Designation: E 2212 – 02a

Standard Practice for
Healthcare Certificate Policy[1]

This standard is issued under the fixed designation E 2212; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ϵ) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This practice covers a policy ("the policy") for digital certificates that support the authentication, authorization, confidentiality, integrity, and nonrepudiation requirements of persons and organizations that electronically create, disclose, receive, or otherwise transact health information.

1.2 This practice defines a policy for three classes of certificates: (*1*) entity certificates issued to computing components such as servers, devices, applications, processes, or accounts reflecting role assignment; (*2*) basic individual certificates issued to natural persons involved in the exchange of health information used for healthcare provisioning; and (*3*) clinical individual certificates issued to natural persons and used for authentication of prescriptive orders relating to the clinical treatment of patients.

1.3 The policy defined by this practice covers: (*1*) definition of healthcare certificates, healthcare certification authorities, healthcare subscribers, and healthcare relying parties; (*2*) appropriate use of healthcare certificates; (*3*) general conditions for the issuance of healthcare certificates; (*4*) healthcare certificate formats and profile; and (*5*) requirements for the protection of key material.

1.4 The policy establishes minimum responsibilities for healthcare certification authorities, relying parties, and certificate subscribers.

2. Referenced Documents

2.1 *ASTM Standards:*

---

[1] This practice is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics , and is the direct responsibility of Subcommittee E31.20 on Data and System Security for Health Information.

Current edition approved May Nov. 10, 2002. Published October January 2003. Originally approved in 2002. Last previous edition approved in 2002 as E 2212–02.

E 2084 Specification for Authentication of Healthcare Information Using Digital Signatures[2]

E 2086 Guide for Internet and Intranet Healthcare Security[2]

2.2 *Other Documents:*

Public Law 104-191, Aug. 21, 1996, Health Insurance Portability and Accountability Act of 1996[3]

RFC 2527—Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, PKIX Working Group Internet Draft, January 3, 2002[4]

RFC 2560—Internet X.509 Public Key Infrastructure Online Certificate Status Protocol, OCSP, June 1999[5]

3. ~~Terminology Certificate and Related Terms—~~ Terminology

3.1 *Certificate and Related Terms* —A certificate, also referred to as a digital certificate or public key certificate, binds a public key value to information identifying the entity associated with the use of a corresponding private key. An entity may be an individual, organization, account, role, computer process, or device. The entity identified within the certificate is referred to as the certificate subject. The certificate is typically used to verify the digital signature of the certificate subject or to encrypt information for that subject. The reliability of the binding of a public key to a certificate subject is asserted by the certification authority (CA) that creates, issues, and distributes certificates. Certification authority is synonymous with certificate authority. Parties that depend on the accuracy of information in the certificate are referred to as relying parties. Certificate users are the collective relying parties and subscribers.

3.2 *Certificate Policy*:

3.2.1 The X.509 standard defines a certificate policy (CP) as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." For example, a particular certificate policy might indicate the type of certificate applicable for authenticating electronic data interchange transactions for the trading of goods within a specified price range. In contrast, Practice E 2212 addresses rules for certificates that support the authentication, authorization, confidentiality, integrity, and nonrepudiation requirements of persons and organizations that electronically create, disclose, receive, or otherwise transact health information.

3.2.2 Certificates contain a registered certificate policy object identifier (OID) that the relying party may use to decide whether a certificate may be trusted for a particular purpose. The OID registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the OID also publishes the CP for examination by certificate users and other parties. Each certificate should refer to a CP, but may also refer to additional nonconflicting CP.

3.2.3 Certificate policies constitute a basis for accrediting CA. Certificate policies are also used to establish a trust relationship between two or more CA (cross-certification). When CA issue cross-certificates, one CA assesses and recognizes the relevant certificate policies of the other CA.

3.3 *Certification Practice Statement* —The term certification practice statement (CPS) is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as "a statement of the practices, which a certification authority employs in issuing certificates." The CPS is differentiated from the CP in the same way that any policy is different from a practice statement. The CPS is a comprehensive description by the CA of the methods, components, and procedures it has elected to implement and which define how it conducts itself throughout the certificate life cycle. A CA with a single CPS may support multiple certificate policies if the certificates it issues will be used for different application purposes or by different certificate user communities, or both. Any number of CA, with unique CPS, may support the same certificate policy.

3.4 *Relationship Between a Certificate Policy and a Certification Practice Statement*:

3.4.1 A certificate policy assigns responsibilities to various participants in a public key infrastructure (PKI). These responsibilities may be stated in differential levels of specificity. For example, a policy may require the CA to confirm subscriber identity but leave the details to the CA to specify in its CPS. In this case, the CPS might include a list of acceptable identification documents and the methods by which the CA, its agents, or both, verify their authenticity. Alternatively, the CA might implement other identity authentication methods that rely upon statements by an employer's human resources manager. With a less specific requirement, the CA has more flexibility in determining its practices and would need to describe what options it has chosen to implement in the CPS.

3.4.2 On the other hand, a policy may have a very specific requirements, such as that the CA must use only cryptographic modules that have been formally certified as complying with the U.S. Federal Information Processing Standard 140-2 Level 3. In this case, the CPS would mirror the policy statement or perhaps extend the policy statement by indicating the name of the cryptographic module in use.

3.4.3 A certificate policy may apply to a group of organizations and is often written for a defined community of relying parties. A CPS is written by a CA and applies only to it. Thus certificate policies are the basis of establishing requirements for interoperability and equivalent assurance criteria on an industry basis. A CPS is specific to a given CA and does not provide a suitable basis for interoperability between CA operated by different organizations.

4. Significance and Use

4.1 The policy defined by this practice is written from the perspective of healthcare relying parties. It defines a set of requirements to ensure that certificates, used for authentication, authorization, confidentiality, integrity, and nonrepudiation of health information by healthcare organizations and persons, have a minimally sufficient assurance level.

4.2 This policy defines a healthcare public key infrastructure that can be used to implement other ASTM standards including Specification E 2084 and Guide E 2086.

4.3 CA that implement procedures satisfying each requirement of the policy should reference the policy's OID in the appropriate fields within its certificates. Relying parties can recognize the inclusion of the policy's OID as an indication that the issuing CA has conformed to the requirements of the policy and that the certificates referencing the policy's OID may be used for healthcare purposes.

4.4 CA that do not comply with all provisions of the policy must not assert the policy's OID in its certificates. A CA that complies with all but a limited number of provisions may reference the policy in its own policy, provided that it clearly states the specific deviations. For example, a healthcare organization might operate an internal CA that complies with all of the provisions of the basic individual certificate class except that it uses a noncomplying cryptographic module for the CA signer keys. The organization might want to use the policy as the basis for establishing trust with external relying parties. While it may not directly assert this policy using the OID, it may reference the policy in a document that includes statements explaining measures it has taken to protect the integrity of the CA signing key. Relying parties or CA wishing to facilitate cross-trust relationships must then make their own risk analysis to determine if the modified policy is adequate for the proposed usage. This assessment, while not as easy as that based upon full compliance, should be significantly facilitated by treating the policy as a reference standard from which to judge the modifications.

4.5 Certificates and the certificate issuance process can vary in at least three distinct ways. The most frequently cited variation is about assurance. Assurance levels vary depending upon the degree of diligence applied in the registration, key generation, certificate issuance, certificate revocation, and private key protection. The required assurance level depends on the risks associated with a potential compromise. The federal PKI, among others, divides assurance into three classes. Rudimentary assurance involves very little control of either the registration process or key security. The federal PKI does not consider rudimentary assurance appropriate for healthcare use. Medium assurance involves a higher degree of diligence in the registration process and requires a number controls over CA keys. Medium assurance is designed for moderate risk applications. High assurance adds additional controls on the CA and subscriber keys as well as careful division of roles in the issuance process. These additions make high assurance certificates more appropriate for higher risk applications. Certificates may also vary depending upon the type of entity whose identity is bound to the certificate. Finally, certificates are often described in terms of appropriate and inappropriate uses.

4.6 The policy does not define certificates in terms of assurance levels. Instead, it defines three classes of certificates (entity, basic individual, and clinical individual) that differ in terms of their primary intended use or purpose and in terms of their intended subscriber type. The three certificate classes are ordered so that the clinical individual certificate must meet all the requirements of the basic individual certificate and the basic individual certificate must meet all the requirements of the entity certificate.

4.7 It is anticipated that the policy will be used to facilitate cross-licensing between healthcare CA. The policy is intended to provide a common reference point for establishing compatibility of purposes, representations, and practices among a number of autonomous healthcare CA.

5. Healthcare Certificate Policy

5.1 The IETF Draft Standard (RFC 2527), Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, describes the expected contents and format of certificate policy statements. It also specifies standard section headings, contents, and numbering. The policy follows the IETF conventions.

5.2 The term "no stipulation" is used whenever the IETF draft includes a section heading for which this ~~specification~~ practice has no requirement.

5.3 IETF Guidelines (RFC 2119) require the use of "must" and "must not" while ASTM International requires the use of "shall" and "shall not." The two sets of terms are defined equivalently. IETF and ASTM International agree in the use of terms "should," "should not," and "may." Annex A1, which contains the healthcare certificate policy (referred to as the policy), follows the IETF conventions.

ANNEX

(Mandatory Information)

A1. HEALTHCARE CERTIFICATE POLICY

~~Contents~~

~~Introduction~~

~~A1.1~~

1. INTRODUCTION

1.1 Overview~~=~~

This certificate policy sets requirements for certificates that support the authentication, authorization, confidentiality, integrity, and nonrepudiation requirements of persons and organizations that electronically create, disclose, receive, or otherwise transact health information. ~~A~~

1.2~~—~~ *Policy Identification*~~=~~

There are three classes of certificates in this policy, which are defined in ~~A1.8.~~ 1.3.3. Each of these classes has an object identifier (OID) ~~that~~ which should be asserted in the *certificatePolicy* extension of certificates that comply with this policy.

~~A1.2.1 The~~

The OID are registered under the ASTM E31.20 ARC as follows:

E31-20 OBJECT IDENTIFIER	::= {iso(1) member-body(2) us(840) 10065}
Healthcare-certificate-policy OBJECT IDENTIFIER	::= {E31-20 2}
id-e3120-certpcy OBJECT IDENTIFIER	::= {Healthcare-certificate-policy 1}
id-e3120-certpcy-entity	::= {Id-e3120-certpcy 1}
id-e3120-certpcy-basicIndividual	::= {Id-e3120-certpcy 2}
id-e3120-certpcy-clinicalIndividual	::= {Id-e3120-certpcy 3}

A

1.3~~—~~ *Community and Applicability*~~—~~

The only persons or organizations expected to benefit from this policy and participate in the PKI it defines (that is, issue, obtain, use, or rely upon healthcare certificates) are CA identified in ~~A1.4;~~ 1.3.1; certificate applicants and subscribers identified in ~~A1.7.1;~~ 1.3.2.1; and qualified relying parties identified in ~~A1.7.4.~~ section 1.3.2.2. Certificates issued under this policy may be used for nonhealthcare purposes; however, assurances for such purposes are outside the scope of this policy.

~~A1.3.1 This~~

This policy is intended to define minimum requirements that must be satisfied by CA issuing certificates to healthcare persons in order for those certificates to be generally acceptable to autonomous healthcare relying parties. This policy assumes that parties participating in the PKI will have healthcare industry roles and responsibilities defined by federal regulation such as that mandated by the Health Insurance Portability and Accountability Act of 1996 also known as HIPAA [Public Law 104-191, Subtitle F–Administrative Simplification, dated Aug 21, 1996], by various state licensing requirements, or by healthcare regulations and accreditation requirements. Further, this policy assumes that all participants are subject to industry scrutiny, either as corporations or as individuals, with respect to how they exercise their healthcare roles and responsibilities. A

1.4—3.1 Certification Authorities (CA)—

This policy is binding on each certification authority (CA) that issues healthcare certificates referencing this policy, and governs CA performance with respect to all the certificates it issues referencing this policy. Each CA must set forth specific practices and processes by which it implements this policy in a publicly available document, a certification practices statement (CPS). Should the CA's CPS contain sensitive security information, the CA may include a summary of the sensitive portions in its publicity available version. Certificates that reference this policy may also reference another policy as long as the other policy does not conflict with any provision of this policy.

A1.5 CA

1.3.1.1 CA Authorized to Issue Certificates under this Policy:

A1.5.1 This Policy

This policy may only be implemented by CA that are owned and operated by:

A1.5.1.1 Healthcare

   a) Healthcare organizations that are either a healthcare provider or a health plan as defined in HIPAA.

A1.5.1.2 Healthcare

   b) Healthcare accreditation bodies, regulators, or government agencies.

A1.5.1.3 Associations

   c) Associations that are aggregations of healthcare persons or organizations. The board of the association board must have a majority representation from the healthcare professionals or organizations qualified as association members.

A1.5.1.4 Agents

   d) Agents of sponsor organizations that qualify under A1.5.1.1, A1.5.1.2, a), b), or A1.5.1.3, c) above, provided that the sponsor maintains responsibility for ensuring that its agent adheres to all provisions of this policy and as long as the sponsor maintains liability for any failure of its agent to exercise appropriate diligence in the fulfillment of those responsibilities.

A1.5.2 Any

Any CA issuing certificates that reference this policy must describe the specific practices by which it implements the requirements of this policy in a public certification practices statement (CPS). The CA must conduct compliance audits as specified in A1.23.

A1.5.3 For section 2.7.

For the benefit of all qualified relying parties, as defined in A1.7.4, section 1.3.2.2, CA referencing this policy must agree to be bound by and comply with provisions of this policy.

A1.6 Registration

1.3.1.2 Registration Authorities (RA) and Certificate Manufacturing Services (CMS)—

This policy considers RA and CMS to be agents or subcontractors of CA. Any activity of such agents related to certificates referencing this policy must comply with this policy's provisions. CA are responsible for ensuring compliance of their agents. A

1.7—3.2 End Entities:

A1.7 3.2.1— Subscribers—

End-entity subscribers recognized by this policy must be either natural persons or resources as defined in this section.

A1.7.2 Subscribers

Subscribers for healthcare certificates that reference either id-e3120-certpcy-basicIndividual or id-e3120-certpcy-clinicalIndividual are limited to natural persons that have a legitimate need to create, access, review, manipulate, or otherwise interact with individually identifiable health information. Such persons must belong to one or more of the following categories of subscribers:

Category	Instances
Independent Practitioners	Licensed or otherwise credentialed healthcare professionals who provide some patient related services independently of any healthcare organization.
Affiliated Persons	Employees or other individuals treated by a healthcare organization as a member of its workforce. For purposes of this policy, healthcare organizations include: (*1*) provider organizations that qualify for the National Provider Identifier; (*2*) payer organizations that qualify for a National Health Plan Identifier; (*3*) clearinghouses accredited by organizations such as the Electronic Healthcare Network Accreditation Commission; (*4*) business associates of healthcare organizations; and (*5*) healthcare regulatory agencies.

Category	Instances
Affiliated Persons	Employees or other individuals treated by a healthcare organization as a member of its workforce. For purposes of this policy, health-care organizations include: i) provider organizations that qualify for the National Provider Identifier; ii) payer organizations that qualify for a National Health Plan Identifier; iii) clearinghouses accredited by organizations such as the Electronic Healthcare Network Accreditation Commission; iv) business associates of healthcare organizations; and v) healthcare regulatory agencies.
Members and Patients	Members/enrollees of health benefit plans and patients of providers. For purposes of this policy, identification of a patient must include reference to specific providers, and identification of members must include reference to a specific payer.

A1.7.3 Healthcare

Healthcare certificates that reference id-e3120-certpcy-entity may identify arbitrary healthcare resources. Such resources include, but are not limited to:

A1.7.3.1 Servers

a) Servers such as SSL servers, or hardware devices such as firewalls and routers;

A1.7.3.2 Applications

b) Applications or processes;

A1.7.3.3 Proxy

c) Proxy certificates that identify natural persons but are issued without the explicit participation of the named person. Proxy certificates are used in a variety of encryption gateway applications and are common in s/MIME applications; and

A1.7.3.4 Computing

d) Computing accounts that are used to manage privileges for groups of individuals acting in a common role.

A1.7.4 *Qualified*

1.3.2.2 Qualified Relying Parties

This policy is intended for the benefit of persons, either organizations or individuals, that rely upon healthcare certificates. Such persons must have a legitimate requirement to access, review, verify, manipulate, or otherwise interact with individually identifiable health information. Q qualified relying parties must be healthcare providers, plans, or healthcare clearinghouses, or their business associates or workforce members, and must agree to the provisions of this policy. The CA may require substantiation of such agreement through execution of a relying party agreement. Persons other than qualified relying parties that rely on certificates that reference this policy do so without the benefit of any warranty described or implied in this policy.

As a practical matter, qualified relying parties may also include subscribers. A relying party agreement should be included as part of the subscriber agreement described in A1.4.

A1.8 *Applicability—Healthcare* section 4.1.

1.3.3 Applicability

Healthcare certificates are intended to support the electronic exchange of all categories of individually identifiable health information. Healthcare certificates generally may be used to facilitate server and client authentication, role-based authorization, confidentiality, integrity, and nonrepudiation of healthcare information exchange.

A1.8.1 Certificates

Certificates issued to patients are intended to support the communication of the patient's personal health information between the subscriber (patient) and the patient's healthcare providers. Similarly, certificates issued to health plan members are intended to facilitate communication of the subscriber's personal health information between the subscriber (member) and the member's health plan personnel and health plan affiliated providers.

A1.8.2 The

The classes of certificates contained in this policy, and a nonbinding description of applicability suited to each class, are described in the following table:

Certificate Class	Applicability
Entity	Suitable for use only to ensure the confidentiality of health information. Entity certificates are not sufficient to authenticate a request for health information.
Basic Individual	Suitable for use in the exchange of health information supporting the provisioning of care. Such exchanges include both administrative and descriptive clinical information.
Clinical Individual	Suitable for use in the exchange of prescriptive clinical information, including clinical orders as well as administrative and descriptive clinical information.

Certificate Class	Applicability
	Suitable for use in the exchange of health information, which under state law requires special protection, and would include among other categories of information, psychiatric evaluation and treatment, and HIV testing, status and treatment.

A1.9 *Factors*

1.3.3.1 Factors in Determining Usage—

Relying parties must evaluate the assurances provided by certificates issued under this policy relative to threats to their application and determine whether: (*1*) this policy provides sufficient assurance; (*2*) certificates referencing this policy must be supplemented with added diligence; (*3*) their application requires a more restricted certificate policy; or (*4*) if the security context of their application should be changed.

A1.9.1 A

A relying party is responsible for determining that the certificate subject is appropriately authorized to conduct the information exchange supported by the relying party's application. To reduce the potential for inappropriate reliance, certificates for a Affiliated p Persons should include value(s) for a *healthcareRoleInfo* attribute in a *subjectDirectoryAttributes* extension as described in the certificate profile included with this policy.

Terminology

A1.10 *Definitions of Terms*:

A1.10.1 *affiliated person*—the subject of a certificate affiliated with a provider or payer that has received a certificate under the policy. Certificates issued to affiliated persons are intended to be associated with the sponsor and the responsibility for authentication lies with the sponsor.

A1.10.2 *certificate*—a record that, at a minimum: (*1*) identifies the certification authority issuing it; (*2*) names or otherwise identifies a subject; (*3*) contains a public key that corresponds to a private key appropriately under the control of the subject; (*4*) identifies its operational period; and (*5*) contains a certificate serial number and is digitally signed by the certification authority issuing it. All reference to certificates in this policy must be meant to refer to healthcare certificates that are certificates used to assure appropriate access to and authenticity of individually identifiable health information.

A1.10.3 *certificate manufacturing service (CMS)*—an entity that is responsible for technical services supporting the manufacturing and delivery of certificates signed by a certification authority, but is not responsible for identification and authentication of certificate subjects (that is, a CMS is delegated or outsourced the task of actually manufacturing the certificate on behalf of a CA). Under this policy, the delegated CMS is considered an agent of the CA.

A1.10.4 *certificate revocation list (CRL)*—a time-stamped list of revoked certificates that has been digitally signed by a certification authority.

A1.10.5 *certification authority (CA)*—an entity that is responsible for authorizing and causing the issuance of a certificate. A certification authority can perform the functions of a registration agent (RA) and a certificate manufacturing service (CMS), or it can delegate or outsource either of these functions to separate entities. A certification authority performs two essential functions. First, it bears responsibility for the accurate identification and authentication of the subscriber named in a certificate as well as verifying that such subscriber possesses the private key that corresponds to the public key that will be listed in the certificate. Second, the certification authority actually creates (or manufactures) and digitally signs the certificate. The certificate issued by the certification authority then represents that certification authority's statement as to the identity of the person, group, server or process named in the certificate and the binding of that person, group, server or process to a particular public-private key pair.

A1.10.6 *certificate subject*—a component of a digital certificate that is identified with the person, group, server, or process that maintains control of the certificate's related private key.

A1.10.7 *certificate validation (verification) agent*—an entity that is responsible for verification of the current status of certificates signed by a certification authority, but is not responsible for the revocation of certificates (that is, a CVA is delegated or outsourced the task of providing to qualified relying parties CRL, OCSP, or other revocation information on behalf of a CA). The CVA is an agent of the CA.

A1.10.8 *distinguished name (DN)*—an identification scheme where entities are described by a list of specific names, with a title on each to indicate the attribute of the entity to which it refers, (for example, country=US, common name=Bob Jones). The underlying name form used in X.509.

A1.10.9 *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*—federal legislation that contains in SubTitle F, Administrative Simplification, provisions that require healthcare organizations to implement standards for electronic transactions, information security, and privacy.

A1.10.10 *healthcare certificate*—for the purposes of this policy, a healthcare certificate means an entity, basic individual, or clinical individual certificate.

A1.10.11 *healthcare person*—a person with a legitimate need to request, access, manipulate, manage, or disclose the personal health information of others. Healthcare persons acquire this status either through licenses granted to them by states or by affiliation with licensed persons or healthcare organizations.

A1.10.12 *healthcare organization*—for purposes of this policy, a healthcare organization is any of the following: (*1*) provider organizations that qualify for the national provider identifier as defined in HIPAA; (*2*) payer organizations that qualify for a national health plan identifier as defined in HIPAA; (*3*) clearinghouses accredited by organizations such as the Electronic Healthcare Network Accreditation Commission; (*4*) business associates of healthcare organizations as defined in HIPAA; or (*5*) healthcare regulatory agencies.

A1.10.13 *independent practitioners*—individuals who are licensed by a state or credentialed by a recognized healthcare association and meet the definition of a provider as defined in HIPAA, and who provide patient care independently of a healthcare organization.

A1.10.14 *internet engineering task force (IETF)*—a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

A1.10.15 *key pair*—two mathematically related keys having the properties that (*1*) one key can be used to encrypt a message that can only be decrypted using the other key, and (*2*) even knowing one key, it is computationally infeasible to discover the other key.

A1.10.16 *object identifier*—a specially formatted sequence of numbers that is registered with an internationally recognized standards organization.

A1.10.17 *off-line mode*—a CA may operate various components of its service while not connected to any network. So operating services reduces the CA's exposure to denial of service or intrusion attacks.

A1.10.18 *out-of-band*—a second, ordinarily nonelectronic, communication channel.

A1.10.19 *person*—an identified entity involved in the exchange of health information. Persons may be artificial, for example, a corporation, group, or role. A human being is a physical or natural person.

A1.10.20 *personal credentials*—documents or other attestations giving proof of a person's qualification to perform specific healthcare functions.

A1.10.21 *PKIX*—an IETF working group developing technical specifications for PKI components based on X.509 Version 3 certificates. RFC 2527 is the specification for certificate policy.

A1.10.22 *policy*—this certificate policy.

A1.10.23 *private key*—the nonpublic portion of a public key pair that is used to create a digital signature.

A1.10.24 *public key*—the key of a public key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via a certificate issued by a certification authority and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

A1.10.25 *qualified relying parties*—a relying party that is a healthcare person or organization and which agrees to the conditions of this policy.

A1.10.26 *registration agent (RA)*—an entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (that is, an RA is delegated certain tasks on behalf of a CA).

A1.10.27 *rekeying*—destruction of an existing private key and creation of a new key pair for subsequent certificate issuance.

A1.10.28 *relying party*—a recipient of a digitally signed message who relies on a certificate to verify the digital signature on the message.

A1.10.29 *responsible person*—a person designated by a sponsor to authenticate requests for certificates on the basis of a person, group, or processes affiliation with the sponsor. Where the sponsor is an individual, the sponsor is the (de facto) responsible person.

A1.10.30 *revoke a certificate*—to prematurely end the operational period of a certificate.

A1.10.31 *role*—a named collection of privileges. Typically, in role-based access control, individuals or groups are assigned to roles that are then expressed in terms of access to specific computer processes.

A1.10.32 *signer certificates*—certificates issued to CA where the related private key is used to sign subscriber certificates. Signer certificates may be self signed by the CA or signed by another CA.

A1.10.33 *sponsor*—a person or organization to which a subscriber may be affiliated (for example, as an employee, agent, member/patient, etc.). The sponsor assumes primary responsibility for certificates issued to affiliates.

A1.10.34 *subject*—a person, group, server, or process whose public key is certified by a certificate. The subject exercises control over the related private key.

A1.10.35 *subscriber*—the party that contracts with the CA for certificate issuance and bears primarily responsibility for use of the related private key. The subscriber is identified in the certificate, although not necessarily as a certificate subject.

A1.10.36 *suspension*—a subscriber's certificates may be suspended if the subscriber license or other qualification becomes subject to temporary restriction that impact the subscriber's privileges to access health information. The certificate can be removed from suspension once the license or other qualification is returned to good standing.

A1.10.37 *trustworthy system*—computer hardware, software, and procedures that: (*1*) are protected from intrusion and misuse; (*2*) provide an appropriate level of availability, reliability, and correct operation; (*3*) are suited to performing their intended functions, and (*4*) adhere to generally accepted security procedures appropriate to the sensitivity of the data that the system processes, transmits, or stores.

A1.11 *Acronyms:*

A1.11.1 *CA—Certification Authority*
A1.11.2 *CFR—Code of Federal Regulations*
A1.11.3 *CMS—Certificate Manufacturing Service*
A1.11.4 *CRL—Certificate Revocation List*
A1.11.5 *CP—Certificate Policy*
A1.11.6 *CPS—Certification Practices Statement*
A1.11.7 *CVA—Certificate Validation Agent*
A1.11.8 *DN—Distinguished Name*
A1.11.9 *HCFA—Health Care Financing Administration, now known as Centers for Medicare and Medicaid Services (CMS)*
A1.11.10 *HIPAA—Health Insurance Portability and Accountability Act of 1996, Public Law 104-191*
A1.11.11 *IETF—Internet Engineering Task Force*
A1.11.12 *LDAP—Lightweight Directory Access Protocol*
A1.11.13 *OCSP—Online Certificate Status Protocol*
A1.11.14 *OID—Object Identifier*
A1.11.15 *PIN—Personal Identification Number*
A1.11.16 *PKCS—Public Key Cryptography Standards*
A1.11.17 *PKI—Public Key Infrastructure*
A1.11.18 *RA—Registration Authority*
A1.11.19 *SPKC—Signed Public Key and Challenge*

General Provisions

Obligations

A1.12

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA Obligations—

The CA is responsible for all aspects of the issuance and management of a certificate, including control over the application and enrollment process and verification of information contained in the certificate, as well as certificate manufacture, publication, revocation, suspension, and renewal. The CA is responsible for ensuring that all aspects of the CA services and CA operations are performed in accordance with the requirements, representations, and warranties of this policy and with the CA's certification practices statement (CPS)

2.A1.13—.1 *Representations By CA—By CA*

By issuing a certificate that references this policy, the CA certifies to the subscriber, and to all qualified relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period and in accordance with this policy, that:

A1.13.1 The

a) The CA has manufactured and issued, and if necessary, will revoke the certificate in accordance with this policy.

A1.13.2 There

b) There are no misrepresentations of fact in the certificate known to the CA, and that the CA has taken reasonable steps to verify all information in the certificate. The CA must include in its CPS the specific measures that it undertakes to verify all information included in the certificate and articulate the major risks leading to misinformation that are not addressed by these measures. If desired, the CA may assert, in its CPS, dollar or other limits to it liability.

A1.13.3 The

c) The subscriber has explicitly acknowledged to the CA the subscriber's acceptance of the subscriber's obligations under this policy.

A1.13.4 The

d) The certificate meets all requirements of this policy and was processed according to the CA's CPS.

A1.14 The

The CA must maintain and make available to qualified relying parties the certificate status (valid, suspended, or revoked) information. Acceptable mechanisms include, but are not limited to, the distribution of certificate revocation lists (CRL) or online certificate status protocol (OCSP). The CA may delegate the performance of this obligation to an identified certificate validation agent (CVA), provided that the CA remains responsible for this functionality.

A1.15 *Registration*

2.1.2 Registration Authority and Certificate Manufacturing Service Obligations—

The CA must retain responsibility for ensuring that all identification and authentication functions and all certificate manufacturing and issuing functions are performed. The CA may delegate specific activities supporting these functions to identified registration authorities (RA) and/or certificate manufacturing services ~~(CMS), or both,~~ (CMS) provided that the CA warrants that these activities will be conducted in accordance with this policy. ~~A1~~

2.16~~—~~.3 *Subscriber Obligations*~~—~~

A subscriber must be either an individual who is the subject of the certificate or an organization acting on behalf of an individual who is the subject of a certificate. ~~S~~ subscriber obligations in these two cases are considered separately:

A1.16.1 ~~Where~~

a) *Where the ~~S~~ subscriber is an ~~I~~ individual~~—~~:* For the benefit of the qualified relying party, the CA must require that the subscriber enter into a binding contract which obligates the subscriber to:

A1.16.1.1 ~~Generate~~

i) Generate a key pair using a trustworthy system, or use a key pair generated in a secure hardware token by the CA or RA and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;

A1.16.1.2 ~~Acknowledge~~

ii) Acknowledge that by accepting the certificate, the subscriber is warranting that all information about the subscriber included in the certificate is true;

A1.16.1.3 ~~Use~~

iii) Use the certificate exclusively for authorized healthcare purposes consistent with this policy;

A1.16.1.4 ~~Acknowledge~~

iv) Acknowledge receipt of security training appropriate to the health information functions for which the certificate is issued; and

A1.16.1.5 ~~Instruct~~

v) Instruct the CA to revoke the certificate promptly upon any actual or suspected loss, inappropriate disclosure, or other compromise of the subscriber's private key.

A1.16.2 ~~Where~~

b) *Where the ~~S~~ subscriber is an ~~O~~ organization ~~A~~ acquiring the ~~C~~ certificate and ~~M~~ managing a ~~P~~ private ~~K~~ key on ~~B~~ behalf of an ~~I~~ individual~~—~~:* For the benefit of qualified relying parties and the identified individual who is a certificate subject, the CA must require that the subscriber enter a binding contract whereby the subscriber agrees to:

A1.16.2.1 ~~Generate~~

i) Generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;

A1.16.2.2 ~~Warrant~~

ii) Warrant that the subject information in the certificate is true and accurate;

A1.16.2.3 ~~Maintain~~

iii) Maintain controls to ensure that the private key can be used only with the knowledge and explicit action of the certificate subject;

A1.16.2.4 ~~Ensure~~

iv) Ensure that the certificate subject has received security training appropriate to the health information functions for which the certificate is issued; and

A1.16.2.5 ~~Instruct~~

v) Instruct the CA to revoke the certificate promptly upon any actual or suspected loss, inappropriate disclosure, or other compromise of the private key.

A1.16.3 ~~Where~~

c) *Where the ~~S~~ subscriber is an ~~O~~ organization ~~O~~ obtaining ~~C~~ certificates for ~~C~~ computer ~~R~~ resources as ~~D~~ defined in section 1.3.2.1:* ~~A1.7.1—For~~For the benefit of qualified relying parties, the CA must require that the subscriber enter a binding contract whereby the subscriber agrees to:

A1.16.3.1 ~~Generate~~

i) Generate a key pair using a trustworthy system and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;

A1.16.3.2 ~~Acknowledge~~

ii) Acknowledge that by accepting the certificate, the subscriber is warranting that all information and representations made by the subscriber that are included in the certificate are true;

A1.16.3.3 ~~Install~~

iii) Install technical and administrative controls over the invocation of related private key to ensure that it is used exclusively for authorized healthcare purposes;

A1.16.3.4 ~~Where~~

iv) Where the resource is an account accessible to multiple persons, maintain a list of authorized users of that account and prevent use by other parties; maintain a log of all use of the related private key, including the date and time of key use and identity

of the person or persons invoking the key use; ensure that all users of the account have received security training appropriate to the health information functions for which the certificate is issued; and

A1.16.3.5 ~~Instruct~~

v) Instruct the CA to revoke the certificate promptly upon any actual or suspected loss, inappropriate disclosure, or other compromise of the resource's private key.

A1.17 ~~*Relying*~~

2.1.4 Relying Party Obligations—

A qualified relying party must not rely on a healthcare certificate unless:

A1.17.1 ~~The~~

a) The reliance was reasonable and in good faith in light of all the circumstances known to the qualified relying party at the time of reliance.

A1.17.2 ~~The~~

b) The purpose for which the certificate was used was appropriate under this policy, under the CA's CPS, and to any implemented *subjectDirectoryAttributes*. The certificate use must be consistent with the qualified relying party's risk analysis of the certificate consuming application.

A1.17.3 ~~The~~

c) The qualified relying party confirmed the current validity of the certificate by checking the most recent CRL or other published revocation information.

The CA may establish additional obligations through agreement with relying parties.

A1.18 ~~*Liability:*~~

A1.18.1 ~~*CA Liability*—Absent~~

2.2 Liability

2.2.1 CA Liability

Absent specific disclaimers of liability to the contrary, a CA is responsible to qualified relying parties for direct damages caused by the failure of the CA to comply with the terms of this policy. The CA is liable for damages only to the extent that the damages result from use of certificates with suitable applications.

With a statement on its issued certificates, or in its CPS, a CA may disclaim any warranty of information accuracy and, instead, promise only to exercise diligence in the verification of all information provided to it and included on the certificate.

A1.18.2 ~~*RA Liability*—For~~

2.2.2 RA Liability

For purposes of this policy, RA are agents of the CA. The CA is responsible to qualified relying parties for damages due to failure of RA to perform functions assigned to it by CA.

A1.19 ~~*Financial Responsibility—No stipulation.*~~

A1.20 ~~*Interpretation and Enforcement:*~~

2.3 Financial Responsibility

No stipulation.

A1~~2~~.4 Interpretation and Enforcement

2~~0~~.4.1~~−~~ *Governing Law—*

Laws of the United States and the state in which the CA is domiciled must govern the enforceability, construction, interpretation, and validity of this policy and the CA's CPS. Further, since all participants in this PKI are subject—directly or indirectly—to HIPAA regulation, interpretation of this policy must be consistent with that regulation.

A1.20.2 ~~*Severability,*~~

2.4.2 Severability, Survival, Merger, Notice—

Should it be determined that one section of this policy is incorrect or invalid, other sections must remain in effect until the policy is updated.

A1.20.3 ~~*Dispute*~~

2.4.3 Dispute Resolution Procedures—

Any disputes arising out of this policy or the CA's CPS, unless precluded by governing law or other agreement, must be resolved pursuant to binding arbitration in accordance with the procedure of a reliable and established alternate dispute resolution (ADR) provider. If a qualified relying party or subscriber submits a dispute to the ADR service, such dispute must be submitted in the county and state in which the CA is domiciled. If a CA submits a dispute to the ADR service, such dispute must be submitted in the county and state in which the defendant qualified relying party or subscriber is domiciled. The prevailing party in a dispute to arbitration is entitled to recover the reasonable attorney's fees expended in the arbitration proceeding as well as in any subsequent proceeding required to enforce the arbitration award.

A1.21 ~~*Fees:*~~

A1.21.1 Practice

2.5 Fees

Practice E 2212, which includes this policy, is available for sale from ASTM International.

A1.21.2 The

The CA may not impose fees on the reading of this policy, the CA's CPS, or any other document incorporated by reference in issued certificates. The CA may charge fees for the issuance of certificates and access to certificates or certificate status information, subject to agreements between the CA and subscriber, or between the CA and relying party, or both. The CA should publish a schedule of its fees in its CPS.

A1.22 *Publication*

2.6 Publication and Validation Services:

A1.22.6.1– *Publication of CA Information—*

Each CA must provide in an online repository that is available to qualified relying parties:

A1.22.1.1 Certificates

    a) Certificates issued by the CA that reference this policy;

A1.22.1.2 A

    b) A certificate revocation list (CRL) or a certificate status database that may be accessed online by use of the online certificate status protocol (OCSP), LDAP query, or other validation protocol;

A1.22.1.3 The

    c) The CA's certificate for its signature key. If the CA's certificate is not a root (self-signed) certificate, then the repository must include a chain of certificates form the CA's certificate to a root certificate;

A1.22.1.4 Past

    d) Past and current versions of the CA's CPS or a summary of key provisions thereof; and

A1.22.1.5 Instructions

    e) Instructions on how to acquire this policy.

A1.22.2 *Frequency*

2.6.2 Frequency of Publication—

The CA must publish its CPS and related documents within 14 days of completion or first effect. Certificates issued by the CA must be published within 72 h of the subscriber's acceptance of the certificate. Information relating to the revocation of a certificate must be published in accordance with A1.50.

A1.22.3 *Access Controls—*The section 4.4.4.

2.6.3 Access Controls

The repository will be available to qualified relying parties on a substantially 24-hours-per-day, 7-days-per-week basis, subject to reasonable scheduled maintenance and the CA's terms of access. CA may impose access controls on certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CA and subscriber, and the sponsors and/or qualified relying parties, or both. parties. The CA should disclose the provisions for such access controls in its CPS or other related document.

A1.23 *Compliance Audit—*Before

2.7 Compliance Audit

Before the initial use of this policy and thereafter at least once every year, the CA must submit to a compliance audit by a security auditor such as certified by the Information Systems Audit and Control Association (CISA) or by the i International i Information s Systems s Security e Certification (CISSP). The purpose of the compliance audit must be to verify that the CA has in place a system to ensure the quality of the CA services that it provides and that the CA complies with all of the requirements of this policy and its CPS.

Where an organization is a CA only for persons affiliated to it, the compliance audit may be performed as part of an internal security audit. A1.

24—.8 *Confidentiality P policy—*

Information regarding subscribers that is submitted on applications for certificates but which is not included in the certificate must be kept confidential by the CA and must be used only for the purpose for which it was collected. Such information must not be released without the prior written consent of the subscriber, unless otherwise required by law. With prior consent of subscribers, such information may be published in public directories.

Identification and Authentication

A1.25 Subject

3. IDENTIFICATION AND AUTHENTICATION

Subject to the requirements noted in A1.25.1-A1.25.3, below, certificate applications may be communicated from the applicant to the CA or RA:

A1.25.1 ~~In~~

  a) In person;

A1.25.2 ~~By~~

  b) By first-class U.S. mail, FedEx or other courier; or

A1.25.3 ~~Electronically~~

  c) Electronically over a secure channel such as that provided by, for the case of affiliated persons, a local network, or, when using the public Internet, methods based on Guide E 2086.

A1.26 ~~*Types*~~

3.1.1 Types of Names—

The subject name used for certificates issued under this policy should be the X.500 Distinguished Name (DN) as detailed in the IETF Draft Standard X.509. Certificates may also include alternate subject name.

A1.27 ~~*Name Meanings—The*~~

3.1.2 Name Meanings

The utility of certificates issued pursuant to this policy requires that the names that appear in the certificate can be understood and used by relying parties. Names used in these certificates must identify the person to which they are assigned in a meaningful way.

A1.27.1 ~~This~~

This policy details naming rules and recommendations for subscriber categories as follows:

~~Resources~~	~~(*1*) Must include in the "O=" component of DN the name of the sponsor healthcare organization~~
Resources	(i) Must include in the "O=" component of DN the name of the sponsor healthcare organization
	~~(*2*) Where the certificate is issued to a secure server, the name of the server should be in the "CN=" component of DN. The name should be of the form <machine name>.<domain name>~~
	(ii) Where the certificate is issued to a secure server, the name of the server should be in the "CN=" component of DN. The name should be of the form <machine name>.<domain name>
	~~(*3*) Where the certificate is issued to an application or process, the name of the application or process should be in the "CN=" component of DN. The name should be of the form <application/process name>.<domain name>~~
	(iii) Where the certificate is issued to an application or process, the name of the application or process should be in the "CN=" component of DN. The name should be of the form <application/process name>.<domain name>
	~~(*4*) Where the certificate is issued to an "account" or a "role," the "CN=" component should include a name which communicates the healthcare function of that account or role (for example, "Medical Records Staff," "Clinical Services Departmental Clerk")~~
	(iv) Where the certificate is issued to an "account" or a "role," the "CN=" component should include a name which communicates the healthcare function of that account or role (for example, "Medical Records Staff," "Clinical Services Departmental Clerk")
~~Independent Practitioners~~	~~(*1*) Must include, in a "CN=" component of DN the first, middle (or initial), and last name of the subscriber~~
Independent Practitioners	(i) Must include, in a "CN=" component of DN the first, middle (or initial), and last name of the subscriber
~~(*2*) To aid in recognition of the subscriber's status, should include, in a "CN=" component of DN, designation of license or credential that qualifies subscriber for independent practice (for example, MD, DO, RN, RRA, CMT, R.Pharm)~~	
(ii) To aid in recognition of the subscriber's status, should include, in a "CN=" component of DN, designation of license or credential that qualifies subscriber for independent practice (for example, MD, DO, RN, RRA, CMT, R.Pharm)	
~~Affiliated Persons~~	~~(*1*) Must include, in a "CN=" component of DN, the first, middle (or initial), and last name of the subscriber~~
Affiliated Persons	(i) Must include, in a "CN=" component of DN, the first, middle (or initial), and last name of the subscriber
	~~(*2*) Must include the name of the sponsor healthcare organization in the "O=" component of DN~~
	(ii) Must include the name of the sponsor healthcare organization in the "O=" component of DN

Members/ Patients	(*1*) Must include in a "CN=" component of DN, either: ~~(*a*) The first, middle (or initial) and the last name of the sub-scriber, and~~ ~~(*b*) Appropriate organization specific patient or member alpha-numeric identifier. This form should be used where privacy con-cerns prevent publication of patient / member identity~~
Members/ Patients	(i) Must include in a "CN=" component of DN, either: (1) The first, middle (or initial) and the last name of the sub-scriber, and (2) Appropriate organization specific patient or member alpha-numeric identifier. This form should be used where privacy con-cerns prevent publication of patient / member identity ~~(*2*) Must include the name of the healthcare organization of which the person is a patient or member in the "O=" component of DN~~ (ii) Must include the name of the healthcare organization of which the person is a patient or member in the "O=" component of DN

~~A1.27.2 Organizational~~

Organizational names should reflect the legal name of the organization as indicated in application for a national payer ID or national provider ID.

~~A1.27.3 Where~~

Where subject private keys are not under the exclusive control of the subject and are managed by an organization, that organization's designation must be included in the "O= " of the subject DN.

~~A1.28 *Rules For*~~

3.1.3 Rules for Interpreting Various Name Forms ~~—~~

The CA may further stipulate how names are to be interpreted by publishing such rules in its CPS.

~~A1.29 *Uniqueness*~~

3.1.4 Uniqueness of Names ~~—~~

The subject DN listed in a certificate must be unambiguous and unique to distinct subscribers of a CA. The CA may issue multiple certificates, each with distinct key usage, to a single subscriber in accordance with the CA's CPS.

~~A1.30 *Name*~~

3.1.5 Name Claim Dispute Resolution ~~Procedure—No stipulation.~~

~~A1.31~~ Procedure

No stipulation.

3.1.6 Recognition, Authentication and Role of Trademarks ~~—~~

No stipulation. ~~A~~

3.1. ~~32—~~ 7 *Method to Prove Possession of Private* ~~Key—In~~ Key

In cases where the subscriber generates its own keys, the CA must require the subscriber to prove possession of the private key corresponding to the public key submitted with the application. This proof should be done by the subscriber using its private key to sign a value and provide that signature to the CA. For example, the applicant can provide a PKCS #10 or signed public key and challenge (SPKC) request where its public key and DN is signed using the subscriber's private key.

~~A1.32.1 In~~

In the case where the subscriber is not the certificate subject, the CA, either directly or through its registration agents (RAs), must establish that the individual or organization has established appropriate security mechanisms to ensure that the person, group, server, or process identified as the certificate subject controls any private key use identified with the certificate.

~~A1.33 *Authentication*~~

3.1.8 Authentication of Organization ~~—~~

The subscriber must present documentation containing its physical location of doing business, the name of its duly authorized representative and that person's role within the organization, and additional business information to include: legal name, type of entity, names of officers, addresses, and phone numbers, as well as any national payer or provider identifier. CA either directly or through their RA must verify this information, as well as the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

~~A~~ 3.1. ~~33~~ 8.1 ~~—~~ *Authentication of Nonhealthcare Organizations Acting as Agents* ~~—~~

Organizations that are not healthcare organizations, but which are agents or business associates of healthcare organizations, may obtain a healthcare certificate after presentation of a business associate contract with a healthcare organization. The business associate contract must meet the requirements for such contracts under the HIPAA Rules for Privacy of Individually Identifiable Health Information (45 CFR 164.502(e)(2)). That healthcare organization must endorse the agent organization's certificate request. The CA must conduct an investigation to determine:

A1.33.1.1 ~~That~~

  a) That the organization exists and is conducting business at the address listed in the certificate application.

A1.33.1.2 ~~That~~

  b) That the certificate application was signed by a signatory who was a duly authorized representative of the organization named therein.

A1.33.1.3 ~~That~~

  c) That the presented business associate contract is current and signed by a responsible person of a qualified healthcare organization and that the endorsement is similarly valid.

~~A1.34~~ *Authentication*

3.1.9 Authentication of Individual Identity—

For subscribers, the CA must ensure that the applicant's identity information is verified in accordance with applicable policy and CPS and that this identity information and public key are properly bound. Additionally, for each accepted application, the CA must record process information to include the method, date and time, and agent of the identity verification.

~~A~~3.1.~~34~~9.1~ *Qualifications of Agents Trusted and Competent to Perform Identification and Authentication Functions*—

The CA is ultimately responsible for complete and accurate identification and authentication of the subscriber as well as their membership in an appropriate healthcare subscriber category. The CA may delegate the actual in-person verification to a trusted and competent agent. Note whereas notaries are, in principle, trusted to perform identity verification, they are not, without special training, competent to verify the applicant's membership in one of the healthcare subscriber categories. Before the CA may delegate responsibility for identification and authentication functions, it must determine that the agent is both trusted to perform the function and competent to determine membership in an appropriate category.

~~A1.34.2~~ *Persons*

Persons who ~~Q~~ qualify as ~~T~~ trusted ~~A~~ agents of CA ~~Include:~~

~~A1.34.2.1 Employees~~ include:

  i) Employees of the CA.

~~A1.34.2.2 Healthcare~~

  ii) Healthcare professionals, provided that the activity on behalf of the CA is bound to professional obligation.

~~A1.34.2.3 Staff~~

  iii) Staff of healthcare organizations, as long as the activity on behalf of the CA is recognized and supervised by the healthcare organization.

~~A1.34.2.4 Persons~~

  iv) Persons licensed by states to perform notarial functions.

~~A1.34.2.5 Persons~~

  v) Persons bonded with respect to activities of this section performed by that agent.

~~A1.34.3 Persons~~

Persons who are competent to determine the applicant's membership in a subscriber category of this policy include:

~~A1.34.3.1 Healthcare~~

  i) Healthcare professionals, as long as the determination is based on their personal knowledge of the applicant's healthcare related activity.

~~A1.34.3.2 Staff~~

  ii) Staff of healthcare organizations, where the determination is made with respect to members of that organization's workforce or its patients/members.

~~A1.34.3.3 Persons~~

  iii) Persons who receive specialized training in the recognition and validation of healthcare credentials. At a minimum, such persons must be familiar with any paper documents that are accepted as evidence of category membership and know procedures by which they may verify the document's authenticity.

~~A~~3.1.~~34~~9.~~4~~2 *Identification and Authentication Requirements by Certificate ~~Class~~*:

~~A1.34.4.1 The~~ Class

The following table summarizes the identification requirements for each certificate class.

Certificate Class	Identification Requirements
~~Entity~~	~~The CA may issue certificates to pseudonyms or nonphysical persons. The CA must confirm the identity of the sponsor's designated responsible individual as specified in A1.35. The CA may then rely upon the designated responsible individual to properly authenticate the entity.~~
Entity	The CA may issue certificates to pseudonyms or nonphysical persons. The CA must confirm the identity of the sponsor's designated responsible individual as specified in 3.1.1.10. The CA may then rely upon the designated responsible Individual to properly authenticate the entity.

15

Certificate Class	Identification Requirements
Basic Individual	The CA must ensure that the applicant's identity information is verified in accordance with this policy and its CPS and that this identity information and public key are properly bound. In general, the applicant's identity and membership category must be verified by the applicant's personal appearance before a competent agent of the CA. Identity and category membership may be verified by reference to: (*1*) The agent's personal knowledge of the applicant; or (*2*) Credentials provided by a healthcare organization; or (*3*) Government issued ID; or (*4*) Any combination thereof. Identity and category membership may be verified by reference to: (i) The agent's personal knowledge of the applicant; or (ii) Credentials provided by a healthcare organization; or (iii) Government issued ID; or (iv) Any combination thereof. The personal appearance need not be contemporaneous (coincident) to the certificate application. If the personal appearance is not contemporaneous with the application process, the CA must employ measures to ensure that the person proving possession of the private key during the application process is the same person identified during the personal appearance. For example, a one-time password assigned during the personal appearance is included in the signed PKCS#10 or SPKC. The CA must explain its procedures in its CPS. The following table provides additional identification requirements for each subscriber category: Independent Practitioners—CA must verify the currency and good standing of the subscriber's licensing or qualifying credential with the issuing authority. Affiliated Persons—CA must verify the applicant's current participation in the affiliated organization's workforce. Members/Patients—CA must verify with the affiliated organization the applicant's current or past plan membership with the relevant health plan, or in the case of patients, that the applicant is now or was a patient of the provider.
Clinical Individual	Same as for basic individual certificates.

A1.35 *Authentication*

3.1.10 Authentication of Resource Identities—

When resources such as computing components (servers, routers, monitoring devices) or communication conveniences such as group or role accounts are named as certificate subjects, the resource must have an organizational sponsor. Prior to issuance of certificate to such resources, the CA must establish a trustworthy method whereby the sponsor may designate one or more responsible individuals, and authorize them to represent the sponsor in connection with the issuance and revocation of the resource certificates. The CA may then rely upon so designated responsible individual(s) to properly authenticate the resource.

A1.35.1 The

The responsible individual may be authenticated by the procedures for affiliated persons within the class of basic individual certificates. Authentication and verification of certificate applications for resources in entity class certificates may be made by validation of a digitally signed message sent from the responsible party.

A1.36 *Certificate individual.*

3.2 Certificate Renewal, Update and Routine Rekey:

A1.36.1 *Routine Rekey*—The Rekey

3.2.1 Routine Rekey

The longer a key is used the greater the susceptibility to loss or compromise. Therefore it is important that a subscriber periodically reestablishes key and identity. When rekeying, a new certificate is issued with the same characteristics as the old but with a different public key (corresponding to a different private key), a different serial number, and potentially a different validity period. CA should specify, in its CPS, the maximum key usage period after which it will require the rekey of issued certificates.

A1.36.2 For

For purposes of rekeying, subscribers must identify themselves as detailed in the following table.

Certificate Class	Routine Rekey Identity Requirements
Entity	Identity may be established with digital signature of sponsor's responsible individual.

Certificate Class	Routine Rekey Identity Requirements
Basic Individual	Identity may be established through the use of the subscriber's current digital signature. The CA should in its CPS specify a period subsequent to initial registration after which the subscriber's identity must be re-established by procedures equivalent to the initial registration.
Clinical Individual	Identity may be established by use of a current digital signature within the currency period of the credentials used to qualify the subscriber. For renewals subsequent to that period, the subscriber's identity must be re-established by procedures equivalent to the original registration.

A1.
37—.2.2 *Certificate Renewal—*

Renewing a certificate involves creating a new certificate with same name, key pair, and other information as the old one, but with a new validity period and serial number. A certificate may be renewed if the old certificate is still current and valid, and the subscriber name and attributes have not changed.

A1.37.1 Prior

Prior to the scheduled expiration of a healthcare certificate, a subscriber may request renewal of his or her certificate from the CA that originally issued the certificate, provided the original certificate has not been suspended or revoked. Such a request may be made electronically via a digitally signed message generated with the subscriber's private key that corresponds to the public key contained in the original certificate. Prior to reissuance, the CA must confirm the accuracy of information contained in the certificate, including but not limited to, the currency of any license, organization role, or credential information contained in the certificate, just as with a first time application. Renewal certificates may be issued without rekeying. Renewal with rekeying requires reauthentication of the subscriber by the CA or RA as specified in A1.36.1.

A1.38 *Certificate Update—Updating* 3.2.1.

3.2.3 Certificate Update

Updating a certificate means issuing a new certificate to an existing subscriber with the same key, different serial number but which differs from an existing certificate in either identifier or other attribute fields. For example, the CA may choose to update the certificate of a subscriber who has received new credentials or whose organizational role has changed. The CA should include in its CPS the procedure by which certificate updates occur. Subject and directory attribute fields require the same proof through update procedures as they would at initial registration.

A1.39 *Rekey*

3.3 Rekey After Revocation—

Applicants whose certificate has been revoked due to a compromise of private key or expiration must be reauthenticated by the CA or RA during the certificate application process, just as with a first-time application.

A1.39.1 When

When a valid certificate is revoked and reissued in order to accommodate inclusion of additional information, or the updating of subject information on the certificate, the new certificate may be reissued without rekeying the original certificate.

A1.40 *Revocation Request—A*

3.4 Revocation Request

A revocation request may be initiated by a subscriber, sponsor, or relying party or by a regulatory body, provided that the certificate is used to conduct a transaction under that body's jurisdiction.

A1.40.1 A

A revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the subscriber's old and potentially compromised key pair. Revocation requests authenticated on the basis of the old key pair must always be accepted as valid. CA should state in its CPS the maximum latency for the processing of such requests.

A1.40.2 Each

Each CA should specify in its CPS specific procedures by which S subscribers who have "lost" lost their private key may revoke the related certificate. Such procedures must support alternatives, possibility possibly nonelectronic, to digital signature based authentication. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

A1.40.3 A

A relying party may request revocation of a certificate by presenting the CA with evidence of key compromise; error; change in certificate content, including but not limited to license or registration revocation; or employment status change. The CA must address revocation requests. If the CA has reason to believe that the revocation request has merit, it must investigate. As soon as the CA has sufficient reason to believe that the certificate is invalid or the key has been compromised, it must make this status information available to relying parties. In order to minimize the need for revocation and reissue following investigation of

third-party requests for revocation, the challenged certificate may be placed on suspended status for the duration of the investigation not to exceed 10 days. Once final determination is made, the certificate may be revoked or removed from suspended status. The graded response to third party requests specified in this paragraph is intended to balance the need to respond in a timely manner to any significant evidence of compromise, error, or change with the need to prevent denial of service resulting from spurious third-party requests for revocation.

~~Operational Requirements~~

~~A1.41   Certificate Application—A~~n

4. OPERATIONAL REQUIREMENTS
4.1 Certificate Application

An applicant for a certificate must complete a certificate application in a form prescribed by the CA and enter into a subscriber agreement with the CA. All applications are subject to review, approval, and acceptance by the CA. The following persons may initiate the certificate application process:

Potential Subscriber	Authorized Initiator
Resource	Sponsor's Responsible Individual
Independent Practitioner	Subscriber
Affiliated Person	Subscriber or Sponsor's Responsible Individual
Member/Patient	Subscriber
Organization	Duly authorized representative only

~~A1.~~

4.~~2~~— *Certificate Issuance*—

Upon successful completion of a subscriber identification and authentication process conducted in accordance with this policy, and after final review and approval of the certificate application, the CA should issue the requested certificate.

~~A1.42.1 The~~

The CA must ensure that certificates are delivered to independent practitioners named in certificates. The CA must not publish a certificate until it has been accepted by and delivered to the applicant.

~~A1.42.2 The~~

The CA may make arrangements with responsible individuals of sponsors to deliver certificates to affiliated persons. If keys must be transported to the certificate subject, the ~~r~~ Responsible ~~i~~ Individual must take steps to prevent unauthorized private key use prior to the subject's receipt of those keys. In every circumstance, the sponsor must take steps to ensure that private key use remains under the identifiable control of the certificate subject and that the subject has accepted responsibility for its use. ~~A1.~~

4.~~3~~— *Certificate Acceptance*—

The CA must contractually require the subscriber to, coincident with or following the issuance of a certificate, indicate the subscriber's acceptance or rejection of the certificate to the CA. In its CPS, the CA must specify its procedures and time frame for certificate acceptance. The maximum period allowed for certificate acceptance must not be more than 30 days. If the subscriber does not indicate acceptance within the maximum time period, then the certificate must be revoked. Certificate acceptance for clinical individual certificates issued under this policy should be accomplished through electronic means with a document digitally signed using the subscriber's private key. ~~A1~~

4.~~4~~4— *Certificate Revocation*~~:~~

~~A1~~4.~~4~~4.1— *Circumstances for Revocation*—

The issuing CA must revoke a certificate:

~~A1.44.1.1 Upon~~

   a) Upon failure of the subscriber (or the sponsor, where applicable) to meet its material obligations under this policy, any applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force;

~~A1.44.1.2 Upon~~

   b) Upon knowledge or reasonable suspicion of private key compromise;

~~A1.44.1.3 If~~

   c) If the CA determines that subject information contained in the certificate is no longer true;

~~A1.44.1.4 If~~

   d) If the CA determines that the certificate was not properly issued in accordance with this policy or the applicable CPS, or both;

~~A1.44.1.5 In~~

   e) In the event that the CA will cease operations, all certificates issued by the CA must be revoked prior to the date that the CA ceases operations; or

~~A1.44.1.6 For~~

   f) For any reason, upon a request by the subscriber or sponsor.

~~A1.44.2 Subscribers,~~

Subscribers, RA and sponsors have a duty to inform the CA if they become aware of inaccuracy of the subject information in the certificate. ~~A1~~

4.45—.1.1 *Permissive Revocation*—
A subscriber may request revocation of the subscriber's certificate at any time for any reason. A sponsor (where applicable) may request revocation of the certificate of any affiliated person or resource at any time for any reason. The issuing CA may also revoke a certificate upon failure of the subscriber (or the sponsor, where applicable) to meet its obligations under this policy, its CPS, or any other agreement, regulation, or law applicable to the certificate.

A1.46 *Required Revocation—A*

4.4.1.2 Required Revocation
A subscriber or sponsor (where applicable) must promptly request revocation of a certificate:
A1.46.1 Whenever
  a) Whenever any of the information on the certificate changes or becomes obsolete;
A1.46.2 Whenever
  b) Whenever the private key associated with the certificate is, or is reasonably suspected of having been, compromised; or
A1.46.3 Whenever
  c) Whenever an affiliated person is no longer affiliated with the sponsor.

A1.47 *Who*

4.4.2 Who Can Request Revocation—
The subscriber, the sponsor (where applicable), the issuing CA, or its delegated RA are authorized to request revocation of certificates issued under this P policy. A qualified relying party may request revocation by specifying reasons in a revocation request. The CA must perform a suitable investigation to determine the validity of this request and take appropriate action as specified in A1.40.

A1.48 *Procedure section 3.4.*

4.4.3 Procedure For Revocation Request—
A certificate revocation request should be communicated to the issuing CA as soon as possible after recognition of compromise or false subject information, either directly or through an authorized RA. A certificate revocation request may be communicated electronically, if it is digitally signed with the private key of the subscriber, or the responsible individual of the applicable sponsor. Alternatively, the subscriber or sponsor may request revocation by contacting the CA or an authorized RA in person and providing adequate proof of identification.

A1.49 *Certificate*

4.4.3.1 Certificate Status or CRL Update—
Promptly following revocation, the CA must update any applicable certificate status databases and include the certificate in the next CRL it issues.

A1.50 *Revocation*

4.4.4 Revocation Request Grace Period—
In cases of key compromise, requests for revocation should be processed immediately upon confirmation of validity. Other revocation requests should be processed within 2 business days. If a revocation request cannot be completed within 2 business days, the certificate should be suspended prior to the completion of the revocation request. The CA must state in its CPS the maximum time within which it will process certificate revocation requests. A1

4.4.5 1— *Certificate Suspension*—
Certificates should be suspended by the CA upon a temporary change in license or employment status that restricts the subscriber's rights to access health information. When the subscriber's license or employment returns to good standing, the certificate may be removed from suspension.
A1.51.1 The
The CA must either suspend or revoke the subscriber's certificate upon notification of a permanent change in license status.
A1.51.2 During
During suspension, an interim healthcare certificate may be issued to the subscriber, if the subscriber is otherwise eligible. Upon removal of the first certificate from suspension, the interim certificate must be revoked.
A1.51.3 Certificate
Certificate suspension should be supported by including the certificate in the CA's CRL with the CRLReason code specified as *certificateHold* with hold instruction *id-holdinstruction-reject* or *id-holdinstruction-callIssuer* . A certificate is returned to good standing subsequent to suspension by changing the CRLReason entry to *removeFromCRL*. A certificate is revoked following suspension and investigation by changing the reason code to "unspecified" or other as appropriate to revocation circumstances.

A1.52 *CRL*

4.4.6 CRL Issuance Frequency—

Where CRL are used, an up-to-date CRL must be issued at least every 24 h or, in the case of a CA that normally operates in off-line mode, each business day. CA issuing clinical individual certificates should issue CRL every 4 h.

A1.53 ~~Online~~

4.4.7 Online Revocation/Status Checking Availability—

Whenever an online certificate status or other database is used as an alternative to a CRL, such database should be updated promptly after revocation or suspension. If the CA processes only allow such databases to be updated on a scheduled basis, this schedule must be published in the CA's CPS.

A1.54 ~~Computer~~

4.5 Computer Security Audit Procedures—

CA system activity, including but not limited to log-ins, file access, and requests, must be automatically recorded in unalterable audit trail files. The CA must establish procedures for the regular review of these files with respect to potential security incidents.

A1.55 ~~Records Archival:~~

A1.55.1 ~~Types~~

4.6 Records Archival

4.6.1 Types Of Records Archived—

The CA must archive records of sufficient detail to establish the proper operations of the CA and the validity of any certificates that it has issued. Qualified relying-party requests to inspect such data must include the specific purpose of the request. The CA may limit disclosure to only those records that it believes are relevant to that specific request and it may deny any request that it believes may result in a compromise of system security.

A1.55.2 ~~At~~

At a minimum, the following data must be archived:

A1.55.2.1 ~~The~~

  a) The CA's CPS(s);

A1.55.2.2 ~~System~~

  b) System and equipment configuration including modifications or updates;

A1.55.2.3 ~~All~~

  c) All computer security audit data;

A1.55.2.4 ~~All~~

  d) All certificate requests, regardless of whether the application was accepted or not. Disclosure of this information is subject to the confidentiality provisions of ~~A1.24;~~

A1.55.2.5 ~~All~~ section 2.8;

  e) All revocation requests, accepted or not;

A1.55.2.6 ~~All~~

  f) All certificates and all CRL or certificate status records generated. For a CA maintaining online status information, a log of changes to the online repository satisfies this ~~requirement;~~

A1.55.2.7 ~~CA~~ requirement.

  g) CA signer certificate(s) and key ~~histories; and~~

A1.55.2.8 ~~Contracts~~ histories.

  h) Contracts between CA and RA, subscribers, and sponsors and any correspondence material to description of the CA's contractual obligations.

A1.56 ~~Retention~~

4.6.2 Retention Period for Archive—

Archive of the key and certificate information must be retained for 7 years or longer, as determined by state or federal statute. Archives of the audit trail files must be retained for at least 6 months, as determined by state or federal statue.

A1.57 ~~Protection~~

4.6.3 Protection of Archive—

The integrity and availability of archive media must be protected. Data accompanying certificate applications but not included in certificates must be protected as confidential information per ~~A1.24.~~

A1.58 ~~Archive~~ section 2.8.

4.6.4 Archive Backup Procedures—

Adequate backup procedures must be put into place so that in the event of loss or destruction of the primary archive, a complete set of backup files will be readily available.

A1.59 ~~Archive~~

4.6.5 Archive Collection System—

No stipulation.A1

4.60—.6 *Procedures to Obtain and Verify Archive Information—*

During the compliance audit required by this policy, the a Auditor must verify the integrity of the archives, and if either copy is found to be corrupted or damaged in any way, it must be replaced with the other copy held in the separate location.

A1.61 *Key Changeover—A*

4.7 Key Changeover

A CA uses a signature pair for creating certificates. The CA must not issue subscriber certificates that precede or extend beyond the validity period of its own signing certificate(s). In particular, the CA certificate validity period must extend one subscriber certificate validity period past the last use of a CA key pair.

A1.61.1 To

To minimize risk of compromise of the CA's key, the CA's signature key may be changed prior to its expiration and a new key maybe used for signing purposes. However, the older signature key must be available for issuing CRL and other status information until all certificates signed by it have expired or been revoked. The older verification key must be available until all certificates signed by the older key have expired or been revoked.

A1.62 *Compromise*

4.8 Compromise and Disaster Recovery:

A14.628.1− *Disaster Recovery Plan—*

The CA must have in place an appropriate disaster recovery and business resumption plan. In particular, this plan must address continued operation of certificate revocation services within 48 h of the unanticipated emergency.

A1.62.2 *Key*

4.8.2 Key Compromise Plan—

The CA must have in place an appropriate key compromise plan detailing its activities in the event of a compromise of the CA private signature key. Such plan must include procedures for:

A1.62.2.1 Requesting

  a) Requesting that any signer certificates related to this key be revoked;

A1.62.2.2 Revocation

  b) Revocation of all certificates signed with this key;

A1.62.2.3 Prompt

  c) Prompt notification to all subscribers of its services and all known qualified relying parties; and

A1.62.2.4 Escrow

  d) Escrow for business continuity purposes.

A1.63 *CA Termination—In*

4.9 CA Termination

In the event that the CA ceases operation, the CA must notify the issuer of any signer certificates, all subscribers, all sponsors, and any known qualified relying parties of its termination prior to the termination. All certificates issued by the CA that reference this policy will must be revoked no later than the time of termination.

Physical, Procedural, and Personnel Security Controls

A1.64 *Site*

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1.1 Site Location and Construction—

The location and construction of the facility housing the CA equipment must be consistent with that used to house high value, sensitive information. Facility location and design combined with other physical controls must provide protection against unauthorized access to CA equipment and records. Secure data centers maintaining an enterprise's health records generally meet these requirements.

A1.65 *Physical Access—The*

5.1.2 Physical Access

The CA, and all RA, must implement appropriate physical security controls to restrict access to the hardware and software used in connection with providing CA services. Access to such hardware and software must be limited to those personnel performing a trusted role as described in A1.66.1 section 5.2.1. Through its agreements with sponsors, the CA must ensure that any software or hardware that support the functions of responsible individuals are appropriately protected.

A1.65.1 The

The CA must implement physical controls to ensure that:

A1.65.1.1 ~~An~~

a) An unalterable access log is maintained and periodically reviewed[6];

A1.65.1.2 ~~Removable~~

b) Removable cryptographic modules are inactivated prior to storage. When not in use, such modules are to be stored in secure containers. Activation data is either memorized or stored in secure containers separate from those storing the cryptographic modules; and

A1.65.1.3 ~~Removable~~

c) Removable media or paper containing sensitive information related to or collected during the conduct of CA operations is stored in secure containers.

A1.65.2 ~~If~~

If the facility housing CA equipment is left unattended, a security check must be performed to ensure that:

A1.65.2.1 ~~The~~

a) The equipment is left in a state appropriate to its current mode of operation;

A1.65.2.2 ~~Any~~

b) Any security containers are properly secured;

A1.65.2.3 ~~Physical~~

c) Physical security systems (locks, vent covers, alarms) are functioning properly; and

A1.65.2.4 ~~Security~~

d) Security controls are activated to prevent unauthorized access.

A1.65.3 ~~In~~

In the event that the facility is to be left unattended, a person or group of persons must be assigned explicit responsibility for making such checks. The last person to depart must initial a sign-out sheet asserting that all necessary controls are in place.

A1.66 *Procedural Controls:*

A1.66.1 *Trusted Roles—CA*

5.2 Procedural Controls

5.2.1 Trusted Roles

CA operations involve the performance of four roles with the following responsibilities:

A1.66.1.1 ~~Administrator~~

a) **Administrator** role that is authorized to install, configure and maintain the CA; maintain user accounts; configure certificate profiles and audit parameters; and generate component keys. The ~~a~~ Administrator is responsible for these activities.

A1.66.1.2 ~~Officer~~

b) **Officer** role that requests and approves certificates and certificate revocations. The ~~o~~ Officer is responsible for verifying the identity of new applicants; approving and executing the issuance of certificates; requesting, approving, and executing certificate revocations.

A1.66.1.3 ~~Auditor~~

c) **Auditor** role that is authorized to view and maintain audit logs and is responsible for overseeing compliance audits to ensure that the CA operates in accordance with its CPS.

A1.66.1.4 ~~Operator~~

d) **Operator** role that is responsible for routine operations of CA equipment and procedures including system backups and recovery.

A1.66.2 *Multiple*

5.2.2 Multiple Roles (Number of Persons Required per Task)~~—~~

Individual CA personnel must be specifically designated to each ~~for~~ of the four designated roles. Individuals may be assigned to multiple roles with the exception that an officer may not assume an administrator or auditor role nor can an administrator assume an auditor role.

The CA system must authenticate its users and assure, though either software or procedure, that appropriate role separation is maintained.

The CA should have a trained backup for each role.

A1.67 *Number*

5.2.3 Number of Persons Required per ~~Task—No stipulation.~~

A1.68 *Personal Security Controls:* Task

No stipulation.

---

[6] *Unalterable* in this sentence refers to the ability to determine if the information contained in the log has been changed since it was originally written.

A1.68.1 Background

5.3 Personal Security Controls

5.3.1 Background and Qualifications—

All employees, contractors, and consultants of CA (collectively, personnel) that have access to or control over cryptographic operations that may materially affect the CA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA's repository, must for purposes of this policy be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who ~~are~~ must be designated to oversee the CA's operations. Such personnel are subject to background screening, training and management.

A1.68.2 Background

5.3.2 Background Check Procedures—

No stipulation.

A1~~5.68~~3.3~ *Training Requirements*—

All personnel performing duties with respect to CA operations must receive comprehensive training, including:

A1.68.3.1 ~~CA~~

a) CA security principles and operations;

A1.68.3.2 ~~All~~

b) All PKI software versions in use by the CA;

A1.68.3.3 ~~All~~

c) All PKI duties that they are expected to perform; and

A1.68.3.4 ~~Disaster~~

d) Disaster recovery and continuity procedures.

A1.68.4 Retraining

5.3.4 Retraining Frequency and Requirements—

The CA must take appropriate action to ensure that all personnel performing duties with respect to CA operations are made aware of changes in CA operations. The CA must have a training plan for any significant changes and must document that the plan was executed. Examples of such changes are software or hardware upgrades, changes in automated security, or relocation of equipment.

A1.68.5 Job

5.3.5 Job Rotation Frequency and Sequence—

No stipulation.

A1~~5.68~~3.6~ *Sanctions for Unauthorized Actions*—

The CA must take appropriate action against personnel who perform actions related to CA operation not authorized by this policy or the CA's CPS.

A1.68.7 Contracting

5.3.7 Contracting Personnel Requirements—

Contractor personnel employed to perform functions related to CA operations are subject to all applicable requirements of this policy.

A1.68.8 Documentation

5.3.8 Documentation Supplied to Personnel—

All CA and RA personnel must sign a statement acknowledging their understanding that certificates issued under this policy will be used to facilitate access to health information, that such data is protected by federal regulation and state law, and that inappropriate acquisition and use of such data may lead to criminal penalty.

~~Technical Security Controls~~

Key

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

~~A1.69 Key~~

6.1.1 Key Pair Generation—

For CA that issue certificates to independent practitioners, CA keys must be generated and stored in hardware cryptographic modules (FIPS 140-1 or 140-2 at level 2 or above).

A1.69.1 ~~For~~

For CA issuing certificates to affiliated persons, CA keys should be generated and stored in hardware cryptographic modules (FIPS 140-1 or 140-2 at level 2 or above). It is understood, though, that sponsors for such CA bear all the costs of and liability for unauthorized copies or loss of such keys. Therefore, subsequent to the sponsor's risk analysis, such a CA may choose to generate keys using software or hardware cryptographic modules with other certification.

A1.69.2 ~~Key~~

Key pairs for subscribers may be generated in either hardware or software. Key pairs for subscribers must be generated in such a way that use of the private key, at all times, remains under the control of the authorized user(s) of the key pair. Acceptable ways of accomplishing this include:

A1.69.2.1 ~~Having~~

 a) Having subscribers generate their own keys on a trustworthy system.

A1.69.2.2 ~~Having~~

 b) Having sponsors generate key pairs on a trustworthy system and manage the distribution of those keys in a way that the certificate subject's acquire and retain control over the use of the private key. This option is permissible only under the condition where the sponsor assumes complete liability for all use of the private key permitted under this policy.

A1.69.2.3 ~~Having~~

 c) Having keys generated in hardware tokens from which private keys cannot be extracted subsequent to initialization. Prior to activation, these tokens must be delivered to subscribers.

A1.69.3 *~~Private~~*

6.1.2 Private Key Delivery to Entity—

Where the subscriber generates its own key pair, no private key delivery is required. Where keys are generated elsewhere, the CA, in its CPS, must specify its procedures for private key delivery that meet the requirements of ~~A1.69.~~

A1.69.4 *~~Subscriber~~ section 6.1.1.*

6.1.3 Subscriber Public Key Delivery to Issuer—

Subscriber public keys are normally transferred to the CA ~~are~~ as part of the certificate issuance process. The subscriber's public key must be transferred to the RA or CA in a way that ensures that:

A1.69.4.1 ~~It~~

 a) It has not been changed during transit;

A1.69.4.2 ~~The~~

 b) The sender possesses the private key that corresponds to the transferred public key; and

A1.69.4.3 ~~The~~

 c) The sender of the public key is the legitimate user claimed in the certificate application.

A1.69.5 ~~Such~~

Such transfers may be accomplished electronically over a secure channel. This channel typically involves use a PKCS#10 message or equivalent. Transfers may also be accomplished via nonelectronic means such as a floppy disk sent by registered mail or courier.

A1.69.6 *~~CA~~*

6.1.4 CA Public Key Delivery to Users—

Subscribers require the CA's public key certificate to verify the subscriber's certificate and to validate trust paths. Therefore, delivery of the CA's certificate should be completed prior to or concurrent with certificate issuance, although CA may support alternate means and schedules as detailed in its CPS. Delivery is typically accomplished by secure communication of a PKCS#7 message, by publication to an online repository, or through out-of-band means.

A1.69.7 *~~Key Sizes—~~Keys*

6.1.5 Key Sizes

Keys should meet or exceed the minimum sizes required by applicable healthcare regulatory requirements.

A1.69.8 *~~Public~~*

6.1.6 Public Key Parameters Generation—

No stipulation.

A1.69.9 *~~1.7~~ Parameter Quality Checking—*

No stipulation.

A1.69.10 *~~.8~~ Hardware/Software Subscriber Key Generation—*

For entity and basic individual certificates, pseudo random numbers and key pairs may be generated in hardware or software. For clinical individual certificates, pseudo random numbers and key pairs must be generated in hardware from which the key cannot be exported.

A1.69.11 *~~Key~~*

6.1.9 Key Usage Purposes—

Public keys that are bound into certificates may be certified for use in signing or encryption. A single public key should not be certified for both signature and encryption use. Dual use may be allowed with entity and basic individual certificates to support legacy secure multipurpose internet mail extensions (s/MIME) applications. Certificates may assert the X.509 key usage bits as follows:

Certificate Class	Key Usage Bits
Entity	dataEncryption digitalSignature

Certificate Class	Key Usage Bits
Basic Individual	dataEncryption digitalSignature nonRepudia- tion (Optional for signature only key. May not be used with dual use keys.)
Clinical Individual	dataEncryption digitalSignature nonRepudia- tion (Manda- tory for signa- ture key.)

~~A1.70~~ *~~Private~~*

6.2 Private Key Protection~~:~~

~~A1~~6.7~~0~~2.1~~–~~ *Standards for Cryptographic Module*~~—~~
For CA issuing certificates to independent practitioners, private keys must be maintained in hardware cryptographic modules that satisfy FIPS 140-1 or FIPS 140-2 at level 2 or higher.

~~A1.70.2 CA~~

CA issuing certificates to affiliated individuals should maintain the CA's private signing keys in hardware modules satisfying FIPS 140-1 level 2 or higher. The organizations sponsoring these CA, however, bear all the costs of and liability for unauthorized copies or loss of the CA's private keys. Therefore, ~~subsequent~~ subject to the sponsoring organization's risk analysis, such a CA may choose to generate keys using software or hardware cryptographic modules with other certification.

~~A1.70.3 For~~

For CA issuing entity certificates, the CA's private key should be maintained in hardware or software satisfying the requirements of FIPS 140-1 or 140-~~1~~2 at level 1 or equivalent.

~~A1.71~~ *~~Private~~*

6.2.2 Private Key (N-M) Multiperson ~~Control—Per A1.66.1.~~

~~A1.72–~~ Control

Per section 5.2.1.

6.2.3 Private Key Escrow~~—~~
In the absence of contrary federal or state law, the private signature key must not be escrowed for retrieval by a third party.

~~A1.73~~ *~~Private~~*

6.2.4 Private Key Backup~~—~~
For the purposes of enabling disaster recovery and ensuring business continuity, the CA may backup or clone the CA's signature key provided that protections against unauthorized access, appropriate to the CA's security environment, are implemented.

~~A1.73.1 A~~

A subscriber may back up the subscriber's private decryption key(s). The CA/RA should inform subscribers of the consequences of the nonavailability of such private key(s) and as to appropriate method(s) for key backup. Subscribers should not backup private signature keys and the CA/RA should inform subscribers of methods for obtaining replacement in the event of private key loss.

~~A1.74~~ *~~Private~~*

6.2.5 Private Key Archival~~—~~
Private signature keys should not be archived.

~~A1.75~~ *~~Private~~*

6.2.6 Private Key Entry into Cryptographic Module~~—~~
The CA private signature key should remain in the cryptographic module that generated them, subject to backup as per ~~A1.73.~~

~~A1.76 Method~~ section 6.2.4.

6.2.7 Method of Activating Private Key~~—~~
Subscribers must be authenticated to cryptographic modules before activation (invocation) of private keys. Acceptable authentication methods include use of passphrase, PIN, biometrics, or a combination thereof. CA should provide information and training regarding configuration of targeted workstation software, hardware, or both, to ensure that this requirement is satisfied. The CA should detail method of training and information sources in its CPS.

A1.77 ~~Method~~

6.2.8 Method of Deactivating Private Key~~:~~

Once activated, cryptographic modules that store subscriber keys should not be left unattended or otherwise available to unauthorized access. After use, software cryptographic modules must be deactivated through manual or automatic log-off procedures. Portable cryptographic tokens (for example, smart cards) must be removed and securely stored. The CA must ensure that information and training regarding configuration of targeted workstation software, hardware, or both, ensures that this requirement is satisfied. The CA should detail method of training and information sources in its CPS.

A1.78 ~~Method~~

6.2.9 Method of Destroying Private Key~~:~~

Upon expiration or revocation of a certificate, or other termination of use of a private key for creating signatures, all copies of the private key should be securely destroyed. For software modules, this can be accomplished by overwriting data; for hardware, this can be accomplished by executing a "zeroize" command.

A1.79 ~~Other~~

6.3 Other Aspects of Key Pair Management~~:—Good Practices:~~

This policy discourages the dual use of single key pairs for both encryption and signature. Ensuring the availability of encrypted information requires that decryption (private) keys be backed up. However, backup or archival of signature keys challenges nonrepudiation, as subscribers can always deny signature, claiming that a private key copy was used to create an unauthorized signature. The party then asserting the signature must prove a negative, that is, that controls over the use of archived copy ~~had~~ have not been breached. However, this policy recognizes that various legacy software (especially those deployed to end users) currently supports only dual-use key pairs and therefore allows such use at the basic individual level. This policy recommends, however, that the CA encourage its subscribers to choose client software that splits signature and encryption functions. The CA should publish these recommendations in its CPS or other document intended for subscribers.

A1.79.1 ~~Public~~

6.3.1 Public Key Archival~~:~~

Public keys are archived as part of certificate archival.

A1.79.2 ~~Usage~~

6.3.2 Usage Periods for the Public and Private Keys~~:~~

CA key pairs must be replaced at least every 6 years. Subscriber key pairs must be replaced at least every 3 years.

A1.79.3 ~~Restrictions~~

6.3.3 Restrictions on CA's Private Key Use~~:~~

The CA's signature key must be used only for signing certificates and revocation lists. The CA may use separate keys for signing certificates and for signing CRL or other revocation information.

A private key used by a RA must be used only to support the RA function, unless specifically authorized otherwise by the CA.

A1.80 ~~Activation Data:~~

A1.80.1 ~~Activation Data~~

6.4 Activation Data

6.4.1 Activation Data Generation and Installation~~:~~

The data used to unlock CA or subscriber private keys, used in conjunction with physical and other access controls, should have a level of strength appropriate to the keys being protected. For private keys related to clinical individual certificates, this activation data should either be biometric or satisfy policy enforced by the hardware module. For keys related to basic individual and entity certificates, activation data can be user selected but the CA should provide guidance as part of its required training. If activation data is transmitted over a network, appropriate channel security must be implemented.

A1.80.2 ~~Activation~~

6.4.2 Activation Data Protection~~:—~~

The data used to unlock CA or subscriber private keys must be projtected from disclosure. Activation data should be biometric or memorized, not written down. If written down, this data must be protected at a level appropriate to the associated cryptographic module and, under no circumstance, stored with the cryptographic module. Protection mechanisms should include an automatic "lock out" after a predetermined number of failed login attempts.

A1.81 ~~Computer~~

6.5 Computer Security ~~Controls:~~

A1.81.1 ~~Specific~~ Controls

6.5.1 Specific Computer Security Technical Requirements~~:~~

The CA must implement the following computer security functions though a combination of operating system, software and physical safeguards:

A1.81.1.1 ~~Require~~

a) Require authenticated logins;

A1.81.1.2 ~~Provide~~

b) Provide security audit capability;

A1.81.1.3 ~~Access~~

c) Access control to CA services and PKI roles;

A1.81.1.4 ~~Enforce~~

d) Enforce separation of duties for PKI roles;

A1.81.1.5 ~~Require~~

e) Require identification and authentication of PKI roles and associated identities;

A1.81.1.6 ~~Require~~

f) Require use of cryptography for session communication over open networks;

A1.81.1.7 ~~Require~~

g) Require secure channel for identification of PKI roles and associated identities; and

A1.81.1.8 ~~Require~~

h) Require recovery mechanism for keys and CA system.

A1.81.2 *Computer*

6.5.2 Computer Security ~~Rating—No stipulation.~~

A1.82 ~~*Life*~~ *Rating*

No stipulation.

6.6 Life Cycle Technical ~~Controls:~~

A1.82.1 *System* *Controls*

6.6.1 System Development Controls—

The CA should take steps to ensure that all hardware and software are appropriate to its CA function. These steps include:

A1.82.1.1 *Acquisition*

a) Acquisition of commercial software from reliable sources using methods that ensure that hardware and software are not tampered with during ~~shipment;~~

A1.82.1.2 ~~Updates~~ shipment.

b) Updates acquired in a similar manner as original equipment and installed by trusted and trained ~~personnel;~~

A1.82.1.3 ~~Dedicating that~~ personnel.

c) Dedicating CA hardware and software to perform only tasks related to CA ~~operations;~~

A1.82.1.4 ~~Taking~~ operations.

d) Taking proper care to prevent malicious code from being loaded onto CA equipment. CA/RA hardware should be scanned for virus before first use and periodically ~~thereafter; and~~

A1.82.1.5 ~~Any~~ thereafter.

e) Any software or hardware designed or developed specially for the CA should be developed in a controlled environment using defined and documented processes.

A1.82.2 *Security*

6.6.2 Security Management Controls—

A formal configuration management methodology should be used for installation and ongoing management of the CA system. The CA must document the initial configuration as well as any modifications or upgrades to the system. When first loaded, the CA must verify that the software is that supplied by the vendor with no modification and ~~that~~ it is the version intended for use. The integrity of CA software should be verified on a regular basis.

A1.82.3 *Life*

6.6.3 Life Cycle Security Rating—

No stipulation.A1

6.83—7 *Network Security Controls—*

The CA must implement appropriate security measures to protect online components against intrusion and denial of service attacks. Such measures include use of guards, firewalls, or filtering routers. Any software present should be necessary to the functioning of the CA; unused network ports and services should be turned off.

A1.84 ~~*Cryptographic*~~

6.8 Cryptographic Module Engineering ~~Controls—No stipulation.~~

~~Certificate and CRL Profiles~~

A1.85~~ ~~ Controls

No stipulation.

27

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile—

Certificates that reference this policy must contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages, including public keys used for digital-signature verification.

A1.85.1 ~~All~~

All certificates that reference this policy must be issued in the X.509 format. In their CPS, CA should identify the certificate extensions supported and specify extensions consistent with the healthcare certificate profile attached to this policy.

A1.86 ~~CRL Profile—If~~

7.2 CRL Profile

If used, CRL will be issued in the X.509 version 2 format. Any CRL issued by CA referencing this policy must include the CRLNumber extension and should use the CRLReason extension. The CA's CPS must identify the CRL extensions supported.

~~Policy Administration~~

A1.87 ~~Policy~~

8. POLICY ADMINISTRATION

8.1 Policy Change Procedures—

ASTM Subcommittee E31.20 is responsible for the maintenance of this policy and will review and revise it as necessary after its approval and publication as an ASTM standard. Subsequent to review, this policy must be submitted to Subcommittee E31.20 for reapproval, revision, or withdrawal. If this policy is withdrawn, CA must discontinue using this policy's OID.

A1.88 ~~Publication~~

8.2 Publication and Notification Procedures—

CA referencing this policy may not publicly post copies of this policy, due to copyright restrictions of ASTM International. ASTM International will make this policy available for a nominal fee at its Internet website (www.astm.org).

A1.89 ~~CPS~~

8.3 CPS Approval Procedures—

A CA's CPS contains implementation details of the CA's service and its procedures. A future ASTM standard for certification practices will specify practices that ensure conformity with this policy.

9. BIBLIOGRAPHY

HCFA Internet Security Policy, Centers for Medicare and Medicaid Services, November 24, 1998. For copy of policy go to http://www.hcfa.gov/security/isecplcy.htm.

Health Insurance Portability and Accountability Act of 1996, Public Law 104-192, Subtitle F-Administrative Simplification, dated August 21, 1996. For copy of legislation go to http://aspe.os.dhhs.gov/admnsimp.

IETF Draft Standard—Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Network Working Group, 26 January 1999. For copy of standard go to http://www.ietf.org/rfc/rfc2459.txt.

IETF Draft Standard—Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, PKIX Working Group Internet Draft, January 3, 2002. For copy of standard go to http://www.ietf.org/html.charters/pkix-charter.html

Public Key Cryptography Standards, Numbers 1-13, RSA Security, Bedford, MA, 1991-2001. For copies of standards go to http://www.rsasecurity.com.

Security and Electronic Signature Standards; Proposed Rule, Department of Health and Human Services, 45 CFR Parts 142 published in the Federal Register, August 12, 1998, Volume 63, Number 155. For copy of standard, go to http://aspe.os.dhhs.gov/admnsimp.

Security Requirements for Cryptographic Modules, FIPS Pub 140-2, Department of Commerce, May 25, 2001. For copy of publication go to http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Standards for Privacy of Individually Identifiable Health Information; Final Rule, Department of Health and Human Services, 45 CFR Parts 160 and 164 published in the Federal Register, December 28, 2000. For copy of standard, go to http://aspe.os.dhhs.gov/admnsimp.

10. ACRONYMS

CA Certification Authority
CFR Code of Federal Regulations
CMS Certificate Manufacturing Service or Centers for Medicare and Medicaid Services
CRL Certificate Revocation List
CP Certificate Policy

CPS Certification Practices Statement
CVA Certificate Validation Agent
DN Distinguished Name
HCFA Health Care Financing Administration, now known as Centers for Medicare and Medicaid Services (CMS)
HIPAA Health Insurance Portability and Accountability Act
IETF Internet Engineering Task Force
LDAP Lightweight Directory Access Protocol
OCSP Online Certificate Status Protocol
OID Object identifier
PIN Personal Identification Number
PKCS Public Key Cryptography Standards
PKI Public Key Infrastructure
RA Registration Authoritygent
SPKC   Signed Public Key And Challenge

11. GLOSSARY

Affiliated Person: The subject of a certificate that is affiliated with a provider or payer whichpayer that has received a certificate under the policy. Certificates issued to Affiliated Persons are intended to be associated with the sponsor and the responsibility for authentication lies with the sponsor.

Certificate: A record that, at a minimum: (*1*) identifies the certification authority issuing it; (*2*) names or otherwise identifies a Subject; (*3*) contains a public key that corresponds to a private key appropriately under the control of the Subject; (*4*) identifies its operational period; and (*5*) contains a certificate serial number and is digitally signed by the certification authority issuing it. All reference to certificates in this policy must be meant to refer to healthcare certificates whichcertificates that are certificates used to assure appropriate access to and authenticity of individually identifiable health information.

Certificate Manufacturing Service (CMS): An entity that is responsible for technical services supporting the manufacturing and delivery of certificates signed by a certification authority, but is not responsible for identification and authentication of certificate subjects (that is, a CMS is delegated or outsourced the task of actually manufacturing the certificate on behalf of a CA). Under this policy, the delegated CMS is considered an agent of the CA.

Certificate Revocation List (CRL): A time-stamped list of revoked certificates that has been digitally signed by a certification authority.

Certification Authority (CA): An entity that is responsible for authorizing and causing the issuance of a certificate. A certification authority can perform the functions of a registration authority (RA) and a certificate manufacturing service (CMS), or it can delegate or outsource either of these functions to separate entities. A certification authority performs two essential functions. First, it bears responsibility for the accurate identification and authentication of the subscriber named in a certificate as well as verifying that such subscriber possesses the private key that corresponds to the public key that will be listed in the certificate. Second, the certification authority actually creates (or manufactures) and digitally signs the certificate. The certificate issued by the certification authority then represents that certification authority's statement as to the identity of the person, group, server or process named in the certificate and the binding of that person, group, server or process to a particular public-private key pair.

Certificate Subject: A component of a digital certificate which is identified with the person, group, server or process which maintains control of the certificate's related private key.

Certificate Validation (Verification) Agent: An entity that is responsible for verification of the current status of certificates signed by a certification authority, but is not responsible for the revocation of certificates (that is, a CVA is delegated or outsourced the task of providing to qualified relying parties CRL, OCSP or other revocation information on behalf of a CA). The CVA is an agent of the CA.

Distinguished Name (DN): An identification scheme where entities are described by a list of specific names, which a title on each to indicate the attribute of the entity to which it refers, (for example, country=US, common name=Bob Jones). The underlying name form used in X.509.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): Federal legislation, which contains in SubTitle F, Administrative Simplification, provisions that require healthcare organizations to implement standards for electronic transactions, information security and privacy.

Healthcare Certificate: For the purposes of this policy, a healthcare certificate means eithermeans an entity, basic individual or clinical individual certificate.

Healthcare Person: A person with a legitimate need to request, access, manipulate manage or disclose the personal health information of others. Healthcare persons acquire this status either through licenses granted to them by states or by affiliation with licensed persons or healthcare organizations.

Healthcare Organization: For purposes of this policy, a healthcare organization is any of the following: (*1*) provider organizations that qualify for the national provider identifier as defined in HIPAA; (*2*) payer organizations that qualify.28 for a

national health plan identifier as defined in HIPAA; (*3*) clearinghouses accredited by organizations such as the Electronic Healthcare Network Accreditation Commission; (*4*) Business associates of healthcare organizations as defined in HIPAA; or (*5*) healthcare regulatory agencies.

Independent Practitioners: Individuals who are licensed by a state or credentialed by a recognized healthcare association, who meet the definition of a provider as defined in HIPAA, and who provide patient care independently of a healthcare organization.

Internet Engineering Task Force (IETF): A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Key Pair: Two mathematically related keys, having the properties that (*1*) one key can be used to encrypt a message that can only be decrypted using the other key, and (*2*) even knowing one key, it is computationally infeasible to discover the other key.

Object Identifier: A specially-formatted sequence of numbers that is registered with an internationally recognized standards organization.

Off-line Mode: A CA may operate various components of its service while not connected to any network. So operating services reduces the CA's exposure to denial of service or intrusion attacks.

Out-of-Band: A second, ordinarily non-electronic, communication channel.

Person: An identified entity involved in the exchange of health information. Persons may be artificial, for example, a corporation, group or role. A human being is a physical or natural person.

Personal Credentials: Documents or other attestations giving proof of a person's qualification to perform specific healthcare functions.

PKIX: An IETF working group developing technical specifications for a PKI components based on X.509 Version 3 certificates. RFC 2527 is the specification for certificate policy.

Policy: This certificate policy.

Private Key: The non-public portion of a public key pair that is used to create a digital signature.

Public Key: The key of a public key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via a certificate issued by a certification authority and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

Qualified Relying Parties: A relying party which is a healthcare person or organization and whichParty that is a healthcare person or organization and which agrees to the conditions of this policy.

Registration Agent (RA): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (that is, an RA is delegated certain tasks on behalf of a CA).

Rekeying: Destruction of an existing private key and creation of a new key pair for subsequent certificate issuance.

Relying Party: A recipient of a digitally signed message who relies on a certificate to verify the digital signature on the message.

Responsible Person: A person designated by a sponsor to authenticate requests for certificates on the basis of a person, group, or processes affiliation with the sponsor. Where the sponsor is an individual the sponsor is the (de facto) responsible person.

Revoke A Certificate: To prematurely end the operational period of a certificate.

Role: A named collection of privileges. Typically, in role based access control, individuals or groups are assigned to roles which are then expressed in terms of access to specific computer processes.

Signer Certificates: Certificates issued to CA where the related private key is used to sign subscriber certificates. Signer certificates may be self signed by the CA or signed by another CA.

Sponsor: A person or organization with to which an subscriber may be affiliated (for example, as an employee, agent, member/patient etc.). The sponsor assumes primary responsibility for certificates issued to affiliates.

Subject: A person, group, server or process whose public key is certified by a certificate. The subject exercises control over the related private key.

Subscriber: The party that contracts with the CA for certificate issuance and bears primarily responsibility for use of the related private key. The subscriber is identified in the certificate although not necessarily as a certificate subject.

Suspension: A subscriber's certificates may be suspended if the subscriber license or other qualification becomes subject to temporary restriction that impact the subscriber's privileges to access health information. The certificate can be removed from suspension once the license or other qualification is returned to good standing.

Trustworthy System: Computer hardware, software, and procedures that are: (*1*) are protected from intrusion and misuse; (*2*) provide an appropriate level of availability, reliability, and correct operation; (*3*) are suited to performing their intended functions, and (*4*) adhere to generally accepted security procedures appropriate to the sensitivity of the data that the system processes, transmits, or stores.

ATTACHMENT—HEALTHCARE CERTIFICATE PROFILE

X1.1 The

The intention of this practice is that certificates issued under ~~the ASTM Healthcare Certificate Policy~~ Practice E 2212 will conform to the specifications of IETF Draft, Internet X.509 Public Key Infrastructure Certificate and CRL Profile (formerly RFC 2459).

X1.2 This

This profile recommends use of a noncritical *subjectDirectoryAttributes* extension to include, in issued certificates, subscriber role and licensing information. Role and licensing information assist relying parties by:

X1.2.1 Disambiguating

   a) Disambiguating name conflicts, especially in the case of independent practitioners. Medical license authorities typically assign a unique license identifier to each licensee. Similarly named individuals can be distinguished by reference to license identifier.

X1.2.2 Facilitating

   b) Facilitating appropriate reliance. Healthcare persons' information privilege derives from the healthcare roles that they occupy. Certificates provide a standard and reliable method to communicate that role information.

X1.3 *Certificate Format and Extensions for End Entities*—See Table X1.1.

X1.4 *OID Suffixes*—See Table X1.2.

X1.5 *HCRole Attribute*—See Tables X1.3 and X1.4.

—

BIBLIOGRAPHY

(**1**) HCFA Internet Security Policy, Centers for Medicare and Medicaid Services, November 24, 1998. For copy of policy, go

A.1 CERTIFICATE FORMAT AND EXTENSIONS FOR END ENTITIES

Note 1—Section heading refers to http://www.hcfa.gov/security/isecplcy.htm.

(**2**) Health Insurance Portability and Accountability Act this document unless otherwise specified.
Note 2—Completion of 1996, Public Law 104-192, Subtitle F-Administrative Simplification, dated August 21, 1996. For copy of legislation, go fields is mandatory unless otherwise noted.
Note 3—Source refers to http://aspe.os.dhhs.gov/admnsimp.
(**3**) IETF section reference in IETF Draft Standard—Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Network Working Group, January 1999. For copy of standard, go to http://www.ietf.org/rfc/rfc2459.txt.
(**4**) IETF Draft Standard—Internet X.509 Public Key Infrastructure Profile.

Field	OID	Support	Source	Comments
Base Certificate P				
Base Certificate				
on		Required	4.1.1.1	
Version		Required	4.1.1.1	
Serial Number		Required	4.1.2.1	
Signature		Required	4.1.2.3	
Issuer Name		Required	4.1.2.4	
Validity		Required	4.1.2.5	UTCtime
Subject DN		Required		CN, O components mandatory and Certification Practices Framework, PKIX Working Group Internet Draft, January 3, 2002. For copy of standard, go to http://www.ietf.org/html.charters/pkix-charter.html.
				(**5**) Public Key Cryptography Standards, Numbers 1-13, L components recommended
Subject DN		Required		CN, O components mandatory; C, OU,S, and L components recommended
subjectPublic KeyInfo algorithm		Required	4.1.2.7	
algorithmIdentifier		Required		MD5 with RSA Security, Bedford, MA, 1991-2001. For copies signature or SHA-1 with RSA signature
algorithmIdentifier		Required		MD5 with RSA signature or SHA-1 with RSA signature
parameters				NULL with RSA signature
subjectPublicKey				
Standard Extensions				
keyUsage		Recommended	4.2.1.3	Critical if specified, values per section 6.1.9 of standards, go to http://www.rsasecurity.com.
				(**6**) Security and Electronic Signature Standards; Proposed Rule, Department E 2212
keyUsage		Recommended	4.2.1.3	Critical if specified, values per section 6.1.9 of E 2212
certficatePolicies		Recommended	4.2.1.5	Noncritical
PolicyInformation				
policyIdentifier				If used, per section 1.2 of H E 2212
policyIdentifier				If used, per section 1.2 of E 2212
policyQualifier		Optional		textual user notice
policyQualifier		Optional		URI of Issuer's CPS and/or textual user notice
subjectAltName		Optional		Required for use with s/mime
extendedKeyUsage		Optional	4.2.1.13	Noncritical
cRLDistributionPoints			4.2.1.14	Noncritical
subjectDirectoryAttributes			4.2.1.9	Noncritical
hcRole		SequenceRecommendedISO/TC215 ASTM (hcRole)		See explanatory text

A.2 OID SUFFIXES

The policy defines OID for various profile elements and Human Services, 45 CFR Parts 142 published values. OID registered under the Subcommittee E31.20 arc and used as suffixes in the Federal Register, August 12, 1998, Volume 63, Number 155. For copy following are:

E31-20 OBJECT IDENTIFIER	::= {iso(1) member-body(2) us(840) 10065}
Healthcare-certificate-policy OBJECT IDENTIFIER	::= {E31-20 2}
id-e3120-certpcy OBJECT IDENTIFIER	::= {Healthcare-certificate-policy 1}
hcRole OBJECT IDENTIFIER	::= {Healthcare-certificate-policy 2}

A.3 HCROLE ATTRIBUTE USED IN THIS PRACTICE

This profile supports the use of standard, go to http://aspe.os.dhhs.gov/admnsimp.
(7) Security Requirements syntax developed for Cryptographic Modules, FIPS Pub 140-2, Department of Commerce, May 25, 2001. For copy of publication, go to http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
(8) Standards an hcRole attribute by the ISO TC-215/W4. The data type is reproduced here as follows:

```
hcRole ATTRIBUTE ::= {
    WITH SYNTAX              HCActorData
    EQUALITY MATCHING RULE   hcActorMatch
    SUBSTRNGS MATCHING RULE  hcActorSubstringsMatch
    ID                       id-at-hcpki-healthcareactor }
with object identifier values assigned by ISO/TS 17090-2,
    id-hcpki-at ::= 1.0.17090.0
    id-at-healthcareactor ::= 1.0.17090.0.1


Data types are defined as follows:
HCActorData ::= SET OF HCActor


HCActor ::= SEQUENCE {
codedData [0]                CodedData OPTIONAL,
    RegionalHCActorData [1]  SEQUENCE OF RegionalData OPTIONAL }


CodedData ::= SET {
    codingSchemeReference [0]    OBJECT IDENTIFIER,
        contains Refrence OID for Privacy an ISO coding scheme reference OID or ISO registered local coding scheme
        —contains Refrence OID for an ISO coding scheme reference OID or ISO registered local coding scheme
        at least ONE of Individually Identifiable Health Information; Final Rule, Department the following must be present
        —at least ONE of the following must be present
    codeDataValue [1]       NumericString, OPTIONAL,
    codeDataFreeText [2]    DirectoryString OPTIONAL }


RegionalData ::= SEQUENCE {
  type      REGIONALDATA.&.id ((SupportedRegionalData)),
  value     REGIONALDATA.&.id ((SupportedRegionalData) (&type))) }


REGIONALDATA ::= CLASS {
  &type,
  &id OBJECT IDENTIFIER UNIQUE }
  WITH SYNTAX {
    WITH SYNATX             &Type
    ID                      &id }
SupportedRegionalData REGIONALDATA ::= {
  coded,
    —implementers should expect future definition of additional regional information objects
 }


coded ::= REGIONAL-DATA {
    WITH SYNTAX             Codealta,
    WITH SYNTAX             CodedlRegionalData,
    ID                      id-hcpki-cd }
with object identifier value assigned by ISO/TS 17090-2, id- hcpki-cd ::= 1.0.17090.1 and Human Services, 45 CFR Parts 160 and 164 published in type definition:
with object identifier value assigned by ISO/TS 17090-2, id- hcpki-cd ::= 1.0.17090.1 and type definition:


CodedRegionalData ::= SEQUENCE {
```

country [0]   **PrintableString(SIZE (2)),**
—ISO3166 code of country of issuing authority
roleAuthority [1]   **DirectoryString,**
—Identifier of role authority as Regional entity
—could be true identifier or lookup string
—for medical licenses, the Federal Register, December 28, 2000. For copy of standard
—for medical licenses, the name of the state license board
,gody
—for certification, the name of the certifying body
—for entoh ttprise
—for enterprise defined roles, the name of the healthcare enterprise
hcRoleClassificationData [2]   **CodedData,**
hcRoleQualifierData [3]   **CodedData OPTIONAL }**

A.3.1 SAMPLE USE OF HCROLE ATTRIBUTE

~~Sample 1://ase Information~~
Sample 1: subjectDirectoryAttribute for Subject's Medical License Information
(**hcRole** OBJECT IDENTIFIER ::= (id-hcp~~ki-at~~),
hcActorData   SET OF {
~~code.odedData ::= {~~
  codedData CodedData ::= {
    codingSchemeReference OBJECT IDENTIFIER ::= OID-for-ISO-Role-Coding,
    ~~codeDataValue NumericString ::= ISO-code-for-phys.ician-role~~
    codeDataValue NumericString ::= ISO-code-for-physician-role
    ~~codhysician) }~~
    codeDataFreeText ::= (physician) }
    ~~—ISO coding may not be necessary for oths.gonal context~~
    —ISO coding may not be necessary for other applications not involving an international context
  regionalHCActorData SEQUENCE OF RegionalData ::= {
    country PrintableString (SIZE(2)) ::=(US),
    roleAuthority DirectoryString ::= (C=US, ST=CA, O=State of California, OU=Medical License Board),
    hcRoleClassificationData CodedData ::= {
      codingSchemeReference OBJECT IDENTIFIER ::= OID-California-MLB-Coding-Scheme,
      ~~state issued licenses will inv/ate specific numbering, restrictions, etc~~
      —state issued licenses will involve state specific numbering, restrictions, etc
      ~~codmber' }~~
      codeFreeText DirectoryString ::= (20A4073) — license ′number′ }
    hcRoleQualifier CodedData ::= {
      codingSchemeReference OBJECT IDENTIFIER ::= OID-California-MLB- Coding-Scheme,
      ~~codeDataValue NumericString ::= (17) – code for posible restriction of California license,~~
      codeDataValue NumericString ::= (17) – code for possible restriction of California license,
      codeFreeText DirectoryString ::= (June 25, 2003) – expiration date of license) }}}

~~Samp.le 2: subjectDirectoryAttribute for Subject's Organizational Role~~
Sample 2: subjectDirectoryAttribute for Subject's Organizational Role
(**hcRole** OBJECT IDENTIFIER ::= (id-hcpki-at),
  hcActorData SET OF {
    —international coding omitted for local (national) only use
    regionalHCActorData SEQUENCE OF RegionalData ::= {
      country PrintableString (SIZE(2)) ::= (US),
      roleAuthority DirectoryString ::= (C=US, ST=CA, O=Suburban Hospital),
      hcRoleClassificationData CodedData ::= {
        codingSchemeReference OBJECT IDENTIFIER ::=OID-ASTM-Role-Coding-Scheme,
        codeDataValue NumericString ::=ASTM-code-for-HIM-File-Clerk,
        codeFreeText PrintableString ::= (Health Information Management Dept File Clerk) } }}

Sample 3: subjectDirectoryAttribute for Subject's Certfication Information
(**hcRole** OBJECT IDENTIFIER ::= (id-hcpki-at),
hcActorData   SET OF {
  codedData Coded Data ::= {
    codingSchemeReference OBJECT IDENTIFIER ::= OID-for-ISO-Role-Coding,
    codeDataValue NumericString ::=ISO-code-for-transcriptionist-role
    codeDataFreeText ::= (transcriptionist) }
  regionalHCActorData SEQUENCE OF RegionalData ::= {
    country PrintableString (SIZE(2)) ::= (US),
    roleAuthority DirectoryString ::= (C=US, O=American Association for Medical Transcription),
    hcRoleClassificationData CodedData ::= {
      codingSchemeReference OBJECT IDENTIFIER ::= OID-AAMT-Coding-Scheme,
      codeDataValue NumericString ::= AAMT-code-for-CMT,
      codeFreeText PrintableString ::= (Certified Medical Transcriptionist) } }}