Designation: E 2212 – 02

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:*

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, P-KIX 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—

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 accrediting CA.

[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 10, 2002. Published October 2002.

[2] *Annual Book of ASTM Standards*, Vol 14.01.

[3] Available at http://aspe.hhs.gov/admnsimp/pl104191.htm.

[4] Available at www.ietf.org/html.charters/pkix-charter.html.

[5] Available at http://www.ietf.org/rfc/rfc2560.txt.

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 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 *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.

A1.2 *Policy Identification*—There are three classes of certificates in this policy, which are defined in A1.8. Each of these classes has an object identifier (OID) that should be asserted in the *certificatePolicy* extension of certificates that comply with this policy.

A1.2.1 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}

A1.3 *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; certificate applicants and subscribers identified in A1.7.1; and qualified relying parties identified in A1.7.4. 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 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.

A1.4 *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 Authorized to Issue Certificates under this Policy:*

A1.5.1 This policy may only be implemented by CA that are owned and operated by:

A1.5.1.1 Healthcare organizations that are either a healthcare provider or a health plan as defined in HIPAA.

A1.5.1.2 Healthcare accreditation bodies, regulators, or government agencies.

A1.5.1.3 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 of sponsor organizations that qualify under A1.5.1.1, A1.5.1.2, or A1.5.1.3, 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 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 the benefit of all qualified relying parties, as defined in A1.7.4, CA referencing this policy must agree to be bound by and comply with provisions of this policy.

A1.6 *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.

A1.7 *End Entities:*

A1.7.1 *Subscribers*—End-entity subscribers recognized by this policy must be either natural persons or resources as defined in this section.

A1.7.2 Subscribers 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.
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 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 such as SSL servers, or hardware devices such as firewalls and routers;

A1.7.3.2 Applications or processes;

A1.7.3.3 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 accounts that are used to manage privileges for groups of individuals acting in a common role.

A1.7.4 *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. Qualified relying parties must be healthcare providers, plans, or healthcare clearinghouses, or their business associates or workforce members, and must agree to the provision 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 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 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 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. 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 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 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 affiliated 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 *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).

A1.13 *Representations 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 CA has manufactured and issued, and if necessary, will revoke the certificate in accordance with this policy.

A1.13.2 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 subscriber has explicitly acknowledged to the CA the subscriber's acceptance of the subscriber's obligations under this policy.

A1.13.4 The certificate meets all requirements of this policy and was processed according to the CA's CPS.

A1.14 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 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) or certificate manufacturing services (CMS), or both, provided that the CA warrants that these activities will be conducted in accordance with this policy.

A1.16 *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. Subscriber obligations in these two cases are considered separately:

A1.16.1 *Where the Subscriber is an 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 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 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 the certificate exclusively for authorized healthcare purposes consistent with this policy;

A1.16.1.4 Acknowledge receipt of security training appropriate to the health information functions for which the certificate is issued; and

A1.16.1.5 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 the Subscriber is an Organization Acquiring the Certificate and Managing a Private Key on Behalf of an 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 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 that the subject information in the certificate is true and accurate;

A1.16.2.3 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 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 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 the Subscriber is an Organization Obtaining Certificates for Computer Resources as Defined in* A1.7.1—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 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 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 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 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 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 Party Obligations*—A qualified relying party must not rely on a healthcare certificate unless:

A1.17.1 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 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 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 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 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:*

A1.20.1 *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, 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 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 E 2212, which includes this policy, is available for sale from ASTM International.

A1.21.2 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 and Validation Services:*

A1.22.1 *Publication of CA Information*—Each CA must provide in an online repository that is available to qualified relying parties:

A1.22.1.1 Certificates issued by the CA that reference this policy;

A1.22.1.2 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 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 and current versions of the CA's CPS or a summary of key provisions thereof; and

A1.22.1.5 Instructions on how to acquire this policy.

A1.22.2 *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 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 qualified relying parties, or both. The CA should disclose the provisions for such access controls in its CPS or other related document.

A1.23 *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 international information systems security 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 *Confidentiality 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 to the requirements noted in A1.25.1-A1.25.3, certificate applications may be communicated from the applicant to the CA or RA:

A1.25.1 In person;

A1.25.2 By first-class U.S. mail or other courier; or

A1.25.3 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 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 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 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 (*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> (*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> (*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")
Independent Practitioners	(*1*) 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)
Affiliated Persons	(*1*) 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
Members/ Patients	(*1*) Must include in a "CN=" component of DN, either: (*a*) The first, middle (or initial) and the last name of the subscriber, and (*b*) Appropriate organization specific patient or member alphanumeric identifier. This form should be used where privacy concerns 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

A1.27.2 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 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 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 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 Claim Dispute Resolution Procedure*—No stipulation.

A1.31 *Recognition, Authentication and Role of Trademarks*—No stipulation.

A1.32 *Method to Prove Possession of Private 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 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 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.

A1.33.1 *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 the organization exists and is conducting business at the address listed in the certificate application.

A1.33.1.2 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 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 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.

A1.34.1 *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 who Qualify as Trusted Agents of CA Include*:

A1.34.2.1 Employees of the CA.

A1.34.2.2 Healthcare professionals, provided that the activity on behalf of the CA is bound to professional obligation.

A1.34.2.3 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 licensed by states to perform notarial functions.

A1.34.2.5 Persons bonded with respect to activities of this section performed by that agent.

A1.34.3 Persons who are competent to determine the applicant's membership in a subscriber category of this policy include:

A1.34.3.1 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 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 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.

A1.34.4 *Identification and Authentication Requirements by Certificate Class*:

A1.34.4.1 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.
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. 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 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 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 Renewal, Update and Routine Rekey:*

A1.36.1 *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 purposes of rekeying, subscribers must identify themselves as detailed in the following table.