 4.7.2; and
c. at least 30 days remain in the validity period of the original Certificate.

If less than 30 days remain in the validity period of the original Certificate, re-keying will still be allowed if it is requested in conjunction with Certificate renewal.

A Re-keyed Certificate will retain the validity period of the old Certificate, unless Certificate re-keying is requested in conjunction with a renewal. In the case of both re-keying and renewal of a Certificate, the validity period of the Re-keyed Certificate will be determined in the same manner as a routine renewal request as per CP/CPS § 4.6.

We will not re-key a Subscriber Certificate if it is revoked. Subscribers with revoked Certificates who would like to have their Certificates replaced will need to follow the procedures for new Certificate issuance.

CA Certificates can be re-keyed if conditions (a)-(c) of CP/CPS § 4.6.1 and (b) of this section are met.

4.7.2 Who may request certification of a new public key

A Subscriber Certificate may be re-keyed by request of the Subscriber or the Subscriber's authorized representative. For Group Certificates, the associated Security Officer may also request re-keying. Additionally, our Registration Authority and our CAs may initiate re-keying of a Subscriber Certificate without a corresponding request from the Subscriber or the Subscriber's authorized representative.

Our CAs may initiate re-keying of their own Certificates if circumstances arise where a CA deems this necessary, including, but not limited to, the circumstances listed in CP/CPS § 4.7.1 (b).

4.7.3 Processing certificate re-keying requests

In the case of re-keying due to private key compromise, our procedures for processing re-keying requests are the same as those for initial Certificate issuance. Specifically, a new Application and Subscriber Agreement must be completed and initial identity verification must be repeated.

In the case of re-keying for other reasons, a CA Officer will review each re-keying request and approve it only upon successful re-authentication of the Subscriber to the CA Officer, and only after the CA Officer has verified conditions (a), (b), and (g) of CP/CPS § 4.6.1 and conditions (b) and (c) CP/CPS § 4.7.1 by reviewing the relevant records in the CA and billing department databases. The remaining conditions in (a) of CP/CPS § 4.7.1 shall be considered verified following attestation by the Subscriber that these conditions are met.

The Subscriber will re-authenticate to the CA Officer by submitting the re-keying request either (1) in a secured and authenticated session or (2) as a Direct message to us at the Direct Address specified by the CA Officer during the re-keying process. If the Subscriber has generated the new key-pair, the Subscriber must also submit a CSR containing the new public key and signed with the new private key in the Direct Message or authenticated session above. Once the re-keying request has been approved by the CA Officer, the new re-keyed Certificate will be issued as per CP/CPS § 4.3.1.1 when we generate the new key-pair, or CP/CPS § 4.3.1.2 when the Subscriber generates the new key-pair and provides the CSR as specified above.

4.7.4 Notification of new certificate issuance to subscriber

See CP/CPS § 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See CP/CPS § 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See CP/CPS § 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other Entities

See CP/CPS § 4.4.3.

4.8 Certificate Modification

Certificate modification means that a new Certificate is issued because information about the Subscriber contained in the old Certificate has changed. The Modified Certificate will contain a new serial number and updated Subject information. The public key will remain the same, unless the old Certificate is also re-keyed at the time of modification. The Modified Certificate may be issued by the same CA or a different CA in our PKI that conforms to this CP/CPS.

Following modification, the old Certificate cannot be further renewed, re-keyed, or modified. Whether or not revocation of the old Certificate is required will be determined in accordance with CP/CPS § 4.9, but it will be automatically revoked within 30 days following issuance of the Modified Certificate if it has not expired and has not been revoked at that time.

4.8.1 Circumstances for certificate modification

Subscriber Certificates may be modified only if:

a. conditions (a)-(e) and (g) for renewal in CP/CPS § 4.6.1 are met,
b. one or more of the following is true:
    i. one or more Subject attributes listed in the Certificate has changed or is incorrect (for example, Subscriber name, Locality, Direct Address or Health Domain Name), or
    ii. one or more additional verified Subject attributes is to be added, or
    iii. one or more Subject attributes or other Certificate content is to be reformatted or changed in a non-substantive manner in order to promote interoperability; or
    iv. one or more Certificate Policy OIDs is to be added or removed, at the discretion of the CA; and
c. at least 30 days remains in the validity period of the Certificate.

If less than 30 days remains in the validity period of the Certificate, modification will still be allowed if it is requested in conjunction with Certificate renewal. If condition (d) of CP/CPS § 4.6.1 is not met or condition (b) of CP/CPS § 4.7.1 is met, modification will be allowed if it is requested in conjunction with Certificate re-keying. When modification in conjunction with re-keying would be allowed except for failure to meet condition (c) of this section, then modification will be allowed if it is requested in conjunction with both renewal and re-keying.

A Modified Certificate will retain the validity period of the old Certificate, unless Certificate renewal is requested in conjunction with the Modification. In the case of concurrent renewal of a Certificate, the validity period of the new Certificate will be determined in the same manner as a routine renewal request as per CP/CPS § 4.6.

CA Certificates can be modified provided conditions (a)-(d) of CP/CPS § 4.6.1 and (b) of this section are met.

4.8.2 Who may request certificate modification

A Subscriber Certificate may be modified by request of the Subscriber, the Subscriber's authorized representative, the issuing CA, or our Registration Authority. For Group Certificates, the associated Security Officer may also request modification. If the Certificate indicates an affiliation between the Subscriber and a Sponsoring Organization, an authorized representative of the Sponsoring Organization may request modification of the Subject attributes that relate to the Sponsoring organization if condition (b)(i) of CP/CPS § 4.8.1 applies.

Our CAs may request modification of their own Certificates.

4.8.3 Processing certificate modification requests

Prior to approval of issuance of the modified Certificate, the Applicant must submit an abbreviated Application pertaining only to those elements that have changed and attest that the remaining elements are unchanged. This abbreviated Application shall be submitted and processed in the same manner as for a new application as described in CP/CPS §§ 4.1 and 4.2. The RA representative will verify the modified Subject information in the same manner that those specific attributes are verified for a new Certificate. Once the information has been verified by the RA representative, the abbreviated Application will be submitted to the CA Officer for approval. Following approval of the abbreviated Application by the CA Officer, the RA representative will update the Subscriber information in the CA Subscriber database to reflect the verified modifications.

When the modification has been requested by the Subscriber, the Subscriber re-authentication and issuance of the modified Certificate shall occur in the same manner as specified in CP/CPS § 4.7.3 when modification is requested in conjunction with re-keying, or as specified in CP/CPS § 4.6.3 when modification is requested without re-keying.

We have policies and procedures in place to schedule revocation of the old Certificate within 30 days after issuance of the new modified Certificate.

4.8.4 Notification of new certificate issuance to subscriber

See CP/CPS § 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See CP/CPS § 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See CP/CPS § 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See CP/CPS § 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

Certificates that have not expired must be revoked if any of the following circumstances exists:

a. the identifying information or affiliation attributes of any names in the Certificate become invalid,
b. the private key associated with the Certificate has been compromised or is suspected of compromise,
c. the Subscriber has violated any of the terms of its Subscriber Agreement associated with the Certificate,
d. the Subscriber is no longer using the Certificate for an appropriate purpose as listed in CP/CPS § 1.4.1,
e. the Subscriber contracts with a third party to manage the Subscriber's private keys for a Group Certificate (e.g. a HISP) as per CP/CPS § 3.2.3.3, and that contract ends,
f. the Subscriber Agreement associated with the Certificate has expired without being renewed, or has been otherwise terminated,
g. an entity authorized to request revocation in CP/CPS § 4.9.2 asks for the Certificate to be revoked, or
h. any other circumstances exist that require revocation under our CP/CPS.

Our Subscriber Agreements require the Subscriber to notify us immediately if any of the circumstances in (a)-(e) exist. Certificates may also be revoked at the discretion of the CA, if such revocation is permitted under this CP/CPS.

4.9.2 Who can request revocation

Requests for revocation of a Certificate may be made by the EMR Direct Management, the Issuing CA, RA, the Subscriber, or the Subscriber's authorized representative. For Group Certificates, the associated Security Officer may also request revocation. If the Certificate indicates an affiliation between the Subscriber and a Sponsoring Organization, an authorized

representative of the Sponsoring Organization may request revocation if condition (b)(i) of CP/CPS § 4.8.1 applies with respect to affiliation attributes, such as when the affiliation ends.

Our CAs may request revocation of their own Certificates, as described further in CP/CPS § 5.7.3.

4.9.3 Procedure for revocation request

Any request for Certificate revocation, other than a request from the CA or Subscriber, shall identify the Certificate to be revoked by serial number and explain the reason for revocation. Subscriber requests for revocation must be made through our secure Subscriber website in a secured and authenticated session in order to ensure that the Certificate revocation request is not malicious. Revocation requests approved by an RA or CA will be submitted to the Issuing CA for processing.

Upon receiving a valid revocation request, the Issuing CA Officer will execute the revocation of the Certificate on the CA System in a secured and authenticated session, specifying the reason for revocation. The CA software is designed to automatically place the corresponding Certificate's serial number and any other required information on its certificate revocation list (CRL), which is updated automatically upon execution of a Certificate revocation. The revoked Certificate will remain on the Issuing CA's CRL until the Certificate expires, and will appear on at least one CRL. If the Issuing CA also operates an OCSP Responder, the Issuing CA software will also be configured to automatically update the Certificate status reflected in OCSP responses.

4.9.4 Revocation request grace period

There is no grace period for revocation under this policy. Our Subscriber Agreements require Subscribers to request the revocation of any Certificate issued to them as soon as the need for revocation comes to their attention.

We have policies and procedures in place requiring our CAs and RAs to request the revocation of a Certificate within our PKI as soon as the need for revocation comes to our attention.

4.9.5 Time within which CA must process the revocation request

We have policies and procedures in place to ensure that our CAs process all approved revocation requests promptly, but in no case more than 8 hours after receipt.

4.9.6 Revocation checking requirement for Relying Parties

Our Relying Party Agreements require Relying Parties to verify that each and every Certificate in a complete Certificate chain within our PKI is not revoked, prior to relying on an end-user Subscriber Certificate in that chain. This includes verifying that each and every Issuing CA Certificate in the chain is not revoked. Our RPAs also require Relying Parties to perform this verification by regularly downloading and appropriately processing the respective CRL or CRLs from our public repositories (see CP/CPS § 2.2.2), and, if no valid CRL is available, not to assume

that a Certificate is not revoked. Our RPAs require a Relying party to reject any Certificates that have been revoked or for which valid and current revocation information is not available. Our RPAs require the Relying Party to determine, in its sole discretion, how often they will re-check for updated revocation data if they employ caching of unexpired and valid CRLs.

4.9.7 CRL issuance frequency

For our Root CAs, the interval between issuance of CRLs shall be no more than 180 days and the time specified in the *nextUpdate* field of each CRL shall be no more than 180 days after the CRL is published. For our subordinate CAs, the interval between issuance of CRLs shall be no more than 31 days and the time specified in the *nextUpdate* field of each CRL shall be no more than 31 days after the CRL is published. Our CA system will automatically issue a new CRL before the time specified in the *nextUpdate* field of that CA's current CRL, even if no changes have occurred. We will also issue a new CRL within 24 hours if there is a change to the CRL. See § 4.9.12 for additional requirements.

Each updated CRL replaces the previous CRL issued by the same CA in the public repository, such that only the most recent CRL deposited by each CA is available in the public repository at any given time.

Additional requirements for phiCert Basic Assurance: For our CAs operating in an offline manner and only issuing CA Certificates, the interval between issuance of CRLs shall be no more than 31 days. For our other CAs issuing Certificates at Basic Assurance, the interval between issuance of CRLs shall be no more than 24 hours.

4.9.8 Maximum latency for CRLs

We will deposit an updated CRL into the repository within 4 hours of generation, and no later than the time specified in the *nextUpdate* field of the CRL that it replaces.

4.9.9 On-line revocation/status checking availability

See CP/CPS § 2.2.

4.9.10 On-line revocation checking requirements

Notwithstanding the requirements of CP/CPS § 4.9.6, if a Certificate lists an OCSP Responder and that Responder is operating and responding to status requests from a Relying Party at a time and in a manner which the Relying Party deems suitable for and consistent with the Relying Party's purposes, then our Relying Party Agreements permit a Relying Party to use a valid OCSP response to determine Certificate revocation status instead of downloading the respective CRL.

4.9.11 Other forms of revocation advertisements available

We do not offer other forms of revocation advertisement at this time.

4.9.12 Special requirements regarding key compromise

In the event of CA Certificate revocation due to the compromise or loss of a CA private key, an updated CRL will be published at the earliest feasible time. In the event of CA Certificate or Subscriber Certificate revocation due to private key compromise or suspected private key compromise, an updated CRL will be issued within 18 hours of receipt of notification by the issuing CA.

See CP/CPS § 5.7.3 for additional requirements regarding CA key compromise.

See CP/CPS § 9.6.3 for additional requirements regarding Subscriber key compromise.

4.9.13 Circumstances for suspension

We do not support suspension of Certificates.

4.9.14 Who can request suspension

We do not support suspension of Certificates.

4.9.15 Procedure for suspension request

We do not support suspension of Certificates.

4.9.16 Limits on suspension period

We do not support suspension of Certificates.

4.10 Certificate Status Services

We may choose to operate one or more OCSP Responders, as discussed in CP/CPS § 2.2.

4.10.1 Operational characteristics

We have no operational requirements for any OCSP Responders we may operate.

4.10.2 Service availability

We have no service availability requirements for any OCSP Responders we may operate.

4.10.3 Optional features

We have no requirements regarding optional features for any OCSP Responders we may operate.

4.11 End of Subscription

We have policies and procedures in place that should a Subscriber Agreement expire or otherwise terminate, a review of all associated Subscriber Certificates is triggered and all unexpired Certificates that were issued to that subscriber are revoked.

4.12 Key Escrow and Recovery

We do not offer key escrow or recovery services.

4.12.1 Key escrow and recovery policy and practices

We do not offer key escrow or recovery services.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Facilities, Management, Operational, and Physical Controls

The following subsections describe non-technical security controls, including physical, procedural, and personnel controls, used by our CAs to securely perform their required functions, including key generation, subject authentication, Certificate issuance, Certificate revocation, auditing, and archiving.

Our Subscriber agreements require Subscribers to maintain suitable Facilities, Management, Operational, and Physical Controls to protect their private keys, consistent with the security requirements imposed by HIPAA/HITECH. See also CP/CPS § 6.2 and its subsections. In addition to any other requirements of this CP/CPS, our Subscriber Agreements require Subscribers to treat all private keys issued to them with no less care and protection than that afforded to protected health information.

5.1 Physical Security Controls

5.1.1 Site location and construction

We use only SSAE-16 certified datacenters and co-location facilities to ensure that our CA and core RA hardware is located in a facility of location and construction appropriate for housing high value, sensitive information, and that the facility design provides robust protection against unauthorized access to CA and RA equipment and records.

5.1.2 Physical access

Our CA/RA equipment shall be protected from unauthorized access at all times, with access limited to authorized personnel, and security mechanisms commensurate with the level of threat in the equipment environment.

We may house our CA servers and cryptographic hardware modules at one or more co-location facilities. Co-location facilities are continuously staffed. Access beyond the reception area of the facility is limited to authorized personnel. Within the secure inner area, the CA equipment is further protected by a locked physical cabinet. Access to the cabinet is restricted to personnel authorized by the CA only.

Our RA core systems, including RA databases, may be operated on virtual machines hosted on hardware provided by our datacenters, with access to the physical equipment restricted to authorized datacenter personnel, or on equipment owned by us and protected in the same manner as the CA systems. Access to the running virtual machine instances is restricted to authorized EMR Direct personnel only. The offices housing the RA representative workstations are protected by inner and outer office doors, which are locked when the offices are not in use. The building housing these offices requires card access for after-hours entry to the lobby area.

5.1.3 Power and air conditioning

CA equipment power is supplied by one or more UPS-protected power feeds with backup on-site generators in case of power feed failure. Co-location facility cooling systems shall be sufficient to prevent overheating and maintain suitable humidity levels.

5.1.4 Water exposures

Our CA equipment is installed such that it is not in unreasonable danger of exposure to water, other than from fire prevention and protection systems.

5.1.5 Fire prevention and protection

Fire prevention and protection systems at our offices and co-location facilities shall be in compliance with applicable law.

5.1.6 Media storage

CA and RA media is stored in a suitable location as to protect it from accidental damage. Removable media containing audit, archive, or backup information is duplicated. One copy is stored in a separate location from the CA and RA equipment, and protected from unauthorized access.

5.1.7 Waste disposal

Sensitive media and documentation that are no longer needed for operations are destroyed in a secure manner. Paper documents that are no longer needed for operations are shredded.

5.1.8 Off-site backup

System backups, sufficient to recover from a system failure, are made on a regular and periodic schedule. At least one backup copy is stored at an off-site location that is separate from the CA/RA equipment and with physical and procedural controls commensurate to those required of the operational CA.

5.2 Procedural Controls

5.2.1 Trusted roles

The following four trusted CA roles are defined for this CP/CPS: Administrator, Officer, Auditor, and Operator.

5.2.1.1 Administrator

An Administrator is authorized to install, configure, and maintain the CA systems, establish and maintain CA system user accounts, configure certificate profiles and templates, configure audit parameters, and generate and backup CA keys. Administrators do not issue Certificates to Subscribers.

5.2.1.2 Officer

An Officer is authorized to request, approve, or execute the issuance, re-keying, revocation, renewal, or modification of Certificates. An Officer is also authorized to register new Subscribers, and to verify the identity of Subscribers and the accuracy of information included in Certificates.

5.2.1.3 Auditor

An Auditor is authorized to review, maintain, and archive audit logs, and to perform or oversee internal compliance audits to ensure that a CA is operating in accordance with this CP and the phiCert CP/CPS.

5.2.1.4 Operator

An Operator is authorized to perform system backup and recovery operations, including changing of any recording media, and is responsible for the routine operation of the CA equipment.

5.2.2 Number of persons required per task

One person is required to execute each task.

5.2.3 Identification and authentication for each role

A person serving in a trusted role must authenticate himself or herself to the CA system before being permitted to perform any actions set forth above for that role or identity. For general CA system administration operations, access is controlled by user account and password and IP address subnet, with access over a TLS connection. For CA functions, access is controlled by client certificate authentication and IP address subnet, with access over a TLS connection.

5.2.4 Roles requiring separation of duties

Individuals are specifically designated to the trusted roles defined above. Individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. The user profiles enforced by the CA system permit only those activities required by the roles designated to each user. No individual shall be assigned more than one identity.

5.3 Personnel Security Controls

5.3.1 Qualifications, experience, and clearance requirements

All Company personnel must be legally eligible to work in the United States. Completion of an I-9 form is required for all employees. Persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, as determined by management.

5.3.2 Background check procedures

We will perform a background investigation in connection with hiring of new personnel to fill trusted CA roles, covering at least the last five years in the areas of employment, education, and law enforcement, and at least the last three years for place of residence. Regardless of the date of the award, the highest educational degree will be verified. Personal references are also checked by our human resources staff or by the hiring manager prior to hiring of personnel to fill trusted CA roles.

5.3.3 Training requirements

Before serving in a trusted role, a person will receive comprehensive training in all aspects of the role they will perform, and, if necessary, training in the principles and operations of our PKI. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.4 Retraining frequency and requirements

Individuals serving in trusted roles will be kept aware of changes to CA operations relevant to their roles. We will implement training/awareness plans for significant changes to CA operations, such as upgrades to CA hardware, software or security systems, and document the execution of such plans. Documentation shall be maintained identifying all personnel who received retraining and the level of training completed.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

We will take appropriate administrative and disciplinary action against personnel who violate the provisions of this CP/CPS, whether through negligence or malicious intent. Administrative and disciplinary actions may include suspension, dismissal, and removal from a trusted role.

5.3.7 Independent contractor requirements

Any independent contractor assigned to perform trusted CA roles shall meet the same personnel requirements and be subject to the same sanctions as set forth in this CP/CPS §§ 5.3.1-5.3.6.

5.3.8 Documentation supplied to personnel

We will provide documentation necessary to perform the duties and procedures required of each role to personnel filling that role.

5.4 Audit Logging Procedures

Our CAs shall generate audit logs for all events relating to the security of the CA according the rules specified in the following subsections. Our CA systems are configured such that all security auditing capabilities of the CA operating system and CA software required by this CP/CPS are enabled, and the CA systems are configured to automatically collect audit log data. We implement supplementary manual procedures to ensure that any audit data that cannot be automatically collected by the CA system is recorded manually in a log book. All audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

5.4.1 Types of events recorded

Every event record includes the date, time, the type of event, success or failure (where appropriate), and the identity of the operator and/or entity that caused the event. The following event types are recorded:

Security audits:

- Any change to the audit parameters (such as audit frequency or type of event audited);
- Any attempt to delete or modify the audit logs;
- Obtaining a third-party time-stamp.

Identification and authentication: - Successful and unsuccessful attempts to assume a role; - Any change in maximum allowed authentication attempts; - Unsuccessful authentication attempts exceeding the maximum allowed during user login; - Unlocking by an Administrator of an account that has been locked due to too many unsuccessful authentication attempts; - Any change in the type of authenticator, e.g. from password to biometrics.
Local or Remote Data Entry: - All security-relevant data that is entered in the system.
Data export and output: - All successful and unsuccessful requests for confidential and security-relevant information.
Key Generation: - Whenever the CA generates a key (excluding single session or one-time use symmetric keys).
Private Key Load and Storage: - Loading of component private keys; - All access to Certificate subject private keys retained within the CA for key recovery purposes.
Trusted Public key entry, deletion, storage: - All changes to the trusted public keys, including additions and deletions.
Private and Secret key export: - Export of private and secret keys (excluding keys used for a single session or message).
Certificates: - All Certificate requests; - All Certificate revocation requests; - Approval or rejection of a Certificate status change request.
CA configuration: - Any security-relevant changes to the CA configuration.

Account administration: - Addition or deletion of a role and/or user; - Modification of access control privileges of a user account or a role.
Profile Management: - All changes to a certificate profile, revocation profile, or certificate revocation list profile.
Miscellaneous: - Appointment of individual to a trusted role; - Installation of the OS; - Installation of the CA software; - Destruction of a hardware cryptographic module; - System startup; - Logon attempts to CA applications; - Attempts to set or modify passwords; - Backing up or restoring CA internal database; - All Certificate compromise notification requests; - Zeroizing of tokens; - Re-keying of the CA; - Configuration changes to the CA server hardware, software, operating system, including patches.
Physical Access: - Any known or suspected violation of physical security.
Anomalies: - Software error conditions; - Software integrity check failures; - Network attacks (suspected or confirmed); - Equipment failure; - Violations of this CP/CPS; - Resetting operating system clock.

5.4.2 Frequency of processing log

Audit logs are reviewed for cause, such as following any alarm or anomalous event. The Auditor briefly inspects all log entries, and more thoroughly investigates any alerts or irregularities in

the log, such as discontinuities or loss of audit data. Any action taken as a result of these reviews is documented.

5.4.3 Retention period for audit log

Security audit log data shall be retained on the CA equipment for a minimum of two months. See CP/CPS § 5.5.2 for long-term retention requirements.

5.4.4 Protection of audit log

The CA system is configured and procedures are in place to ensure that only persons assigned to trusted roles have read access to audit logs, and only authorized personnel may archive the logs. Original audit logs are not modified. Original audit logs may be deleted from the CA system by a CA Administrator as part of rotating the audit file, but only after successful archival has been confirmed by a CA Administrator.

5.4.5 Audit log backup procedures

Audit log files are backed up at least monthly. A copy of the audit log back-up is stored in a safe, secure location separate from the location where the data was generated.

5.4.6 Audit collection system (internal vs. external)

The audit logging system is internal to each CA system. The CA system is configured such that the security audit processes are invoked at startup of the CA software and cease only after shutdown of the software. Should it become apparent that an automated security audit system has failed, we shall cease all CA operations except for revocation processing until the security audit capability can be restored.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

The Auditor reviewing the audit logs shall notify a CA Officer of any irregularities or evidence of attempts to breach system security. The CA Officer shall ensure that these findings are handled properly to identify and address any associated security vulnerabilities. We also undertake automated quarterly vulnerability scans of CA systems.

5.5 Records Archival

5.5.1 Types of records archived

The following types of records shall be archived in sufficient detail as to verify that the CA was properly operated as well as to verify the validity of any Certificate throughout its validity period:

1. Any accreditation of the Issuer CA,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA,
4. System and equipment configurations, modifications, and updates,
5. Certificate and revocation requests,
6. Identity authentication data,
7. Any documentation related to the receipt or acceptance of a Certificate or token,
8. Subscriber Agreements,
9. Issued Certificates,
10. A record of Certificate re-keys,
11. CRLs,
12. Any data or applications necessary to verify an archive's contents,
13. Compliance auditor reports,
14. Any changes to the Issuer CA's audit parameters,
15. Any attempt to delete or modify audit logs,
16. Key generation (excluding session keys),
17. Access to Private Keys for key recovery purposes,
18. Changes to trusted Public Keys,
19. Export of Private Keys,
20. Approval or rejection of a Certificate status change request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security,
25. Violations of the CP or CPS, and
26. All audit logs generated in accordance with CP/CPS § 5.4.

5.5.2 Retention period for archive

CA archives are retained for a minimum of seven years and six months. The retention term for Certificates begins on the date of Certificate expiration or revocation, whichever is earlier.

5.5.3 Protection of archive

Only authorized individuals are permitted to add to or delete from the archive.

5.5.4 Archive backup procedures

A backup of all archive media is stored in a separate, safe, secure storage facility.

5.5.5 Requirements for time-stamping of records

CA system time is regularly updated using the Network Time Protocol to synchronize system clocks. Automatically generated CA archive records are automatically time-stamped as they are

created. The “valid from” field of a Certificate serves as the time-stamp of its issuance. The “revocation date” field on a CRL servers as the time-stamp of Certificate revocation. Other archive records may be manually date-stamped, as applicable.

5.5.6 Archive collection system (internal or external)

No stipulation beyond the provisions specified in CP/CPS § 5.4.6.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key Changeover

To minimize risk to the PKI through compromise of a CA’s key, new Root CA Certificates with new private signing key will be phased in for use every 15 years. Only the new CA keys will be used for Certificate signing purposes from that time. The older, but still valid, CA Certificates will remain available to verify old signatures until all of the CA and/or Subscriber Certificates signed under it have also expired. The old private keys will be retained and protected, as they will still be used to sign CRLs that contain Certificates that were originally signed with those keys.

5.7 Compromise and Disaster Recovery

This section describes procedures relating to notification and recovery in the event of compromise or disaster affecting the CA.

5.7.1 Incident and compromise handling procedures

If we become aware of a hacking attempt or other form of potential compromise of one of our CAs, it shall be promptly investigated in order to determine the nature and the degree of any damage sustained. We will assess the scope of potential damage in order to determine if the CA needs to be rebuilt, if any or all associated Certificates need to be revoked, and/or if the CA key needs to be declared compromised. If the CA key is suspected of compromise, the procedures outlined in CP/CPS § 5.7.3 shall be followed.

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

We backup copies of CA systems, including duplicate hardware modules, databases, and CA private keys in order to rebuild the CA capability in case of hardware failure or corruption of software and/or data. At least one copy is stored securely in a location separate from the CA system, in an encrypted manner. During restoration of corrupted CA systems, priority shall be given to the generation of Certificate status information if the CA signing keys have not been destroyed, or to the generation of a new CA key pair if the CA signing keys have been destroyed.

5.7.3 Entity private key compromise procedures

If a Root CA key is compromised or is reasonably suspected by us of being compromised, we will notify by automated email all Subscribers with Certificates with a CA Chain containing that Root CA at their contact addresses on file. This notification will include notice of the compromise or suspected compromise of the Root CA Certificate, notice that the corresponding self-signed Certificate must be removed from any Relying Party application, and the location of a new Root Certificate that shall be distributed as specified in CP/CPS § 6.1.4. Additionally, all affected valid Subscriber Certificates that are not revoked or expired will be renewed by an unaffected Subordinate CA and the original Subscriber Certificates revoked.

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

5.7.4 Business continuity capabilities after a disaster

In the case of a disaster in which the CA equipment is damaged and inoperative, we will reestablish CA operations as quickly as possible at a suitable location in accordance with our Company disaster recovery plan, where we will rebuild the CA equipment and CA system from a secure backup.

If all copies of a CA signature key are destroyed, the CA shall generate a new CA key pair and request revocation of any unexpired Certificates previously issued to it (other than self-signed Certificates), and, if applicable, request recertification of its new public key. If the CA is a Root CA, a new self-signed Certificate will be generated and distributed as specified in CP/CPS § 6.1.4. For any CA requiring new keys, all unexpired CA and end entity Certificates previously issued by that CA will then be reissued. In such events, Relying Parties shall decide of their own volition and at their own risk whether to continue to use Certificates signed with a destroyed private key pending reestablishment of CA operations with new Certificates.

5.8 CA or RA Termination

In the event of termination of one or more of our CAs, all unexpired and unrevoked Certificates signed by the respective CAs will be revoked. EMR Direct or its successors will make reasonable arrangements to retain the archival records of any terminated CA or RA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

All key pairs used in our PKI shall be RSA keys.

6.1.1.1 CA Key Pair Generation

Each of our CAs will generate its own cryptographic key pair to sign Certificates, CRLs, and status information in accordance with the requirements of CP/CPS § 6 and subsections. These keys shall be generated on a hardware cryptographic module that is well protected and suitable for this purpose, according to our formalized and auditable key generation ceremony procedure, by personnel in trusted roles. Should any failures or anomalies be encountered during the key generation process, we will document these failures or anomalies along with any corrective action taken prior to continuing with the key generation process.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pairs shall be generated using a hardware or software cryptographic module that is suitable for this purpose, operating on physical hardware that is well protected. The RA shall be treated as a Subscriber for the purposes of this section.

6.1.2 Private key delivery to subscriber

When Subscriber keys are generated by the Subscriber, no delivery of the private key to the Subscriber is required.

When Subscriber keys are generated by our CA or RA, the Subscriber's private key will be delivered to the Subscriber through our secure Subscriber website. To ensure that the correct private key is delivered securely to the correct Subscriber, the Subscriber downloads the private key in a secured and authenticated TLS-protected online session. The download of the private key in this manner serves as an acknowledgement of receipt of the private key by the Subscriber. Following download by the Subscriber, we will destroy our copy of the Subscriber private key. We do not retain any copy of the Subscriber private key after delivery of the private key to the Subscriber.

To protect the private key from compromise or modification during the delivery process, the private key is encrypted using a cryptographic algorithm and key size at least as strong as the private key itself. To protect the private key from activation during the delivery process and ensure delivery of the activation data to the correct Subscriber, the corresponding activation data will be transmitted to the Subscriber using a separate secure channel selected from the delivery methods in our Subscriber records, including but not limited to telephone, US mail, courier, SMS, and fax.

6.1.3 Public key delivery to certificate issuer

For keys generated by the CA system, no delivery of the public key to the certificate issuer is required. As per CP/CPS § 4.3.1.1, this applies to all Subscriber keys that are not generated by the Subscriber.

For keys generated by the Subscriber, the Subscriber public key shall be delivered electronically to the certificate issuer in the form of a Certificate Signing Request (CSR). As per CP/CPS § 4.3.1.2, the Subscriber's verified identity is bound to the public key by requiring the Subscriber to upload the CSR content to our Subscriber website in a secured and authenticated TLS-protected session. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys that will be used to sign the Subscriber's certificate.

6.1.4 CA public key delivery to relying parties

Each of our CAs' public keys is available within its respective CA Certificate. Each CA Certificate is available online at a location specified in each Sub-CA or Subscriber Certificate issued by that CA, as detailed further in CP/CPS §§ 7.1.2.9 and 7.2.2.

Our Root CA Certificate(s) are also available on our public website for download. Our Root CA Certificate(s) may also be made available in one or more bundles of Certificates intended as a collection of trusted anchors, distributed by us or by others, alone or together with other Certificates issued by us or by others. We may not be aware of all such existing bundles.

To assist Relying Parties in determining the authenticity of one of our Root CA Certificates they may obtain through the above or other methods, certificate identifiers based on a cryptographic hash of each Root CA Certificate are also listed on our website. For Relying Parties who determine that their use of our Root CA Certificate(s) requires a higher level of assurance, our Root CA Certificate(s) and/or hash values may also be delivered, upon request, to a Relying Party using a commercially reasonable out-of-band medium trusted by the Relying Party. We may charge a fee for such delivery.

6.1.5 Key sizes

RSA public keys shall be at least 2,048 bits in size if the corresponding Certificate expires before 1/1/2031, and at least 3,072 bits in size if the corresponding Certificate expires after 12/31/2030.

For elliptical curve algorithms, public keys for CA Certificates shall be at least 384 bits in size, public keys for end entity Certificates shall be at least 224 bits in size if the corresponding Certificate expires before 1/1/2031, and at least 256 bit size if the corresponding Certificate expires after 12/31/2030.

CAs shall use the SHA-256, SHA-384, or SHA-512 hash algorithm when digitally signing Certificates or CRLs. Use of TLS or similar security protocol to accomplish the requirements of the CP/CPS shall require at a minimum AES-128 or equivalent for symmetric keys, 2,048 bit RSA

or equivalent for asymmetric keys before 1/1/2031, and 3,072 bit RSA or equivalent for asymmetric keys after 12/31/2030.

6.1.6 Public key parameters generation and quality checking

CA public key parameters are generated in accordance with FIPS Publication 186. A public RSA exponent of 65537 shall be used.

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

Certificates issued by our CAs shall assert key usage purposes based on the intended application of the key pair, as discussed further in CP/CPS §§ 7.1.2.3, 7.1.2.4, and 7.1.2.7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Cryptographic modules should be minimally validated to the FIPS 140 level identified below for the relevant party (or provide an equivalent protection):

CA	Level 2
RA	Level 1
HISP	Level 2
Subscriber	Level 1

Our CAs and our RA use cryptographic modules meeting the above requirements. The HISP requirement applies to HISPs accredited under the HISP Accreditation Program administered by DirectTrust.

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

See CP/CPS § 5.2.2.

6.2.3 Private key escrow

We do not escrow private keys. Our Subscriber Agreements require Subscribers to agree that private keys corresponding to a Subscriber Certificate that asserts the digitalSignature key usage bit will not be escrowed.

6.2.4 Private key backup

The purpose of private key backup is to allow the user of a key to reconstitute said key in case of destruction or corruption for business continuity purposes. Only CA Administrators may backup our CA keys and only in an encrypted form to a system under our control. All backup copies are accounted for and protected. At least one backup copy of each CA private signature key is stored in a separate location. Access to the backup is restricted to CA Administrators.

Our Subscriber Agreements require Subscribers to back up their own private keys to a secure offsite location in a manner and form of their choosing, as long as all copies are held in the Subscriber's control and never stored in plain text form outside of the Subscriber's cryptographic module. We do not provide private key backup services to Subscribers.

6.2.5 Private key archival

The purpose of private key archival is to provide for reuse of the private key in the future, e.g., use to decrypt an archived document. We do not provide private key archival services to our Subscribers. We do not archive CA private signature keys.

Although we expect that Subscribers will chose to archive their private encryption keys for the purposes of decrypting archived data that was encrypted with the corresponding public key, we make no stipulation in our Subscriber agreements regarding any requirement to do so. Each Subscriber is solely responsible for determining if private key archival is appropriate for their specific circumstances, and, if required, choosing the manner, form, and location in which their keys are archived, subject to the same security requirements for private key backup described in CP/CPS § 6.2.4.

For Subscriber keys that are dual-use (encryption and signature) keys, should a Subscriber's circumstances require archival of private keys, our Subscriber Agreements require that Subscribers agree that they will cease all use of any private key that corresponds to a revoked or re-keyed Certificate, or to a Certificate that expired without being renewed, except for the sole purpose of decrypting materials that were previously encrypted with the associated public key.

6.2.6 Private key transfer into or from a cryptographic module

Private keys shall not exist at any time in plaintext form outside of a cryptographic module.

Transfer of keys into or from the cryptographic modules of our CA systems is restricted to CA Administrators. CA private signature keys shall only be exported for purposes of key backup as described in CP/CPS § 6.2.4.

We have no other requirements regarding Subscriber procedures for private key transfer into or from their cryptographic modules beyond the general requirement to protect their private key specified in CP/CPS § 5.

6.2.7 Private key storage on cryptographic module

CA private keys are stored on a cryptographic module according to the manufacturer's instructions.

6.2.8 Method of activating private key

Authorized CA Officers and CA Administrators may activate or use our CA private keys only after authenticating themselves to one of our CA systems. We have no requirements regarding Subscriber procedures for Subscriber private key activation beyond the general requirement to protect their private key specified in CP/CPS § 5.

6.2.9 Method of deactivating private key

Private keys stored on CA HSM devices are (1) deactivated by authorized personnel via a deactivation procedure on the CA system when not needed for CA functions or automated CRL generation, and (2) automatically deactivated on shutdown of the CA system or HSM device.

6.2.10 Method of destroying private key

We destroy our private signing keys when they are no longer needed using suitable methods. Keys stored on hardware security modules are erased according to the manufacturer's instructions. HSM devices will be zeroized prior to removal from service according to the manufacturer's instructions.

Our Subscriber Agreements require Subscribers to destroy their private keys, using any suitable method, when they are no longer needed or when the operational period for key pair usage as defined in CP/CPS § 6.3.2 has ended, unless the Subscriber archives the private keys as discussed in CP/CPS § 6.2.5.

6.2.11 Cryptographic Module Rating

See CP/CPS § 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Public keys are archived as part of the Certificate archival process in accordance with CP/CPS § 5.5.

6.3.2 Certificate operational periods and key pair usage periods

Root CA Certificates shall have a validity period of 20 years. Subordinate CA Certificates shall have a validity period of no more than 15 years. Subscriber Certificates shall have a validity period of no more than 3 years. Our CAs shall not issue Subscriber Certificates or Subordinate CA Certificates with an expiration date after the expiration date of the respective CA Certificate.

CA Root private keys will be used for a maximum of 20 years following generation. Subordinate CA private keys will be used for a maximum of 15 years following generation. Our Subscriber Agreements will require Subscribers to cease use of any particular private signing key after a maximum of 6 years following its generation.

Additional requirements for phiCert Basic Assurance: Subordinate CA Certificates shall have a validity period of no more than 10 years. Subordinate CA private keys will be used for a maximum of 10 years following generation to sign CRLs or OCSP responder Certificates, and for a maximum of 6 years to sign all other Certificates. Our Subscriber Agreements will require Subscribers to cease use of any particular private key after a maximum of 3 years following its generation.

See also CP/CPS § 5.6 regarding private key changeover.

6.4 Activation Data

6.4.1 Activation data generation and installation

The activation data used to unlock CA, RA, or Subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. When the activation data for Subscriber keys is transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic key. When one of our CAs uses a password as activation data for the CA signing key, at a minimum the password shall be changed upon CA re-key.

6.4.2 Activation data protection

CA personnel are instructed not to write down or share activation data used to unlock CA private keys. Activation data shall be memorized and/or recorded and securely stored, and shall not be stored with the cryptographic module.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

Our CA systems provide the following computer security functions, either as a function of the respective operating system, or through a combination of the operating system, software, and/or physical safeguards: authenticated logins, security audit controls, and access control to authorized individuals.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System development controls

The software systems for our CAs are developed and maintained in a controlled development environment, with modern source code control. CA hardware and software are dedicated to performing only CA functions. All hardware or software updates are tested, documented, and approved before implementation. Updates are installed in a professional and controlled manner. Proper care is taken to prevent malicious software from being loaded onto the CA and RA Equipment. Periodic scanning for malicious software is performed. We may use virtualized hardware at our discretion, provided that the virtual hardware conforms to the requirements of this CP/CPS.

6.6.2 Security management controls

Configuration, modifications, and upgrades of the security-related features of our CA systems are documented and controlled. Only authorized Administrators may configure, modify, or upgrade CA systems. All access for these purposes is logged.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network Security Controls

All networked information transfer to or from one of our CAs is performed through secure networks. Firewall devices are configured such that no access to CA systems is allowed except through these secure networks. RA Workstations used to access our CA systems are restricted to these secure networks. All changes to firewall configurations are documented.

We employ appropriate security measures to ensure that our CA systems are guarded against intrusion attacks. Unused network ports and services on our CA equipment are disabled.

6.8 Time-stamping

All system clocks for our CA systems shall be synchronized by use of a trusted time service. Our systems are configured to synchronize at each start-up and again at regular intervals. Asserted times are accurate to within three minutes.

7 Certificate, CRL, and OCSP Profile

7.1 Certificate Profile

Certificates issued by our CAs conform to the X.509 v3 certificate profile detailed in the document entitled Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May, 2008, issued by the Internet Engineering Task

Force, hereafter referred to as “RFC 5280”. These requirements and those of the following subsections are enforced by use of defined certificate profiles in our CA Software.

7.1.1 Version number(s)

Our CAs issue X.509 Version 3 (“X.509 v3”) Certificates.

7.1.2 Certificate extensions

All Certificates issued by our CAs must contain values for all of the Certificate Extensions listed in this section, unless otherwise specified. We may also include other valid certificate extensions conforming to RFC 5280. All extensions are marked with criticality of false, unless otherwise specified. The meaning and purpose of these extensions is detailed in RFC 5280.

7.1.2.1 Authority key identifier

This extension is set for all Subscriber and CA Certificates, except for self-signed Root Certificates. The value is set to the same value as the subject key identifier listed in the Certificate of the Issuing CA. For Root Certificates, this extension is optional but when used, by definition, shall be the same as the subject key identifier.

7.1.2.2 Subject key identifier

This extension is used to identify the specific public key contained in a Certificate. For CA Certificates, the value will be taken from the CSR supplied by the Subject CA, if provided. In all other cases, the value will be computed as the 160-bit hash of the public key, as per the method described in RFC 5280 § 4.2.1.2.

7.1.2.3 Basic constraints

This extension is marked as CRITICAL in all Certificates issued by our CAs. For end entity Subscriber Certificates, this extension is set to false. For our CA Certificates, this extension is set to true.

7.1.2.4 Key usage

This extension is marked CRITICAL in all Certificates issued by our CAs. The following key usage bits as defined in RFC 5280 shall be asserted for end entity Subscriber Certificates used for both signing and encryption (dual-use Certificates): digitalSignature and keyEncipherment. If separate signing and encryption Certificates are issued to a Subscriber, the signing Certificate shall assert only the digitalSignature bit and the encryption Certificate shall assert only the keyEncipherment bit. The following key usage bits shall be asserted for CA Certificates: keyCertSign and cRLSign. CA Certificates may also assert the digitalSignature bit for the purposes of signing OCSP responses. The nonRepudiation bit shall not be asserted in Group Certificates or dual-use Certificates.

7.1.2.5 Certificate policies

For CA Certificates, this extension may list the Object Identifiers (OIDs) of a set of allowable policies under which the Subject CA may issue Certificates. When the Issuing CA does not wish to limit the set of policies under which the Subject CA may issue Certificates, it may assert the special Object Identifier *anyPolicy* with a value of { 2 5 29 32 0 } in this extension. See also CP/CPS §§ 1.3.2.

For end entity Subscriber Certificates, this extension shall list the phiCert certificate policy OID(s), as defined in CP/CPS § 1.2, identifying the policy or policies under which the Certificate was issued. For Direct Messaging Certificates issued by a DirectTrust Bundle CA, this extension shall also list (a) the OID identifying the DirectTrust CP under which the Certificate was issued, (b) a DirectTrust entity category OID, as defined in CP/CPS § 3.1.7, (c) the DirectTrust LoA OID, as referenced in CP/CPS § 3.2.3.1, corresponding to the level of assurance of identity proofing under which the Certificate was issued, and (d) if the Certificate was issued to a Device, the DirectTrust Device OID as referenced in CP/CPS § 1.1.4. For end entity Subscriber Certificates that name an organization in the O attribute of the Subject Distinguished Name and assert an entity category OID, the entity category OID corresponding to the organization's category will be asserted.

For all Certificates, other than self-signed CA Certificates, where the Issuing CA Certificate does not list the identifier *anyPolicy* in its certificate policies extension, only those OIDs listed in the certificate policies extension of the Issuing CA Certificate, or in a valid policy mapping extension of a CA Certificate when present, may be included in this extension.

7.1.2.6 Subject alternative names

This extension appears only in end user Subscriber Certificates. As required by the Direct Project Applicability Statement § 1.4, for address-bound Certificates, this extension will contain the full Direct Address as an *rfc822Name*. For domain-bound Certificates, this extension will contain the fully qualified Health Domain Name as a *dnsName*. For Certificates issued to individuals or organizations with a valid NPI or to an individual or Device sponsored by an organization with a valid NPI, the NPI number shall also be encoded into the Certificate as an *otherName* entry as described further in CP/CPS § 3.1.1.6.

7.1.2.7 Extended key usage

This extension may appear only in end entity Certificates, and shall not conflict with the primary key usage(s) asserted in the Certificate as per CP/CPS § 7.1.2.4. The following values are defined in RFC 5280. Subscriber Certificates will include the following KeyPurposeId values: id-kp-emailProtection when issued for Direct Messaging purposes; id-kp-serverAuth and/or id-kp-clientAuth when issued for infrastructure purposes. Internal Certificates issued by a CA for the purpose of signing OCSP responses will assert the following KeyPurposeId: id-kp-OCSPSigning.

7.1.2.8 CRL Distribution Points

This extension shall appear in all Subscriber Certificates and subordinate CA Certificates, and shall contain a sequence of at least one DistributionPoint, each containing a distributionPoint field with a single general name of type URI, identifying a method and location for retrieval of the current CRL issued by the CA that also issued the Certificate. For self-signed Root CA Certificates, this extension is not used.

7.1.2.9 Authority Information Access

This extension shall appear in all Certificates, other than self-signed Root CA Certificates, and shall contain an AccessDescription pair with the accessMethod OID equal to id-ad-caIssuers and the accessLocation general name of Type URI specifying the location where Certificates issued to the Issuing CA can be found. Issuing CAs may optionally include an additional AccessDescription pair in the Certificates they issue with the accessMethod OID equal to id-ad-ocsp and the accessLocation general name of Type URI specifying the location of an appropriate OCSP responder.

7.1.3 Algorithm object identifiers

All Certificates issued by our CAs are signed using the following signature algorithm: sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11).

All Certificates issued by our CAs use the following subject Public Key Algorithm: rsaEncryption (OID 1.2.840.113549.1.1.1)

7.1.4 Name forms

Requirements for name forms in our Certificates are detailed in CP/CPS §§ 3.1.1 and 7.1.2.6. Subject and Issuer fields of the Certificate shall be populated with X.500 Distinguished names composed of the attributes required by CP/CPS § 3.1.1.

7.1.5 Name constraints

The Name Constraints extension is not used in CA Certificates issued by our CAs.

7.1.6 Certificate policy object identifier

See CP/CPS § 7.1.2.5.

7.1.7 Usage of Policy Constraints extension

The Policy Constraints extension is not used in CA Certificates issued by our CAs.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued by our CAs may contain a CPS Pointer qualifier in the certificate policies extension containing a URI pointing to our CP/CPS.

7.1.9 Processing semantics for the critical Certificate Policies extension

Certificates issued by our CAs shall not include critical certificate policies extensions. However, our Relying Party Agreements require Relying Parties to consider the certificate policies listed in the certificate policies extension when determining whether or not a Certificate issued by one of our CAs will be used for an appropriate purpose.

7.2 CRL Profile

CRLs are issued by our CAs and conform to the X.509 v2 CRL profile detailed in RFC 5280. We do not generate delta CRLs. These requirements and those of the following subsections are enforced by defined CRL profiles in our CA software.

7.2.1 Version number(s)

Our CAs issue X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

Each CRL contains a non-critical Authority Key Identifier extension that is set to the same value as the subject key identifier listed in the Certificate of the Issuing CA.

Each CRL contains a non-critical CRL Number extension containing a monotonically increasing number for the CRL scope, incremented with each update to the CRL.

Each CRL may optionally contain a non-critical Authority Information Access extension containing an AccessDescription pair with the accessMethod OID equal to id-ad-caIssuers and the accessLocation general name of Type URI specifying the location where the CA Certificate of the CA signing the CRL can be found.

Each CRL entry contains a non-critical CRL reasonCode entry extension, listing the reason the corresponding Certificate was revoked, as determined by the CA Officer at the time of revocation.

CRLs issued by our CAs are signed using the following signature algorithm: sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11).

7.3 OCSP Profile

Each CA may optionally maintain an OCSP Responder. OCSP Responders will operate in accordance with the OCSP Protocol defined in RFC 2560, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”, issued by the IETF, June 1999.

7.3.1 Version number(s)

OCSP Responders will operate in accordance with version 1 of the OCSP Protocol.

7.3.2 OCSP extensions

No stipulation.

8 Compliance Audit and Other Assessment

8.1 Frequency or circumstances of assessment

We will initiate a compliance audit of our CA once every two years. These audits may be part of an accreditation process. We may, in our sole discretion, perform additional internal or external audits or other assessments as we deem appropriate. Our co-location facilities are also subject to their own SSAE-16 assessments.

8.2 Identity/qualifications of assessor

A qualified auditor will be approved by our Certification Practice Officer and may be internal or external to our Company. The compliance auditor will be thoroughly familiar with the requirements which we impose on the issuance and management of our Certificates, and be competent in the field of compliance audits. Alternatively, the Certification Practice Officer may develop an internal audit process.

8.3 Assessor's relationship to assessed entity

An auditor will describe their relationship to us and to any other PKI participants in their report, including an indication as to whether the assessor is internal to one or more of the PKI participants or an independent compliance auditor. For the biennial audit required by CP/CPS § 8.1, the compliance auditor shall be either an independent private firm, or an independent accreditation body, or sufficiently organizationally separated from the audited component to provide an unbiased, independent evaluation, and may not have served us in the development or maintenance of our CA facilities or this CP/CPS.

8.4 Topics covered by assessment

The biennial assessments of CP/CPS § 8.1 will cover those topics deemed necessary by the auditor to ensure that we are properly implementing the provisions of this CP/CPS. If this assessment is performed according to an internal audit process as per CP/CPS § 8.2, our Certification Practice Officer must approve the audit process only after determining that it covers those topics required to make these same assertions.

Any additional audits or other assessments we may perform as per CP/CPS § 8.1 may relate to the Company as a whole, or a particular component of it, or other PKI participants, and will cover those topics relevant to that audit or assessment, as determined at our sole discretion.

8.5 Actions taken as a result of deficiency

We will take steps as we deem appropriate as a result of any deficiency found during an assessment of our CA/RA operations or practices. Such steps may include, but are not limited to, temporary suspension of operations until deficiencies are corrected, changes to this CP/CPS, changes in personnel, procedures, policies, and/or equipment, and additional or more frequent compliance assessments. When other participants are the assessed entity or entities, such steps may include, but are not limited to, revocation or suspension of Certificates issued to those entities and claims for damages against the assessed entity.

8.6 Communication of results

We may choose to publish results of any assessment of our Company operations or practices in our public document repository, but are not required to do so. The repository is detailed in CP/CPS § 2. We may also choose to submit results or links to these results to other entities. Assessments of other entities will not be published in our public document repository without approval of the assessed entity, but, at our sole discretion, may be made available to the assessed entity by electronic or other means.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Current fees for Certificate application processing, issuance, renewal, revocation, modification, and re-keying are made available to Subscribers and Applicants on our website or in written materials. We reserve the right to change these fees at any time.

9.1.2 Certificate access fees

We do not charge a fee as a condition of making publically published Certificates available to Relying Parties through our website. See also CP/CPS § 6.1.4. Subscriber Certificates are made available to the corresponding Subscriber after payment of any required fees described in our Application materials and Subscriber Agreements.

9.1.3 Revocation or status information access fees

We do not charge a fee to Relying Parties as a condition of accessing publically available CRLs or to access any publically available OCSP responders.

9.1.4 Fees for other services

We do not charge a fee for access to this CP/CPS by a Relying Party, Applicant, or Subscriber. Any use made for purposes other than viewing the document, such as reproduction,

redistribution, modification, or creation of derivative works, is subject to a license agreement with us.

9.1.5 Refund policy

Our Subscriber refund policy is defined in our Subscriber Agreements and Application materials.

9.2 Financial Responsibility

EMR Direct is a business unit of California Mediterranean, a California Limited Liability Company.

9.2.1 Insurance coverage

EMR Direct maintains at least $1 million in general liability insurance coverage for errors and omissions with a commercial insurance carrier.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

We offer no insurance or warranty coverage for end entities.

9.2.4 Fiduciary Relationship

To the extent permitted by applicable law, our Subscriber Agreements and Relying Party Agreements disclaim any fiduciary relationship between us on one hand and a Subscriber or Relying Party on the other hand.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

Except for information released by us in this CP/CPS or available through other public channels, all information pertaining to the security or operation of the CA or RA is confidential. EMR Direct management is responsible, in its sole discretion, for determining what other information related to our PKI is confidential or not confidential. Confidential information need not be clearly marked as such.

9.3.2 Information not within the scope of confidential information

See CP/CPS § 9.3.1.

9.3.3 Responsibility to protect confidential information

All Participants in the PKI and any outside contractors or auditors will each secure and protect any confidential information under this CP/CPS using a reasonable degree of care, and require

the same from each of their respective employees, agents, or contractors. Notwithstanding the above, in the event that the disclosure of confidential information is required by law, regulation, or court order, such disclosure is permitted, and the disclosing party must notify us as soon as possible and prior to making the required disclosure.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

Our Subscriber Agreements, Relying Party Agreements, and website Privacy Policy define our privacy policies.

9.4.2 Information treated as private

Our Subscriber Agreements, Relying Party Agreements, and website Privacy Policy dictate what information is deemed private.

9.4.3 Information not deemed private

Any information included in a Certificate is deemed not private. Any information in the public domain is not treated as private. This includes, but is not limited to, information available in public NPI records, WHOIS databases, or through the world wide web or other public Internet resource. Our Subscriber Agreements, Relying Party Agreements, and website Privacy Policy may dictate other information that is deemed not private.

9.4.4 Responsibility to protect private information

We will use commercially reasonable efforts to secure private information.

9.4.5 Notice and consent to use private information

Our use of private information shall be dictated by our Subscriber Agreements, Relying Party Agreements, and website Privacy Policy.

9.4.6 Disclosure pursuant to judicial or administrative process

We shall not disclose private information unless allowed by our Subscriber Agreements, Relying Party Agreements, or website Privacy Policy, or unless required by applicable law or court order.

9.4.7 Other information disclosure circumstances

Not applicable.

9.5 Intellectual Property Rights

We will not knowingly violate the intellectual property rights held by others. This CP/CPS is copyrighted by us. We hold the copyright to the Certificates that we issue. We grant our

Subscribers a license to use Certificates issued to them for any purpose permitted by this CP/CPS, including a non-exclusive, royalty-free license to reproduce, publish and distribute these Certificates to facilitate permitted uses. Such license terminates when the Certificate expires or is revoked. We reserve the right to revoke a Certificate or reject an Application for a Certificate at any time and at our sole discretion. Other documents referenced in this CP/CPS may be copyrighted by other parties. phiCert is a trademark of EMR Direct. Responsibilities of Subscribers relating to trademarked names used in their Certificates are detailed in CP/CPS § 3.1.6.

9.6 Obligations, Representations and Warranties

The warranties, disclaimers of warranty, and limitations of liability among Company, Resellers, third party Registration Authorities, and their respective Customers within our PKI are set forth and governed by the respective agreements among them. Our Subscriber Agreements and Relying Party Agreements contain the warranties, disclaimers of warranty, and limitations of liability listed below.

This section of the CP/CPS relates only to the warranties and disclaimers of warranty that our CAs shall make to end user Subscribers to whom they issue Certificates and to Relying Parties, and the limitations of liability they shall place on such Subscribers and Relying Parties.

9.6.1 CA obligations, representations and warranties

Except as expressly stated in this CP/CPS, we make no representations or warranties regarding our certification services. We reserve the right to modify such representations as we see fit, at our sole discretion, or as required by law. We will use commercially reasonable efforts to ensure that Subscriber agreements and Relying Party Agreements bind the respective participants within our PKI. This includes, but is not limited to, requiring assent to a Subscriber Agreement as a condition of enrollment and requiring assent to a Relying Party Agreement as a condition of receiving Certificate status or revocation information. Such Agreements must include the provisions specified in this document related to Liability, Financial Responsibility, Interpretation and Enforcement.

Our Subscriber Agreements include a warranty to Subscribers that:

a. There are no material misrepresentations of fact in the Certificate known to or originating from us,
b. There are no errors in the Certificate introduced by us as a result of a failure to exercise reasonable care in processing the Certificate Application or creating the Certificate,
c. Their Certificate(s) meet all material requirements of this CP/CPS,
d. Revocation services and use of a repository conform to this CP/CPS in all material aspects,

e. We have complied with all applicable laws and regulations when issuing their Certificate.

Our Relying Party Agreements include a warranty to Relying Parties who reasonably rely on a Certificate pursuant to CP/CPS § 2.1.2 that:

a. All information in such a Certificate has been verified according to the requirements of our CP/CPS, and
b. We have substantially complied with this CP/CPS, and all applicable laws and regulations when issuing the Certificate.

9.6.2 RA obligations, representations and warranties

Conforming CAs must require RAs operating on their behalf to represent that they comply, in all material aspects, with this CP/CPS, their corresponding CP/CPS or RPS, and all applicable laws and regulations when participating in the issuance and management of Certificates.

9.6.3 Subscriber obligations, representations and warranties

A Subscriber must enter into the applicable Subscriber Agreement as a condition of obtaining a Certificate. The use of a private key is permitted only after the Subscriber has accepted the corresponding Certificate, entered into a valid Subscriber Agreement, and paid any required fees. Our Subscriber Agreements require Subscribers to:

a. read, understand, and agree with the terms of this CP/CPS,
b. use their Certificates in accordance with CP/CPS § 1.4,
c. cease use of their private keys at the end of their subscription period or following expiration or revocation of the corresponding Certificate,
d. promptly notify us if any information in their Certificate is inaccurate or has changed, and
e. protect their private keys from unauthorized access in accordance with CP/CPS § 6.2.

For Direct Messaging Certificates issued by one of our DirectTrust Bundle CAs, our Subscriber Agreements additionally require Subscribers to:

f. limit Users to their employees, agents, and Affiliates.

Furthermore, if a Subscriber discovers or has reason to believe that Subscriber's Private Key has been compromised or that information contained within their Certificate is incorrect or has changed, the Subscriber Agreements require Subscriber to:

g. promptly notify us to request revocation of the Certificate in accordance with CP/CPS § 4.9, and

h. promptly notify any person or organization that may reasonably be expected to rely on Subscriber's Certificate or any digital signature verifiable with reference to the Subscriber's Certificate.

Subscriber Agreements also prohibit Subscribers from:

i. monitoring, interfering with, or reverse engineering the technical aspects of our PKI, or
j. intentionally compromising the security of our PKI.

Our Subscriber Agreements further require Subscribers to warrant that:

k. All information supplied by the Subscriber or Subscriber's agent and contained in the Certificate is true,
l. All representations made by the Subscriber in the Certificate Application submitted by the Subscriber or Subscriber's agent are true,
m. No unauthorized person has ever had access to Subscriber's private key corresponding to the public key listed in the Certificate,
n. Subscriber is an end-user and is not using said private key to digitally sign any other Certificate, similar security instrument, or CRL, as a CA or otherwise,
o. Each digital signature created using said private key is the digital signature of the Subscriber and that the corresponding Certificate was valid (not expired or revoked) at the time that the digital signature was created, and
p. The Certificate is being used exclusively for legal and authorized purposes consistent with this CP/CPS.

Additional Subscriber representations regarding entity classification may also be required, as discussed in CP/CPS S § 3.1.7. Subscribers shall also agree in our Subscriber Agreements to protect their private keys at all times, in accordance with this CP/CPS, to abide by all terms, conditions, and restrictions levied on the use of their private keys and Certificates, and to promptly notify our CA or RA upon suspicion of loss or compromise of their private keys, as required by this CP/CPS. Our Subscriber Agreements state that Subscribers failing to meet the requirements of the CP/CPS for the protection of private keys are solely responsible for any loss or damage resulting from such failure. Subscriber is also solely responsible for any acts or omissions of any representative or agent acting on their behalf for Certificate application, renewal, re-keying, modification, or revocation.

9.6.4 Relying party obligations, representations and warranties

Relying Party obligations under this CP/CPS apply to Relying Parties (RPs) within our PKI through one or more Relying Party Agreements (RPAs) approved by us. RPAs state that assent to the terms of the respective RPA is a condition of using or otherwise relying on Certificates. Relying

Parties that are also Subscribers agree to be bound to the terms of both the applicable RPAs and their respective Subscriber Agreement(s) when using Certificates.

Our RPAs require Relying Parties to acknowledge that we are not responsible for assessing the appropriateness of the use of a Certificate for any given purpose, and also require that before any act of reliance, a Relying Party must:

a. be familiar with our CP/CPS;
b. independently assess the appropriateness of the use of a Certificate for any given purpose, including, but not limited to, consideration of the level of assurance asserted, and examination of all Certificate fields and extensions, including but not limited to key usage and extended key usage extensions (see CP/CPS § 7.1.2);
c. determine that the Certificate will, in fact, be used for an appropriate purpose, and not for a restricted or prohibited purpose, as described in CP/CPS § 1.4;
d. use appropriate hardware and/or software to properly apply the appropriate technical methods to perform digital signature verification or any other cryptographic operation they wish to perform;
e. identify the Certificate chain of Issuing CAs from the Certificate upon which they wish to rely up to and including the corresponding Root Certificate and verify that the digital signature on each and every Certificate in the Certificate chain, including the Certificate upon which they wish to rely, is a valid signature of the CA issuing that Certificate;
f. verify that the basic constraints extension of every Certificate in the Certificate chain is compatible with its use in the chain in accordance with CP/CPS § 1.4.2;
g. verify that each and every Certificate in the Certificate chain is not revoked, in accordance with CP/CPS §§ 4.9.6 and 4.9.10,
h. further verify trust in accordance with any verification procedures or methods described in § 4.0 of the Direct Project Applicability Statement.

Our RPAs require that a Relying Party must NOT rely on a Certificate if any of the following is true:

i. the level of assurance provided by a Certificate is not appropriate for the certificate use required, as determined by the Relying Party, or
j. the verification procedures above are unsuccessful, or
k. one or more of the Certificates in the Certificate chain, including the Certificate upon which they wish to rely, is expired, is not yet valid, or has been revoked.

If all of the checks described above are successful, our RPAs state that the Relying Party is entitled to rely on the Certificate only if reliance upon the Certificate is reasonable under the

circumstances, and that if circumstances warrant additional assurances, that it is the sole responsibility of the Relying Party to obtain such assurances before reliance on the Certificate can be deemed reasonable. If government statute or regulation require the Relying Party to have additional agreements in place with the Subscriber or any other party prior to using the Certificate or public key, then it is the sole responsibility of the Relying Party to execute the required agreements before using the Certificate or public key.

Relying Party Agreements also prohibit Relying Parties from:

l. monitoring, interfering with, or reverse engineering the technical aspects of our PKI, or
m. intentionally compromising the security of our PKI.

Our Relying Party Agreements require Relying Parties to acknowledge that as a condition of relying on a Certificate:

n. they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in said Certificate, including knowledge on PKI, on using digital certificates, and on our policies,
o. they are solely responsible for deciding whether or not to rely on such information, and
p. they shall bear any and all legal consequences of their failure to perform the Relying Party obligations described in this CP/CPS.

9.6.5 Obligations, representations and warranties of other participants

The obligations, representations and warranties among Company, CAs, RAs, Subscribers, Relying Parties, and any other participants within our PKI are set forth and governed by the respective agreements among them.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, our Subscriber Agreements and Relying Party Agreements shall disclaim all possible warranties, including any warranty of merchantability and/or fitness for a particular purpose.

9.8 Limitations of Liability

To the extent permitted by applicable law, our Subscriber Agreements and Relying Party Agreements shall limit our liability. In no event and under no circumstances shall EMR Direct be liable for any indirect, punitive, exemplary, reliance, special, incidental, or consequential damages (including, without limitation, damages for loss of business, loss of business opportunities, business interruption, loss of data, loss of profits, and loss of goodwill), whether arising from contract, tort, legislation, or any other theory of liability, any death or personal injury, any liability arising from reliance on information in a Certificate if the fault in the verified information is due to fraud or willful misconduct of the Applicant, from the usage of a

Certificate that is not valid or has not been used in conformance with this CP/CPS, or from compromise of a Subscriber's private key. Further, we shall have no liability if we cannot execute the revocation of Certificate for reasons outside of our control. Any liability shall be subject to a cap limiting our damages to two (2) times the purchase price of the Certificate, and shall apply on a per Certificate basis regardless of the number of transactions or causes of action arising out of or related to such Certificate or any services provided in respect to such Certificate. The foregoing limitations shall apply even if we have been advised of the possibility of those damages.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, our Subscriber Agreements may require Subscribers, organizations, and any representative or agent submitting an Application on behalf of a Subscriber to defend, indemnify, and hold EMR Direct, its subsidiaries, officers, employees, agents, and contractors harmless for any loss or damage resulting from one or more of the following:

a. Any falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
b. Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
c. The Subscriber's use of a Certificate other than as permitted by the Subscriber Agreement, this CP/CPS, and any applicable law,
d. The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key,
e. The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that interferes or infringes upon the Intellectual Property Rights of a third party, or
f. Any other event or circumstance as included in our Subscriber Agreements.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, our Relying Party Agreements require Relying Parties to indemnify us for any loss or damage resulting from one or more of the following:

a. The Relying Party's failure to perform the obligations of a Relying Party,

b. The Relying Party's reliance on a Certificate that is not reasonable under the circumstances,
c. The Relying Party's failure to check the status of such Certificate to determine if the Certificate or any Certificate in its Certificate chain is expired or revoked, or
d. Any other event or circumstance as included in our Relying Party Agreements.

9.10 Term and Termination

9.10.1 Term

This CP/CPS becomes effective when approved by us. This CP/CPS has no specified term and will remain effective until it is modified or terminated by us.

9.10.2 Termination

We may terminate or revoke this CP/CPS, certain portions of it, or its application to any particular participant in our PKI. We may do so, at our sole discretion, at any time and for any reason.

9.10.3 Effect of termination and survival

The requirements of this CP/CPS shall remain in effect through the end of the archive period of the last Certificate issued.

Our Subscriber Agreements and Relying Party agreements may further dictate the effect of termination and survival.

9.11 Individual notices and communications with participants

Requirements for Individual notices and communications shall be dictated by our Subscriber and Relying Party Agreements.

9.12 Amendments

9.12.1 Procedure for amendment

We may occasionally amend, revise, update, or otherwise modify this CP/CPS. We may do so in our sole discretion, at any time and for any reason.

9.12.2 Notification mechanism and period

If this CP/CPS is changed, we will publish the updated CP/CPS to our document repository on or before the effective date of the updated CP/CPS. We may choose to remove outdated versions of this CP/CPS from the repository.

9.12.3 Circumstances under which OID must be changed

Some changes to this CP/CPS will not materially reduce the assurance that a policy or its implementation provides. Such changes to this CP/CPS will not require a change in the CP OID. On the other hand, some changes will materially change the acceptability of Certificates for specific purposes, and these changes may require corresponding changes to the CP OID. The determination as to whether or not the OID must be changed will be made by our Certification Practice Officer.

9.13 Dispute Resolution Procedures

Disputes between us and one of our Customers shall be resolved pursuant to provisions in the applicable agreement between the parties. To the extent permitted by applicable law, our Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. In the event of any dispute related to our CP/CPS, we may issue one or more statements of guidance, which we may choose to publish on our public website.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the State of California, USA, shall govern the enforceability, construction, interpretation, and validity of this CP/CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in California, USA. This choice of law is made to ensure uniform procedures and interpretation for all Participants in our PKI, no matter where they are located.

This governing law provision applies only to this CP/CPS. Agreements incorporating this CP/CPS by reference may have their own governing law provisions.

9.15 Compliance with Applicable Law

This CP/CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. We will comply with all applicable laws. Our Subscriber Agreements and Relying Party Agreements include provisions requiring Subscribers and Relying Parties to comply with all applicable laws.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

Our Subscriber Agreements and Relying Party Agreements shall contain an entire agreement clause. Headings, subheadings, and other captions in this CP/CPS are intended only for convenience and reference and shall not be used in interpreting, construing, or enforcing any of the provisions of this CP/CPS.

9.16.2 Assignment

Our Subscriber Agreements and Relying Party Agreements shall contain an assignment clause, which may act to limit the ability of a party in these agreements to assign its rights or delegate its obligations under the agreement to another party.

9.16.3 Severability, Survival, Merger, and Notice

To the extent permitted by applicable law, our Subscriber Agreements and Relying Party Agreements shall contain severability, survival, merger, and notice clauses.

Should it be determined that any clause of our CP/CPS is incorrect or invalid, the other clauses of our CP/CPS shall remain in effect until our CP/CPS is updated. Each and every provision of this CP/CPS §§ 9.7, 9.8, 9.9.1, and 9.9.2 is intended to be severable and independent of any other provision and is to be enforced as such.

This CP/CPS shall be binding upon the successors, executors, heirs, representatives, agents and assigns of the parties to whom this CP/CPS applies.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Our Subscriber Agreements and Relying Party agreements require Participants to agree that waiver of one breach of contract by us does not constitute a continuing waiver or a future waiver of other breaches of contract.

9.16.5 Force Majeure

To the extent permitted by applicable law, our Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting us in case of an event outside the reasonable control of the affected party or parties, including any provision of any applicable law, regulation, or order; failure of any electrical, communication, or other system over which we have no control; fire, flood, or other natural disaster; strike; acts of war or terrorism; acts of god; or any other similar cause beyond our reasonable control and without our fault or negligence.

9.17 Other Provisions

No stipulation.