PARK AVENUE CAPITAL LLC

dba MaxMD

Certificate Practices Statement

V2.0.1

December 19, 2022

Table of Contents

1. INTRODUCTION

This document is the MaxMD, Inc. ("MaxMD") Certificate Practices Statement (CPS) that outlines the legal, commercial, and technical principles and practices related to MaxMD's support of Direct exchange. This CPS applies to all entities participating in or using MaxMD's certificate services, Registration Authorities (RAs), Subscribers, and Relying Parties. Park Avenue Capital dba MaxMD operates at 2200 Fletcher Avenue, Suite 506, Fort Lee, NJ 07024. Our server name is www.maxmdirect.com and our DNS address is also www.maxmdirect.com.

1.1 Overview

This Certificate Practices Statement abides strictly by the DirectTrust.Org CP V 2.0. Only sections or practices that are specific to MaxMD are outlined in this document. All other practices and operations are as specified in the CP. Please reference DirectTrust.org CP at https://www.directmdemail.com/documents/DirectTrust_CP_V2.0.pdf (a pdf copy is enclosed) as well as the Certificate Profiles mapping at https://www.directmdemail.com/documents/DirectPolicy

1.1.1 Certificate Policy (CP)

MaxMD Policy OID maps as follows:

DirectTrust CP 2.0	id-DTorg-policies.(1.4) 1.3.6.1.4.1.41179.0.2.0
DirectTrust IAL 2	id-DTorg-LoAs.(5) 1.3.6.1.4.1.41179.1.5
DirectTrust LoA 3	id-DTorg-LoAs.(3) 1.3.6.1.4.1.41179.1.3
DirectTrust CE	id-DTorg-Cat.(1) 1.3.6.1.4.1.41179.2.1
DirectTrust BA	id-DTorg-Cat.(2) 1.3.6.1.4.1.41179.2.2
DirectTrust HE	id-DTorg-Cat.(3) 1.3.6.1.4.1.41179.2.3
DirectTrust Patient	id-DTorg-Cat.(4) 1.3.6.1.4.1.41179.2.4
DirectTrust Non Declared	id-DTorg-Cat.(5) 1.3.6.1.4.1.41179.2.5
DirectTrust Device	id-DTorg.(3) 1.3.6.1.4.1.41179.3.1

1.1.2 Relationship between this CPS and DirectTrust CP

MaxMD CPS is audited by the EHNAC P&S program as well as the DirectTrust.org HISP, RA, and CA Accreditation program. This Certificate Practices Statement abides strictly by the DirectTrust.Org CP V 2.0

1.1.3 Relationship between this DirectTrust CP and the CA CP

The MaxMD CA CP is the DirectTrust.org CP V 2.0.

1.1.4 Relationship between DirectTrust CP and EHNAC-DirectTrust Accredited Entities

Conformance to an Active CP Version is a requirement for accreditation under the EHNAC DirectTrust Accreditation program as described in CP Section 1.5.3, and entities accredited under this program have been audited regarding implementation of practices in compliance with an Active CP version in conjunction with proper use of the DirectTrust policy OIDs. DirectTrust publishes bundles

of trust anchors for the purpose of assisting Relying Parties in verifying the accredited status of HISPs, CAs, and RAs, available at bundles.directrust.org.

1.2 Document Name and Identification

This CPS is numbered CPSV2.0.1 to indicate its correspondence to the DirectTrust.org CP Version 2.0. It is published at https://www.directmdemail.com/documents/DirectTrust_CP_V2.0.pdf.

1.3 PKI Participants

1.3.1.3 Certification Authority (CA)

MaxMD signs certificate signing requests (CSRs) and issues public key X.509 certificates to Direct exchange or Direct Project organizational or individual Subscribers. MaxMD conforms to the policies of the DirectTrust.org CP V 2.0. For ease of reference herein, MaxMD may be referred to as "Issuer CA".

1.3.2 Registration Authorities (RAs)

In conformance with the CP, MaxMD may act as RA or may delegate the collection of identity proofing to a trusted agent that has executed the MaxMD Agent Registration Agreement that binds their behavior to the roles and responsibilities defined therein.

1.3.3 Subscribers

A Direct Subscriber is an entity who uses Direct services and PKI to support Direct transactions and communications. Subscribers are not always the party identified in a certificate, such as when Direct Organizational certificates are issued to a Health Domain address. The Subject of a certificate is the party named in the certificate. A Subscriber, as used herein, refers to both the subject of the certificate and the entity that contracted with the Issuer CA for the certificate's issuance in accordance with this certificate policy. A Subscriber may contract a third party to manage their subscriptions, e.g. in the case of a Group certificate managed by a HISP, an authorized officer at the HISP is also a Subscriber, and each Subscriber must abide by the required Subscriber Agreements. Prior to verification of identity and issuance of a certificate, a Subscriber is an Applicant.

1.3.3.1 Health Information Service Providers (HISPs)

MaxMD operates as a HISP and processes Direct Compliant messages to and from Direct addresses. Acting in the capacity of an agent for the Subscriber, the HISP will hold and manage PKI private keys associated with a Direct digital certificate on behalf of the Subscriber.

1.3.4 Relying Parties

A Relying Party uses a Subscriber's X.509 certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the

Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information (CRL or OCSP).

1.3.5 Other Participants

Certain MaxMD Direct HISP customers are designated as "Trusted Agents". Trusted Agents are authorized by MaxMD Direct HISP and MaxMD RA to gather documentation and perform RA functions in relation to the issuance of a digital certificate.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The primary anticipated use for a Direct Trust Community X.509 certificate is in the exchange of electronic messages grounded in the specification of the Direct Project. This includes S/MIME message signature verification and S/MIME message encryption. Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the certificate. However, each Relying Party must evaluate the application environment and associated risks before deciding on whether to accept a certificate issued under this CP for a particular transaction.

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct to a known level of assurance when the certificate was issued. Certificates issued under this policy may not be used where prohibited by law.

1.5 Policy Administration

1.5.1 Organization administering the document

MaxMD is the entity responsible for administering this policy statement. MaxMD may be contacted at:
MaxMD
Suite 506
2200 Fletcher Avenue
Fort Lee, New Jersey 07024
Tel: 1-201-963-0005
Fax: 1-201-482-5925

1.5.2 Contact Person

Questions regarding this policy can be sent to:
IT Regulatory Officer
MaxMD
Suite 506

2200 Fletcher Avenue
Fort Lee, New Jersey 07024
Tel: 1-201-963-0005
Fax: 1-201-482-5925

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

IT Regulatory Officer
MaxMD
Suite 506
2200 Fletcher Avenue
Fort Lee, New Jersey 07024
Tel: 1-201-963-0005
Fax: 1-201-482-5925

1.5.4 Certification Practices Statement Approval Procedures

Approval of this CP/CPS and any amendments hereto is by MaxMD. Amendments may be made by updating this entire document or by addendum. MaxMD determines whether changes to this CPS require notice or any change in the OID of a certificate issued pursuant to this CPS.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Acronym	Meaning
BA	Business Associate
CA	Certification Authority
CE	Covered Entity
CFR	Code of Federal Regulation
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DTPC	DirectTrust Policy Committee
HE	Healthcare Entity
HISP	Healthcare Information Services Provider
ID	Identity
IdM	Identity Management
IETF	Internet Engineering Task Force
ISSO	Information Systems Security Officer
LoA	Level of Assurance
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Health Information Technology
PKI	Public Key Infrastructure

RA	Registration Authority
RFC	Request For Comments
S/MIME	Secure Multipurpose Internet Mail Extensions
TA	Trusted Agent

1.6.2 Definitions

Terms and Definitions are specified in DirectTrust.org CP V 2.0

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

MaxMD publishes this CPS, certificate terms and conditions, the relying party agreement and the subscriber agreement in the official MaxMD repository at
https://www.directmdemail.com/documents/DirectPolicy
Any revocation data on issued digital certificates is published at location of the CRL distribution point or OCSP responder specified in the certificate.

2.1.1 Repository Obligations

The MaxMD Repository operates 24 hours per day, 7 days per week with 99% availability overall per year.

2.2 Publication of certification information

The MaxMD certificate services and the MaxMD repository are accessible through several means of communication:

1. On the web: https://www.directmdemail.com/documents/DirectPolicy
2. By email to support@Max.MD
3. By mail addressed to: MaxMD, 2200 Fletcher Ave., Fort Lee, NJ 07024
4. By telephone Tel: 1-201-963-0005
5. By fax: 1-201-482-5925

MaxMD publishes CRLs to allow relying parties to determine the validity of a certificate issued by MaxMD. Each CRL contains entries for all revoked un-expired certificates issued. The CRL Distribution point is defined within each certificate.

2.2.3 Interoperability

MaxMD participates in DirectTrust Interoperability Testing and seeks to be 100% interoperable with all accredited DirectTrust entities.

2.3 Frequency of Publication

This CPS is available in the repository prior to issuance of any certificates referencing this CPS. CRLs from the MaxMD CA expire every 30 days and are updated whenever a new entry is added, or every thirty days, whichever is earlier.

2.4 Access controls on repositories

Parties (including Subscribers and Relying Parties) accessing the MaxMD Repository (https://www.directmdemail.com/documents/DirectPolicy) and other MaxMD publication resources (CRLs and OCSP) are deemed to have agreed with the provisions of this CP/CPS and any other conditions of usage that MaxMD may make available. Parties demonstrate acceptance of the conditions of usage of this CPS by using a MaxMD-issued certificate. Failure to comply with the conditions of usage of the MaxMD Repositories and web site may result in termination of the relationship between MaxMD and the party, at MaxMD's sole discretion, and any unauthorized reliance on a certificate shall be at that party's risk.

2.4.1 Access Controls on Repositories

The MaxMD Repository (https://www.directmdemail.com/documents/DirectPolicy) contains documentation including this CPS, the MaxMD CP and RPS. It is available in read only format and publicly available at all times.
Admin tools to submit PII artifacts are available via an HTTPS link provided to the customer by a MaxMD Officer. MaxMD Officers and Administrators are granted read only access to the artifacts via an administrative tool.
Private keys are wrapped in a FIPS 140-2 level 3 Hardware Security Module and stored in a private table. All cryptographic functions involving the private key are performed within the Hardware Security Module. The private key can never be activated outside of the Hardware Security Module.
Public key and certificates are stored in a private table and published via a DNS responder to the public.
Message logs are stored on the STA server and extracted to a database table that where users may read records they are authorized to view.
All CA events are logged on the STA server and maintained for the required seven years and six months specified in the CP.

3 Identification and Authentication

MaxMD follows the procedures outlined in the CP and issues DirectTrust LoA 3 and DirectTrust IAL 2 identity proofed certificates

3.1 Naming

3.1.1 Types of Names

All certificates shall use non-null DN name forms for the issuer and subject names. As specified in the Direct Project Applicability Statement for Secure Health Transport, certificates tied to full Direct addresses ("Address certificates") shall contain the Direct address in the subjectAltName extended

attribute as an rfc822Name. Certificates tied to a Direct domain ("Organizational certificates") shall contain the domain name in two places:
1. The subjectAltName extension formatted as a dNSName, and
2. The CN of the Subject DN.

3.1.2 Need for Names to be Meaningful

Names used in certificates shall uniquely identify the organization or person to which they are assigned and shall be easily understood by humans.

3.1.3 Anonymity or Pseudonymity of Subscribers

MaxMD CA does not issue anonymous certificates. Pseudonymous certificates may be issued as long as name space uniqueness requirements are met.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

MaxMD publishes certificates in DNS and enforces uniqueness of the subject DN within our namespace. An attempt to duplicate a name will fail to publish in DNS.

3.1.6 Recognition, Authentication, and Role of Trademarks

Should it come to the attention of the Officer or the Administrator that a certificate infringes on the intellectual property of another entity, the MaxMD CA reserves the right to revoke such certificate.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The MaxMD HISP generates and maintains the private key. All private keys are generated within a FIPS 140-2 level 3 Hardware Security Module. They are wrapped prior to export and then stored in a secure table. The MaxMD CA does not transport or import private keys to or from any other source.

3.2.2 Authentication of Organization Identity

Requests for organizational certificates must include the organization name, mailing address, and documentation of the existence of the organization as well as the requested domain name that will appear in the certificate (see section 3.1.1 for details).

The requesting organization must be qualified in one of the following categories:

- HIPAA Covered Entity.
- HIPAA Business Associate, or
- Healthcare-related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA.

Each organizational certificate must represent a legally distinct entity. Each organization executes a Master Services Agreement with MaxMD . MaxMD performs a credit check and validates the entity type. EIN numbers and other submitted data are validated against commercially available databases.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

MaxMD validates the identity of the Trusted Agent or the administrative representative of an organizational certificate according to procedures for either DirectTrust LoA 3 or DirectTrust IAL 2 in the MaxMD RPS and the DirectTrust CP.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

MaxMD requires that all human subscribers sharing a role based certificate are required to be registered with the MaxMD RA and identity proofed to the level of the role-based certificate.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

MaxMD requires that all human subscribers sharing a Group Certificate are required to be registered with the MaxMD RA and identity proofed to the level of the group certificate as more fully described in the MaxMD RPS

3.2.3.4 Authentication of Devices

When a certificate is issued for a device, there must be a human sponsor. The human sponsor will be identity proofed to the level of the certificate. The sponsor will also provide

- Equipment Identification (e.g. Health Domain Name, DNS name, Device Identifier, or Health Endpoint Name associated with the Device).
- Equipment Public Keys
- Equipment authorizations and attributes (to be included in the certificate)
- Contact Information

3.2.3.5 Authentication of Human Subscribers for Content Commitment Certificates

The Private Key of a Content Commitment certificate may be held and managed by a Custodian on behalf of the Subscriber however the use and activation of the private key are limited to the Subscriber and not shared with the Custodian.

3.2.3.6 Verification of NPI Number

If the NPI Number is included in a Certificate, MaxMD requires the number to be verified against the NPI Registry provided by the Centers for Medicare & Medicaid Services (CMS).

3.2.4 Non-verified Subscriber Information

All Subscriber information placed in a DirectTrust certificate must be verified and a certificate issued within 30 days of completion of verification. Any non-verified Subscriber information shall not be included in the Certificate.

3.2.5 Validation of Authority

MaxMD Direct HISP shall confirm the contact information and authority of the certificate requester with an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication. MaxMD Direct HISP shall then use that information to contact the certificate requester to verify the authenticity of the request.
The MaxMD RA or its Trusted Agent validates the identity of individual certificates according to procedures for DirectTrust LoA 3 or DirectTrust IAL 2 as defined in the MaxMD RPS and the MaxMD CP. The RA or Trusted Agent will verify the relationship between the organization and all subscribers with access to the organization certificate.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

The MaxMD CA does not rekey existing certificates. The process to replace a key is to revoke the existing certificate and key, create a new Certificate Signing Request (CSR) and upon verification of the certificate owner, the new CSR will be signed and the certificate published.

3.3.2 Identification and Authentication for Re-key after Revocation

If a DirectTrust certificate is revoked, the Subscriber shall go through the initial identity verification process described in section 3.2 to obtain a new certificate.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised. Either the MaxMD Administrator or Officer must authenticate the request.

4 Certificate Life-Cycle

4.1 Application

4.1.1 Submission of Certificate Application

The MaxMD HISP officer shall receive a Direct Project Sales Order form from a contracted customer applicant or an individual authorized to request certificates on behalf of the Applicant. For certificates that include a domain name, the Domain Name Registrar record maintained by the domain registrar

presumptively indicates who has authority over the domain. If a certificate request is submitted by an agent of the domain owner, the agent must also submit a document that authorizes Subscriber's use of the domain.

MaxMD Direct HISP may not provide certificates to an entity that is on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business. A current list can be found at the following site:
https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

4.1.2. Enrollment Process and Responsibilities

MaxMD Direct HISP shall require each Applicant to submit a Direct Project Sales Order Form with information necessary to create a Certificate Signing Request (CSR). The MaxMD RA or its Trusted Agent shall ensure the identity of the administrative contact and the users on the Order Form.

4.2 Certificate Application Processing

The MaxMD CA and RA or its Trusted Agent will verify that the information in a certificate signing request is accurate and reflect the information presented by the Subscriber.

4.2.1 Performing Identification and Authentication Functions

After initiating a certificate application, MaxMD Direct RA or its Trusted Agent shall verify the applicant in accordance with Section 3.2. After verification is complete, MaxMD Direct HISP must evaluate the corpus of information and decide whether or not to issue the certificate.
MaxMD Direct HISP shall ensure that all communication between MaxMD RA and MaxMD CA regarding certificate issuance or changes in the status of a certificate are made using secure and auditable methods. MaxMD Direct HISP shall protect all sensitive information obtained from the Applicant and securely exchange this information with the CA and RA in a confidential and tamper-evident manner that is protected from unauthorized access. MaxMD Direct HISP must track the exchange using an auditable chain of custody.

4.2.2 Approval or Rejection of Certificate Applications

MaxMD Direct HISP shall reject any certificate application that MaxMD Direct HISP cannot verify. MaxMD Direct HISP shall also not initiate a certificate application if MaxMD Direct HISP reasonably believes that issuing the certificate could damage or diminish MaxMD's reputation or business.

If some or all of the documentation used to support the application is in a language other than English, a MaxMD Direct HISP employee skilled in such language and having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the final cross-correlation and due diligence. MaxMD Direct HISP may also rely on a translation of the relevant portions of the documentation by a qualified translator.

If the certificate application is not rejected and is successfully validated, MaxMD Direct HISP will approve the certificate application, upload all of the information used to verify the applicant to a server

controlled by MaxMD, and issue the certificate. Rejected Applicants may re-apply. MaxMD Direct HISP shall contractually obligate Subscribers to check the data listed in the certificate for accuracy prior to using the certificate.

4.2.3 Time to Process Certification Applications

MaxMD Direct HISP shall confirm certificate application information and requests issuance of the digital certificate within a reasonable time frame, usually within two business days after receiving all necessary details and documents from the Applicant. For LoA 3 and IAL 2 Certificates, MaxMD Direct HISP must ensure that the Applicant's identity was verified prior to the initial issuance.

4.3. Certificate issuance

4.3.1. Actions during Certificate Issuance

MaxMD Direct HISP shall verify the source of a certificate request and the identity of the Applicant in a secure manner prior to issuing a certificate.

4.3.2. Notification to Subscriber of Issuance of Certificate

MaxMD Direct HISP may deliver certificates in any secure manner within a reasonable time after issuance. Generally, the public certificate is published in DNS. The private key is not distributed. MaxMD shall notify Subscribers that the Certificate has been issued.

4.4. Certificate acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate's issuance.

4.4.2. Publication of the Certificate

End-entity certificates are published by delivering them to the HISP with notification to the Subscriber. They are then published in DNS.

4.4.3. Notification of Certificate Issuance to Other Entities

Certificates are published in DNS and may be retrieved using standard DNS query functions.

4.5. Key pair and certificate usage

4.5.1. Subscriber Private Key and Certificate Usage

MaxMD acting as HISP shall take possession of the private key and protect it from access by unauthorized parties. The Private Key shall only be used as specified in the key usage extension of the corresponding certificate. Each party with access to the Private Key is contractually obligated to protect the Private Key from unauthorized use or disclosure. The MaxMD CA generates and maintains the private key. All private keys are generated within a FIPS 140-2 level 3 Hardware Security Module. They are wrapped prior to export and then stored in a secure table. The MaxMD CA does not transport or import private keys to or from any other source.

4.5.2. Relying Party Public Key and Certificate Usage

See section 9.6.4

4.6. Certificate renewal

4.6.1. Circumstance for Certificate Renewal

MaxMD Direct HISP may authorize the renewal of a certificate if:

- the associated public key has not reached the end of its validity period,
- the Subscriber name and attributes are unchanged,
- the associated private key remains uncompromised, and
- Re-verification of the Subscriber's identity is not required under Section 3.3.1.

MaxMD Direct HISP shall make reasonable efforts to notify Subscribers via email of the imminent expiration of a digital certificate and may begin providing notice of pending expiration 60 days prior to the expiration date.

4.6.2. Who May Request Renewal

Only an authorized representative of a Subscriber as defined in Section 3.2.5 may request renewal of the Subscriber's certificates.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are the same as those used during the certificate's original issuance. MaxMD Direct HISP may not renew a certificate if it cannot verify any rechecked information. MaxMD Direct HISP may reuse identity vetting if location and Domain Name Registrar information have not changed. If the Subscriber's contact information and Private Key have not changed, the HISP may use the Subscriber's same CSR as was used for the previous certificate.

4.6.4. Notification of New Certificate Issuance to Subscriber

MaxMD Direct HISP shall notify Subscribers of renewed certificates in a secure fashion.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate's renewal.

4.6.6. Publication of the Renewal Certificate

Renewed certificates are published by delivering the certificate to the HISP on behalf of the Subscriber. All renewed certificates are published in DNS.

4.6.7. Notification of Certificate Issuance to Other Entities

MaxMD publishes renewed certificates in DNS and other entities may access them via ordinary DNS query tools.

4.7. Certificate re-key

4.7.1. Circumstance for Certificate Rekey

Re-keying a certificate consists of creating a new certificate with a new public key and serial number while keeping the subject information the same. The new certificate may have a different validity period, key identifiers, CRL and OCSP distributions, and a different signing key. After re-keying a certificate, MaxMD Direct HISP will revoke the old certificate. Essentially, MaxMD will revoke the old certificate and issue a new certificate.

4.7.2. Who May Request Certificate Rekey

The certificate subject or the Issuer CA or RA may request certificate rekey.

4.7.3. Processing Certificate Rekey Requests

If the Subscriber's other contact information and Private Key have not changed, the request may use the previously provided CSR for that Subscriber. Otherwise, the HISP must submit a new CSR for the Subscriber. MaxMD Direct HISP may re-use existing verification information unless re-verification is required under section 3.3.1 or MaxMD Direct HISP believes that the information has become inaccurate.

4.7.4. Notification of Certificate Rekey to Subscriber

MaxMD Direct HISP shall notify the Subscriber within a reasonable time after the certificate issues.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Issued certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate is rekeyed.

4.7.6. Publication of the Issued Certificate

Rekeyed certificates are published by delivering them to the HISP on behalf of the Subscribers. The HISP will continue to secure the private key and publish the public certificate in DNS.

4.7.7. Notification of Certificate Issuance to Other Entities

MaxMD publishes renewed certificates in DNS and other entities may access them via ordinary DNS query tools.

4.8. Certificate modification

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate (e.g., changes to email address or non-essential parts of names or attributes). The new certificate may have the same or a different subject public key. After modifying a certificate, MaxMD Direct HISP will revoke the old certificate. After certificate modification the old certificate shall not be further re-keyed, renewed, or modified.

4.8.1. Who May Request Certificate Modification

MaxMD Direct HISP or a Subscriber may request modification of a certificate.

4.8.2. Processing Certificate Modification Requests

Prior to requesting certificate modification, MaxMD Direct HISP shall verify any information that will change. MaxMD Direct HISP shall not request a modified certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2. The Subscriber representative shall be identity proofed as described in section 3.2

4.8.3. Notification of Certificate Modification to Subscriber

MaxMD Direct HISP shall notify the Subscriber within a reasonable time after the modified certificate issues.

4.8.4. Conduct Constituting Acceptance of a Modified Certificate

Issued certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate is rekeyed.

4.8.5. Publication of the Modified Certificate

Modified certificates are published by delivering them to the HISP on behalf of Subscribers. The HISP will continue to secure the private key and publish the public certificate in DNS.

4.8.6. Notification of Certificate Modification to Other Entities

MaxMD publishes renewed certificates in DNS and other entities may access them via ordinary DNS query tools.

4.9 Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, MaxMD Direct HISP shall verify the identity and authority of the entity requesting revocation. MaxMD Direct HISP will revoke a certificate if any of the following occur:

1. The Subscriber requested revocation of its certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the certificate or the Private Key used to sign the certificate was compromised;
4. The Subscriber or their contracted HISP breached a material obligation under the CP, the CPS, or the relevant Subscriber Agreement;
5. The Subscriber's or MaxMD Direct HISP 's obligations under the CP or CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
6. The certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
7. MaxMD Direct HISP received a lawful and binding order from a government or regulatory body to revoke the certificate;
8. MaxMD Direct HISP 's right to manage certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
9. A court or arbitrator revoked the Subscriber's right to use a name or mark listed in the certificate, or the Subscriber failed to maintain a valid registration for such name or mark;
10. Any information appearing in the Certificate was or became inaccurate or misleading;
11. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;

MaxMD Direct HISP will also revoke a certificate if the binding between the subject and the subject's public key in the certificate is no longer valid or if an associated Private Key is compromised.

4.9.2. Who Can Request Revocation

The Subscriber or another appropriately authorized party may request revocation of a certificate. MaxMD Direct HISP may require that the revocation request be made by either the organizational contact, billing contact or domain registrant.

MaxMD Direct HISP or MaxMD shall revoke a certificate if it receives sufficient evidence of compromise of or loss of the private key. Entities other than the certificate subject may request revocation of a certificate for problems related to fraud, misuse, or compromise by filing a "Certificate Problem Report". All certificate revocation requests must include the identity of the entity requesting revocation and the reason for revocation.

4.9.3. Procedure for Revocation Request

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. After receiving a revocation request:

1. MaxMD Direct HISP shall log the identity of the entity making the request or problem report and the reason for requesting revocation and submit a copy of the request to MaxMD.
2. If applicable, MaxMD Direct HISP shall confirm the revocation request with a known administrator via out-of-band communication (e.g., telephone, fax, etc.). MaxMD Direct HISP must always revoke the certificate if the request is confirmed as originating from the Subscriber.
3. If the request originated from a third party, then MaxMD Direct HISP shall investigate the report within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of complaints/reports received about a particular certificate or website,
    c. the entity making the complaint (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. relevant legislation.
4. If revocation is appropriate, MaxMD Direct HISP shall revoke the Certificate.

MaxMD Direct HISP shall maintain a continuous 24/7 ability to internally respond to any high priority complaints and problems. If appropriate, MaxMD Direct HISP may forward complaints to law enforcement.

4.9.4. Revocation Request Grace Period

All revoked certificates are immediately listed in the MaxMD CA CRL.

4.9.5. Time within which RA Processes the Revocation Request

MaxMD Direct HISP shall process all certificate revocation requests within 8 hours after their receipt.

4.9.6. Revocation Checking Requirement for Relying Parties

A relying party should check the revocation status of a certificate each time it is used.

4.9.7 CRL Issuance Frequency

A DirectTrust CRL is issued and posted to the repository listed in section 2.2.1 every 30 days when there are no changes or updates to be made to ensure timeliness of information. A CRL may be issued more frequently than every 30 days if new entries are made to the CRL. The MaxMD CA will ensure that superseded CRLs are removed from the public repository upon posting of the latest CRL. All changes to CRLs are updated immediately and are available at https://www.directmdemail.com/documents/DirectPolicy.

4.9.8 Maximum Latency of CRLs

CRLs shall be posted upon generation but within no more than four hours after generation. Furthermore, a new CRL shall be published no later than the time specified in the nextUpdate field of the most recently published CRL.

4.9.9 On-Line Revocation/Status Checking Availability

MaxMD does not deploy an Online Certificate Status Protocol (OCSP) at this time.

4.9.10 On-Line Revocation/Status Checking Requirements

MaxMD does not deploy an Online Certificate Status Protocol (OCSP) at this time.

4.9.11 Other Forms of Revocation Advertisements Available

MaxMD does not offer alternatives to the MaxMD CA CRL.

4.9.12 Special Requirements Related to Key Compromise

In the event of a Key Compromise, MaxMD shall immediately revoke the certificate and rekey a new certificate. A follow up investigation will proceed to determine the nature and extent of the compromise.

4.9.13. Circumstances for Suspension

MaxMD does not support Certificate Suspension.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate status services

4.10.1. Operational Characteristics

Certificate status information is available via CRL. MaxMD will introduce an OCSP responder when it is required.

4.10.2. Service Availability

Certificate status services are available 24x7 without interruption.

4.10.3. Optional Features

OCSP Responders are not available at this time.

4.11. End of subscription

A Subscriber's subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 Key Escrow and Recovery

MaxMD does not support Key Escrow.

4.12.1 Key Escrow and Recovery Policy and Practices

Not Applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not Applicable

5 Facility Management and Operations Controls

5.1 Physical Controls

The CA is housed at Rackspace in Fort Worth, Texas. This is a SSAE 16 Type II SOC 2* certified facility. All physical control requirements of the DirectTrust.org CP V 2.0 are met or exceeded.

5.2 Procedural Controls

The MaxMD procedure manual defines the roles required by this section of the CP.

5.2.1. Trusted Roles

Personnel acting in trusted roles include MaxMD Direct HISP's system administration personnel and personnel involved with identity vetting and the issuance and revocation of certificates. MaxMD Direct HISP has distributed the functions and duties performed by persons in trusted roles so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. MaxMD Direct HISP has ensured that all personnel in trusted roles are free from conflicts of interest that might prejudice the impartiality of MaxMD Direct HISP's operations. MaxMD Direct HISP maintains a list of personnel appointed to trusted roles and reviews this list annually. The following positions are designated as Trusted Positions; Administrator, Auditor, Officer and Operator. Definitions of the Trusted Positions are as follows;

a. Administrator- Administrators are authorized to install, configure, and maintain the Certificate Authority (CA); establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.

b. Auditor - Auditors are authorized to maintain audit logs. Auditors are responsible for reviewing, maintaining, and archiving audit logs performing and overseeing internal compliance audits to ensure that the CA is operating in accordance with its Certification Practice Statement (CPS).

c. Officer- Officers are authorized to request or approve certificates or certificate revocations, register new subscribers and request the issuance of certificates, verify the identity of Subscribers and accuracy of information included in certificates, approve and assist in the executing the issuance of certificates, and requesting, approving and executing the revocation of certificates.

d. Operator- Operators are authorized to perform system backup and recovery. System operations. Backup and Recovery is automated through our managed hosting at Rackspace.

5.2.2. Number of Persons Required per Task

Two persons are required to be trained per task.

5.2.3. Identification and Authentication for each Role

MaxMD Direct HISP requires all personnel to authenticate themselves to MaxMD Direct HISP's systems before they are allowed access to the system.

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

- The verification of information in certificate applications,
- The approval of certificate applications, and
- The approval of revocation requests.

The duties are separated between the Officer and the Administrator. Both are required to participate in the tasks above.

5.3 Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

MaxMD Direct HISP's practices provide reasonable assurance of the trustworthiness and competence of our employees and of the satisfactory performance of their duties. For DirectTrust.org LoA 3 or DirectTrust.org IAL 2 certificates, an individual performing a trusted role of the MaxMD Direct HISP must be legally eligible to work in the United States.

5.3.2. Background Check Procedures

MaxMD Direct HISP verifies the identity of each person appointed to a trusted role and performs a background check prior to allowing the person to act in a trusted role. MaxMD Direct HISP shall require each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee shall verify the individual's identity using the required forms of government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified). Background checks include employment history, education, character references, social security number, previous residences, driving records and criminal background. Background investigations are performed by a competent independent party that has the authority to perform background investigations. MaxMD Direct HISP performs checks of previous residences over the past three years. All other checks are for the previous five years. MaxMD Direct HISP verifies the highest education degree obtained regardless of the date awarded. MaxMD Direct HISP shall refresh background checks at least every ten years.

5.3.3. Training Requirements

MaxMD Direct HISP shall provide skills training to all personnel involved in PKI operations. The training relates to the person's job functions and covers:

- basic Public Key Infrastructure (PKI) knowledge,
- software versions used by MaxMD Direct HISP,

- authentication and verification policies and procedures,
- disaster recovery and business continuity procedures,
- common threats to the validation process, including phishing and other social engineering tactics, and
- Applicable industry and government guidelines.

Validation personnel must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges.

5.3.4. Retraining Frequency and Requirements

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. MaxMD Direct HISP shall make all individuals acting in trusted roles aware of any changes to MaxMD Direct HISP's operations. If MaxMD Direct HISP's operations change, MaxMD Direct HISP must provide training to all personnel acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

MaxMD has no requirement for job rotation.

5.3.6. Sanctions for Unauthorized Actions

All MaxMD Direct HISP personnel are subject to the MaxMD Disciplinary Action Policy.

5.3.7. Independent Contractor Requirements

All independent contractors working on behalf of the MaxMD Direct HISP are subject to the personnel control requirements defined in the DirectTrust.org CP V 2.0

5.3.8. Documentation Supplied to Personnel

All personnel working on behalf of the MaxMD Direct HISP will receive the MaxMD Policy Manual.

5.4 Audit Logging Procedures

5.4.1. Types of Events Recorded

MaxMD Direct HISP's systems requires identification and authentication at system logon using a unique user name and password. MaxMD Direct HISP shall enable all essential event auditing capabilities of its operations in order to record the events listed below. If an application cannot automatically record an event, MaxMD Direct HISP shall use a manual procedure to satisfy these requirements. For each event, MaxMD Direct HISP shall record the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. MaxMD Direct HISP shall make these event records available to MaxMD and MaxMD's auditors as proof of MaxMD Direct HISP's practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by remote access to the RA systems
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION
Whenever the CA generates a key
PRIVATE KEY LOAD AND STORAGE
The loading of Component Private Keys
All access to the certificate subject Private Keys retained within the CA for recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
Any change to the trusted public keys, including additions and deletions
SECRET KEY STORAGE
The manual entry of secret keys used for authentication
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CA CONFIGURATION
Any security-relevant changes to the configuration of a CA system component
CERTIFICATE STATUS CHANGE APPROVAL AND REJECTION
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
TIME STAMPING
A third-party time stamp is obtained
MISCELLANEOUS

Auditable Event
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System
Installation of a PKI Application
Installation of Hardware Security Modules
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
Backup of the internal CA database
Restoration from backup of the internal CA database
File manipulation (e.g., creation, renaming, moving)
All certificate compromise notification requests
Zeroizing HSMs
Re-key of the Component
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of the CPS or RPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

MaxMD Direct HISP shall regularly review the logs generated by MaxMD Direct HISP 's systems, make system and file integrity checks, and conduct a vulnerability assessment. During these checks, MaxMD Direct HISP shall (1) check whether anyone has tampered with the log, (2) scan for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepare a written summary of the

review. MaxMD Direct HISP shall investigate any anomalies or irregularities found in the logs. MaxMD Direct HISP shall make these logs available to MaxMD upon request.

5.4.3. Retention Period for Audit Log

MaxMD Direct HISP shall retain audit logs on-site for at least two months.

5.4.4. Protection of Audit Log

MaxMD Direct HISP personnel are required to keep all generated audit log information on their equipment until after it is copied by a MaxMD Direct HISP system administrator. MaxMD Direct HISP shall configure its systems to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period.

5.4.5. Audit Log Backup Procedures

MaxMD Direct HISP shall make backup copies of its audit logs on a monthly basis.

5.4.6. Audit Collection System (internal vs. external)

Automatic audit processes must begin on system startup and end at system shutdown. MaxMD Direct HISP shall promptly notify MaxMD if the integrity of the system or confidentiality of the information protected by a system is at risk. If a security audit system has failed MaxMD shall cease all operations except for revocation processing until the security audit capability is restored.

5.4.7. Notification to Event-causing Subject

MaxMD Administrators shall be notified of all events and shall follow notification procedures suitable to the event.

5.4.8. Vulnerability Assessments

MaxMD Direct HISP shall perform routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of its systems. MaxMD Direct HISP shall routinely assess the sufficiency of its risk control policies, procedures, information systems, technology, and other arrangements. MaxMD currently uses Rackspace Rackwatch and Alert Logic Software for intrusion detection monitoring and threat assessment reporting.

5.5 Records Archival

The MaxMD procedure manual defines the roles required by this section of the CP.

5.5.1 Types of Events Archived

1. MaxMD is EHNAC accredited as a CA RA and HISP. This can be validated on the EHNAC.ORG website. MaxMD stores locally the results of third party accreditations.
2. The MaxMD CP and CPS are available on our website at https://www.directmdemail.com/documents/DirectPolicy
3. The MaxMD CA relies upon the operation of the MaxMD RA and its Trusted Agents. The data center operations are at Rackspace.
4. System and equipment configurations are RedHat Enterprise Linux servers at Rackspace with a CISCO ASA 5525 Firewall. Intrusion detection monitoring is done in real time by Alert Logic Software. Systems Modifications are done using best practices. Modifications are tested on local machines, committed to a repository, published to a QA server at Rackspace, further tested and reviewed, and then published to production.
5. Certificate and revocation requests are reviewed by the MaxMD operations team and confirmed and signed by the ISO or his designee,
6. Identity authentication data is maintained by the RA or the Trust Agent, all data is stored securely.
7. Any documentation related to the receipt or acceptance of a certificate or token is maintained by the RA or the Trust Agent.
8. Subscriber Agreements are maintained is a version control library at MaxMD.
9. Issued certificates are published in DNS and maintained in a relational database.
10. Certificate re-keys occur by revoking the existing certificate and issuing a new certificate.
11. The MaxMD CRL is signed by the MaxMD CA certificate. It is renewed at least once every thirty days. Its URL is referenced in every certificate issued by the MaxMD CA.
12. To achieve HIPAA compliance, all messages that terminate in the MaxMD SMTP endpoint have unalterable mirrored copies in an archive folder. Every customer has the ability to zip and download their archive.
13. Compliance auditor reports are available from Rackspace after executing their NDA,
14. Any changes to the Issuer CA's audit parameters are reflected in updated versions of this CPS.
15. Audit logs are write only files that are rotated either daily or based on size. Modifications would require root access and is not permitted,
16. Key generation occurs inside the HSM. The Private Key will be wrapped by the HSM and saved in a database.
17. Access to wrapped Private Keys for key recovery purposes can be accomplished from the database backups.
18. Changes to trusted Public Keys are done by revoking certificates and reissuing them.
19. Export of Private Keys is not permitted.
20. Approval or rejection of a certificate status change request is done by review and consensus of the ISO and the HIPAA privacy officer.
21. Appointment of an individual to a trusted role is the responsibility of the MaxMD CEO.
22. Destruction of a cryptographic module shall be documented and logged by the ISO.
23. Certificate compromise notifications shall be logged and documented by the ISO. Should such occur, certificate revocation shall occur.
24. Remedial action taken as a result of violations of physical security is handled by Rackspace.
25. Violations of the CP or CPS are reviewed by the ISO and corrective action is taken as suits the violation.
26. Modifications and updates to system or configuration
27. All Audit logs

5.5.2 Retention Period for Archive

CA archives shall be kept for a minimum of seven years & 6 months.

5.5.3 Protection of Archive

Only authorized individuals shall be permitted to add to or delete from the archive. Archive media shall be stored on our Rackspace servers.

5.5.4 Archive Backup Procedures

Data on our Rackspace Servers are backed up incrementally daily and fully backed up weekly. Backups are encrypted and maintained at a secure offsite facility by Iron Mountain.

5.5.5 Requirements for Time-Stamping of Records

All records are timestamped by the system clock on the Rackspace Servers. These server times are synched to the nist.gov time server.

5.5.6 Archive Collection System (Internal vs. External)

Currently logs are SMTP logs, Tomcat logs and system log files which are maintained in place. When it becomes a consideration, a region of the Network Addressable storage unit will be allocated for Archive storage.

5.5.7 Procedures to Obtain & Verify Archive Information

Archives shall be retrieved via administrative software tools. A digest of each file will be maintained to authenticate and verify it as unchanged.

5.6 Key Changeover

The CA will not issue Subscriber certificates that extend beyond the expiration date of the MaxMD CA certificate and public keys, and the CA certificate validity period must extend one Subscriber certificate validity period past the last use of the CA private key. To minimize risk to the PKI through compromise of a CA's key, the private signing key will be changed more frequently, and only the new key will be used for certificate signing purposes from that time. The older, but still valid, certificate will be available to verify old signatures until all of the Subscriber certificates signed under it have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected. MaxMD will rekey the CA certificate at least once every ten years.

5.7 Compromise and Disaster Recovery

The MaxMD Policy manual and Business Recovery plan implement policies and procedures that meet section 5.7 of the DirectTrust.org V 2.0 CP.

5.7.1. Incident and Compromise Handling Procedures

MaxMD Direct HISP shall promptly notify MaxMD if a disaster causes MaxMD Direct HISP's operations to become inoperative.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

MaxMD Direct HISP shall reestablish operations as quickly as possible after a disaster or data corruption.

5.7.3. Entity Private Key Compromise Procedures

In the event of a private key compromise, the corresponding certificate shall be rekeyed according to procedures in section 4.7.

5.7.4. Business Continuity Capabilities after a Disaster

MaxMD Direct HISP has implemented data backup and recovery procedures. MaxMD Direct HISP Business Continuity Management Program (BCMP) that provides for the reestablishment of capabilities as quickly as possible. This plan is reviewed, and updated annually.

5.8. CA and RA Termination

In the event of CA or RA termination, certificates signed by the CA shall be revoked.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair generation is done using a FIPS 140 Level-2 HSM at Rackspace in Fort Worth, Texas. This is a SSAE 16 Type II SOC 2* certified facility.

6.1.2 Private Key Delivery to Subscriber

Private keys are not delivered to subscribers. They are wrapped by a FIPS 140 Level-2 HSM at Rackspace in Fort Worth, Texas. This is a SSAE 16 Type II SOC 2* certified facility.

6.1.3 Public Key Delivery to Certificate Issuer

In accordance with the Applicability Statement for Secure Health Transport, all public keys are contained in certificates that are published in either DNS or LDAP.

6.1.4 CA Public Key Delivery to Relying Parties

MaxMD delivers its CA to the DirectTrust.org Trust Bundle. It is also available at https://www.directmdemail.com/documents/DirectPolicy

6.1.5 Key Sizes

MaxMD follows the CP requirement for key sizes. MaxMD issues 2048 bit RSA Key with Secure Hash Algorithm 2 (SHA-256).

6.1.6 Public Key Parameters Generation and Quality Checking

MaxMD generates Public Keys via the FIPS 140-2 Bouncy Castle Library in the hardware security module.

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

The MaxMD Root certificate and MaxMD Subscriber certificates follow the requirements of the DirectTrust.org CP V 2.0.

Subscriber certificates shall assert the following key usage bits:

- digitalSignature
- keyEncipherment

Subscriber certificates that are dual-use certificates MUST not assert the contentCommitment bit. Subscriber certificates shall also assert an extended key usage bit of emailProtection and a BasicConstraint of CA:FALSE.

The CA root certificate assert the following key usage bits:

- cRLSign
- keyCertSign
- digitalSignature

The CA root certificate asserts a Basic Constraint of CA:TRUE.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

MaxMD uses a FIPS 140-2 level 3 Hardware Security Module for CA and RA cryptographic functions.
MaxMD as a HISP uses the Java Reference Implementation version 5.1.
Cryptographic modules are minimally validated to the FIPS 140 level identified below for the relevant party (or an equivalent protection):
CA Level 2
RA Level 1
HISP Level 2
Subscriber Level 1

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

No stipulation.

6.2.3 Private Key Escrow

MaxMD does not escrow private keys.

6.2.4 Private Key Backup

As per our Policy manual, MaxMD wraps private keys using a FIPS 140 Level-2 HSM at Rackspace in Fort Worth, Texas. The wrapped keys are backed up daily. Backup tapes are encrypted.

6.2.5 Private Key Archival

MaxMD does not archive private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

MaxMD private keys are generated inside a Hardware Security Module. They are wrapped with a RSA 256 secret key using AES 128 and then exported and stored inside our secure server in a MYSQL table.

6.2.7 Private Key Storage on Cryptographic Module

The MaxMD HISP protects the private keys by wrapping them using a FIPS 140-2 Level 3 Hardware Security Module.

6.2.8 Method of Activating Private Keys

MaxMD as CA shall activate Private Keys when the subscriber certificate is signed. Private Keys can only be unwrapped and activated within the Hardware Security Module. All cryptographic functions involving the Private Key are performed within the Hardware Security Module.

6.2.9 Methods of Deactivating Private Keys

MaxMD Hardware Security Module deactivates its Private Keys automatically when not in use. The HSM prevents unauthorized access to any activated cryptographic modules.

6.2.10 Method of Destroying Private Keys

Individuals in trusted roles shall destroy private signature keys when they are no longer needed. Subscriber private signature keys shall be destroyed when they are no longer needed, or when the

certificates to which they correspond are revoked.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

Public keys are archived as part of the certificate archival process.

6.3.2 Certificate Operational Periods/Key Usage Periods

The MaxMD CA private key and root certificate will expire in no more than 20 years. No subscriber key shall be used for signing for more than 6 years. Subscriber certificates shall have a maximum lifetime of 3 years.

6.4 Activation Data

The MaxMD activation process requires secure private key administrator access to the HSM at Rackspace. The activation process requires an additional activation password to sign the subscriber certificate.

6.4.1 Activation Data Generation and Installation

The MaxMD CA and MaxMD HISP generates activation data that has sufficient strength to protect its respective Private Keys. The MaxMD CA utilizes the HSM as activation data for signing keys.

6.4.2 Activation Data Protection

Only authorized personnel can initiate the activation data. Access is controlled through two factor authentication. Private key activation happens within the FIPS 140 Level-2 HSM using a partitioned password requiring at least 16 alphanumeric characters.

6.4.3 Other Aspects of Activation Data

Any subscribers whose certificates include the content commitment bit shall be authenticated to the cryptographic module prior to activation of the private key prior to each digital signature. This level of authentication requires a secure authentication protocol and multi-factor authentication process with a time-sensitive one time password.

6.5 Computer Security Controls

MaxMD participates in the Electronic Healthcare Network Accreditation Commission (EHNAC) Privacy & Security (P&S) Accreditation Program for the healthcare industry. This independent accreditation is reviewed every other year and includes a third party evaluation of MaxMD's operating environment, privacy controls, technical performance, resources, and security posture. As a part of this accreditation EHNAC performs on-site visits to both the MaxMD business office and to Rackspace.

6.5.1 Specific Computer Security Technical Requirements

MaxMD CA shall secure its systems and authenticate and protect communications between its systems and trusted roles. MaxMD CA servers and support-and-vetting workstations must run on trustworthy systems that are configured and hardened using industry best practices. MaxMD Direct HISP shall scan all systems for malicious code and protected against spyware and viruses.

The MaxMD CA shall configure its CA systems, including any remote workstations, to:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage the privileges of users and limit users to their assigned roles,
3. generate and archive audit records for all transactions,
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

The MaxMD CA shall communication between a trusted role and its CA system via private key pair using ssh.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

All software is developed in stages;

- On local workstations and then committed to a version control repository
- Code is then published from the repository to an evaluation server environment where quality assurance is performed.
- Upon management approval, the code is then published from the repository to the production environment.

6.6.2 Security Management Controls

The version control system logs all changes and provides a resource for change logging and fallback.

6.7 Network Security Controls

All information transferred from the CA is done over secure communication networks. MaxMD CA shall document and control the configuration of its systems, including any upgrades or modifications made. MaxMD CA shall protect its systems with firewall(s) and shall only use internal IP addresses. MaxMD CA

shall configure its firewalls and boundary control devices to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of its CA services.

MaxMD CA shall block all ports and protocols and open only necessary ports to enable RA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled.

6.8 Time Stamping

All system clocks are synchronized to a National Bureau of Standards time server.

7 Certificate, CRL, and OCSP Profiles Format

MaxMD conforms to the DirectTrust.org CP V 2.0 formats.

7.1 Certificate Profile

DirectTrust may, from time to time, publish definitive and authoritative Certificate Profiles that may further constrain the requirements described in this Section. MaxMD will modify our CPS to conform with requirements as they are adopted.

7.1.1 Version Numbers

MaxMD will issue X.509 v3 certificates, which means the version field shall contain the integer 2.

7.1.2 Certificate Extensions

MaxMD will use standard certificate extensions that are compliant with IETF RFC 5280. The Key Usage, Extended Key Usage, and Basic Constraints extensions shall be populated as specified in section 6.1.7 of the certificate policy. The CRL Distribution Points extension may be populated with a CRL URL as specified in section 2.2.1 of the certificate policy. The Authority Information Access extension may be populated with an OCSP Responder location as specified in section 2.2.1 of this CPS.
The Subject Alternative Name extension shall be populated as specified in section 3.1.1 of this CPS. The Certificate Policies extension shall be populated as defined in section 7.1.6 of this CPS.

7.1.3 Algorithm Object Identifiers

End Entity Certificates signed by MaxMD will use the SHA-256 signature algorithm and identify it using the following OID:
sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates issued by a MaxMD CA will use the following OID for identifying the

subject public key algorithm:
rsaEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

See section 3.1.1 of this CPS.

7.1.5 Name Constraints

No stipulation other than those specified in section 3.1.

7.1.6 Certificate Policy Object Identifier

Certificates shall assert at least one of the policy OIDs defined in section 1.2 of this CPS.

7.1.7 Usage of Policy Constraints Extension

MaxMD may add policy constraints as OIDS in the certificate.

7.1.8 Policy Qualifiers Syntax and Semantics

MaxMD may add policy constraints as OIDS in the certificate.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

This policy does not require the certificatePolicies extension to be critical. Relying Parties whose client software does not process this extension risk using certificates inappropriately.

7.2 CRL Profile

DirectTrust may, from time to time, publish definitive and authoritative CRL Profiles that may further constrain the requirements described in this section.

7.2.1 Version Numbers

The MaxMD CA issues X.509 version 2 CRLs, which means the version field should contain the integer 1.

7.2.2 CRL and CRL Entry Extensions

The MaxMD CA conforms to the CRL and CRL Extensions profile defined in IETF RFC 5280.
The MaxMD CA signs the CRL using the SHA-256 signature algorithm and identify it using the following OID:
sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

The CRL contains a CRL Reason Code entry extension for each entry.

7.3 OCSP Profile

MaxMD does not deploy an OCSP responder at this time.

8 Compliance Audits and Other Assessments

MaxMD is participant in both the EHNAC and DirectTrust.org accreditations program and submits to audits by them or their agents.

8.1 Frequency and Circumstances of Assessment

The EHNAC and DirectTrust.org audits occurs at least every two years.

8.2 Identity/Qualifications of Assessor

DirectTrust and/or EHNAC is responsible for the competence in the field of compliance audits.

8.3 Assessor's Relationship to Assessed Entity

MaxMD is a member of DirectTrust. EHNAC is an independent agency.

8.4 Topics Covered by Assessment

DirectTrust in partnership with EHNAC has an accreditation program to certify the compliance of CAs, RAs, and HISPs. This program defines the topics of the assessment.

8.5 Actions Taken as a Result of Deficiency

If an audit reports any material noncompliance with applicable law, this CPS, the RPS, the CP, or any other contractual obligations related to MaxMD Direct HISP 's services (to the extent such information is audited), then (1) MaxMD will document the discrepancy, (2) MaxMD will promptly notify MaxMD Direct HISP, and (3) MaxMD Direct HISP will develop and execute a plan to cure the noncompliance.

8.6 Communication of Results

EHNAC and DirectTrust each provide a web page for CAs to report the status/results of the compliance assessment and audit process.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

MaxMD charges Subscriber fees for certificate issuance and renewal. Such fees are detailed in applicable sales orders or agreements between MaxMD and Subscriber. MaxMD retains its right to effect changes to such fees. MaxMD customers will be suitably advised of price amendments as detailed in relevant customer agreements.

9.1.2 Certificate Access Fees

MaxMD reserves the right to establish and charge a reasonable fee for access to its database of certificates.

9.1.3 Revocation or status information access fees

MaxMD does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a MaxMD issued certificate through the use of Certificate Revocation Lists. MaxMD reserves the right to establish and charge a reasonable fee for providing certificate status information services via OCSP.

9.1.4 Fees for other services

MaxMD provides other services as part of its ongoing business. Description of those services and associated fees can be found on the MaxMD web sites (www.maxmdirect.com) or in applicable sales orders or agreements between MaxMD and Subscriber.

9.1.5 Refund policy

MaxMD's refund policy shall be defined in agreements between MaxMD and Subscriber where applicable.

9.2 Financial responsibility

9.2.1 Insurance coverage

MaxMD carries business insurance under the following policies

General Liability	
Personal Injury	$1,000,000.
General Aggregate	$2,000,000.
Products	$2,000,000.
Auto	$1,000,000.
Umbrella Liability	$9,000,000.

Workers Comp	$500,000.
Cyber Liability	$5,000,000.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

Subscribers should refer to the Subscriber Agreement that they have with MaxMD.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

MaxMD keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys
- Any activation data used to access private keys or gain access to the CA system
- Any business continuity, incident response, contingency, and disaster recovery plans
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information
- Any information held by MaxMD as private information in accordance with Section 9.4
- Any transactional, audit log and archive record identified in Section 5.4 or 5.5, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP/CPS)

9.3.2 Information not within the scope of confidential information

Subscriber application data identified herein as being published in a digital certificate is considered public and not within the scope of confidential information. Subscribers acknowledge that revocation data of all certificates issued by the MaxMD CA is public information and is periodically published every 24 hours at the MaxMD repository.

9.3.3 Responsibility to protect confidential information

MaxMD observes applicable rules on the protection of personal data deemed by law or the MaxMD privacy policy (see Section 9.4 of this CP/CPS) to be confidential.

9.4 Privacy of personal information

9.4.1 Privacy plan

MaxMD has implemented a privacy policy, which is in compliance with this CP/CPS. The MaxMD privacy policy is published at https://www.directmdemail.com/documents/PrivacyPolicy

9.4.2 Information treated as private

Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private.

9.4.3 Information not deemed private

Certificates, CRLs, and personal or corporate information appearing in them are not considered private.

9.4.4 Responsibility to protect private information

Each party shall protect the confidentiality of private information that is in its possession, custody or control with the same degree of care that it exercises with respect to its own information of like import, but in no event less than reasonable care, and shall use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information.

9.4.5 Notice and consent to use private information

A party may use private information with the subject's express written consent or as required by applicable law or court order.

9.4.6 Disclosure pursuant to judicial or administrative process

MaxMD shall not release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom MaxMD owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

9.4.7 Other information disclosure circumstances

All personnel in trusted positions handle all information in strict confidence, including those requirements of US and European law concerning the protection of personal data.

9.5 Intellectual property rights

MaxMD, its strategic partners, and other business associates, each own all their respective intellectual property rights associated with their databases, web sites, MaxMD digital certificates and any other publication originating from MaxMD including this CP/CPS.
The word “MaxMD” is a trademark of Park Ave Capital LLC. MaxMD may have other trade and service marks that have not been registered, but that nonetheless are and shall remain the property of MaxMD.
Certificates are the exclusive property of MaxMD. MaxMD gives permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. MaxMD reserves the right to revoke the certificate at any time and at its sole discretion.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Private and public keys are the property of the Subscribers.
All secret shares (distributed elements) of the MaxMD private keys remain the respective property of MaxMD.
Except as expressly stated in this CP/CPS, MaxMD makes no representations or warranties regarding its public service. MaxMD reserves its right to modify such representations as it sees fit, at its sole discretion, or as required by law. Only to the extent specified in the relevant sections of this CP/CPS, MaxMD promises to:

- Comply with this CP/CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the MaxMD Repository and web site for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue digital certificates in accordance with this CP/CPS and fulfill its obligations presented herein.
- Provide support to Subscribers and Relying Parties as described in this CP/CPS.
- Revoke certificates according to this CP/CPS.
- Provide for the expiration and renewal of certificates according to this CP/CPS.
- Make available a copy of this CP/CPS and applicable policies to requesting parties.
- Warrant the accuracy of information published on a Qualified Certificate issued pursuant to the requirements of the European Directive 99/93.
- Warrant that the signatory held the private key at the time of issuance of a certificate issued pursuant to the requirements for Qualified Certificates as in the European Directive 99/93.

MaxMD does issue Certificates for email and intranet use and disclaims any and all warranties (including name verification) for Email Certificates, Unified Communications Certificates, and other Certificates issued to individuals and intranets (e.g., where a non-public or non-standard Top Level Domain is used or where they are addressed to IP space allocated as private by RFC1918), which are not intended to be relied upon by the general public.
The Subscriber also acknowledges that MaxMD has no further obligations under this CP/CPS.

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93, MaxMD:

- Does not warrant the accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of MaxMD except as it may be stated in the relevant product description contained in this CP/CPS.
- Shall incur no liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this CP/CPS.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Shall have no liability if it cannot execute the revocation of a certificate for reasons outside its own control.
- For acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys

MaxMD requires RAs operating on our behalf to represent that they have followed this CP and the relevant CPS (or a qualifying RPS) when participating in the issuance and management of certificates. Unless otherwise stated in this CP/CPS or the applicable Subscriber Agreement, Subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring that they and their agents have adequate knowledge and training on PKI.
- To generate a secure private / public key pair to be used in association with the certificate request submitted to MaxMD.
- Ensure that the public key submitted to MaxMD is the correct one and corresponds with the private key used.
- Provide correct and accurate information in communications with MaxMD and alert MaxMD if any information originally submitted has changed since it was submitted to MaxMD.
- Use MaxMD certificates for legal and authorized purposes in accordance with this CP/CPS.
- Cease using the certificate if any information in it becomes misleading, obsolete or invalid.
- Cease using the certificate if it is expired and remove it from any applications and/or devices it has been installed on.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a MaxMD certificate.
- Request the revocation of a certificate in case of any occurrence that might materially affect the integrity of the certificate.

Without limiting other Subscriber obligations stated in this CP/CPS, Subscribers are solely liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

Upon accepting a certificate the Subscriber represents, warrants and covenants to MaxMD, to Application Software Vendors, and to Relying Parties that at the time of acceptance and until further notice:

- Transactions effectuated using the private key corresponding to the public key included in the certificate are the acts of the Subscriber and that the certificate has been accepted and is properly operational at that time and until further notice to MaxMD.
- The Subscriber retains control of the Subscriber's private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use and that no unauthorized person has ever had access to the Subscriber's private key.

- All representations made by the Subscriber to MaxMD regarding the information contained in the certificate are accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber receives notice of such information, the Subscriber shall act promptly to notify MaxMD of any material inaccuracies contained in the certificate.
- The certificate is used exclusively for authorized and legal purposes, consistent with this CP/CPS, and that the Subscriber will use the certificate only in conjunction with the entity named in the organization field of the certificate
- The Subscriber agrees with the terms and conditions of this CP/CPS and other agreements and policy statements of MaxMD.
- The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, fair trade practices and computer fraud and abuse,
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

9.6.2 RA Representations and Warranties

MaxMD requires RAs operating on our behalf to represent that they have followed the DirectTrust.org CP V 2.0 and this relevant CPS as well as the MaxMD RPS when participating in the issuance and management of certificates.

9.6.3 Subscriber Representations and Warranties

Unless otherwise stated in this CP/CPS or the applicable Subscriber Agreement, Subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring that they and their agents have adequate knowledge and training on PKI.
- To generate a secure private / public key pair to be used in association with the certificate request submitted to MaxMD.
- Ensure that the public key submitted to MaxMD is the correct one and corresponds with the private key used.
- Provide correct and accurate information in communications with MaxMD and alert MaxMD if any information originally submitted has changed since it was submitted to MaxMD
- Read, understand and agree with all terms and conditions in this CP/CPS and associated policies published in the MaxMD Repository at https://www.directmdemail.com/documents/DirectPolicy
- Use MaxMD certificates for legal and authorized purposes in accordance with this CP/CPS.
- Cease using the certificate if any information in it becomes misleading, obsolete or invalid.
- Cease using the certificate if it is expired and remove it from any applications and/or devices it has been installed on.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a MaxMD certificate.
- Request the revocation of a certificate in case of any occurrence that might materially affect the integrity of the certificate.
- For acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys

Without limiting other Subscriber obligations stated in this CP/CPS, Subscribers are solely liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.
Upon accepting a certificate the Subscriber represents, warrants and covenants to MaxMD, to Application Software Vendors, and to Relying Parties that at the time of acceptance and until further notice:

- Transactions effectuated using the private key corresponding to the public key included in the certificate are the acts of the Subscriber and that the certificate has been accepted and is properly operational at that time and until further notice by MaxMD.
- The Subscriber retains control of the Subscriber's private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use and that no unauthorized person has ever had access to the Subscriber's private key.
- All representations made by the Subscriber to MaxMD regarding the information contained in the certificate are accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber receives notice of such information, the Subscriber shall act promptly to notify MaxMD of any material inaccuracies contained in the certificate.
- The certificate is used exclusively for authorized and legal purposes, consistent with this CP/CPS, and that the Subscriber will use the certificate only in conjunction with the entity named in the organization field of the certificate
- Make reasonable efforts to acquire sufficient knowledge on using digital certificates and PKI.

9.6.4 Relying Parties Representations and Warranties

- The Subscriber agrees with the terms and conditions of this CP/CPS and other agreements and policy statements of MaxMD.
- The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, fair trade practices and computer fraud and abuse,
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

A Relying Party accepts that in order to reasonably rely on a MaxMD certificate, the Relying Party must:

- Study the limitations to the usage of digital certificates and be aware of the limitations of liability of MaxMD for reliance on a MaxMD-issued certificate.
- Verify the MaxMD certificates by referring to the relevant CRL or OCSP and also the CRLs or OCSP of any intermediate CA or root CA as available through MaxMD's repository.
- Trust a MaxMD certificate only if it is valid and has not been revoked and is unexpired.
- Read, understand and agree with all terms and conditions in this CP/CPS and associated policies published in the MaxMD Repository at https://www.directmdemail.com/documents/DirectPolicy
- Take any other reasonable steps to minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; and finally,
- Rely on a MaxMD certificate, only as may be reasonable under the circumstances, given:
- Any legal requirements for the identification of a party, the protection of the confidentiality or privacy of information, or the legal enforceability of the transaction in accordance with any laws that may apply;

- All facts listed in the Certificate, or of which the Relying Party has or should have notice, including this CP/CPS;
- The economic value of the transaction or communication, if applicable;
- The potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction or communication;
- The applicability of the laws of a particular jurisdiction, including the jurisdiction specified in an agreement with the Subscriber or in this CP/CPS;
- The Relying Party's previous course of dealing with the Subscriber, if any;
- Usage of trade, including experience with computer-based methods of trade; and
- Any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining.

9.6.5 Representations and Warranties of Affiliated Organizations

Same as 9.6.3

9.6.6 Representations and Warranties of Other Participants

Same as 9.6.4

9.7 Disclaimers of warranties

MaxMD disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law. In no event and under no circumstances (except for MaxMD's own fraud or willful misconduct) shall MaxMD be liable for any or all of the following and the results thereof:

- Any indirect, incidental or consequential damages.
- Any costs, expenses, or loss of profits.
- Any death or personal injury.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this CP/CPS.
- Any other damages except for those due to reliance, on the information featured on a certificate, or on the verified information in a certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant.
- Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CP/CPS.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or in this CP/CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses.
- Any liability that arises from compromise of a Subscriber's private key.

9.8 Limitations of liability

MaxMD certificates may only be used in connection with data transfer and transactions having a US dollar (US$) value of less than $1 million. In no event and under no circumstances (except for fraud or willful misconduct) will the aggregate liability of MaxMD, whether jointly or severally, to all parties including without any limitation a Subscriber, an applicant, a recipient, or a Relying Party for all digital signatures and transactions related to such certificate exceed $1 million.

9.9 Indemnities

By accepting or using a certificate, each Subscriber and Relying Party agrees to indemnify and hold MaxMD, as well as any of its respective parent companies, subsidiaries, directors, officers, employees, agents, and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that MaxMD, and/or the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from that party's: (i) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional; (ii) violation of the Subscriber Agreement, Relying Party Agreement, this CP/CPS, or any applicable law; (iii) compromise or unauthorized use of a Certificate or Private Key caused by the negligence of that party and not by MaxMD (unless prior to such unauthorized use MaxMD has received an authenticated request to revoke the Certificate); or (iv) misuse of the Certificate or Private Key.

9.10 Term and termination

9.10.1 Term

This CP/CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version or is otherwise terminated in accordance with this Section 9.10.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this document will be communicated via the MaxMD Repository (https://www.directmdemail.com/documents/DirectPolicy) upon termination. That communication will outline the provisions that may survive termination of this CP/CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the Validity Periods of such Certificates.

9.11 Individual notices and communications with participants

MaxMD accepts notices related to this CP/CPS by means of digitally signed messages or in paper form addressed to the locations specified in Section 2.2 of this CPS. Upon receipt of a valid, digitally signed acknowledgment of receipt from MaxMD, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed to the street address specified in Section 2.2.

9.12 Amendments

9.12.1 Procedure for amendment

Revisions not denoted “significant” shall be those deemed by the MaxMD Policy Authority to have minimal or no impact on Subscribers and Relying Parties using certificates and CRL’s issued by MaxMD. Such revisions may be made without notice to users of this CP/CPS and without changing the version number of this CP/CPS. Controls are in place to reasonably ensure that the MaxMD CPS is not amended and published without the prior authorization of the MaxMD Policy Authority.

9.12.2 Notification mechanism and period

MaxMD will notify all interested persons of proposed changes, the final date for receipt of comments, and the proposed effective date of proposed changes on its Web site. There is no fixed notice and comment period. Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact the parties may be changed without notice and are not subject to the notification requirements herein.

9.12.3 Circumstances under which OID must be changed

If a change in MaxMD's Certificate Policy or Certification Practices is determined by the MaxMD Policy Authority to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of this CP/CPS will also contain a revised OID for that type of certificate.

9.13 Dispute resolution provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, mediation, umpire, binding expert’s advice, co-operation monitoring and normal expert’s advice) the parties agree to notify MaxMD of the dispute with a view to seek dispute resolution.

9.14 Governing law

This CP/CPS is governed by, and construed in accordance with the law of the State of New Jersey. This choice of law is made to ensure uniform interpretation of this CP/CPS, regardless of the place of residence or place of use of MaxMD digital certificates or other products and services. New Jersey law

applies in all of MaxMD's commercial or contractual relationships in which this CP/CPS may apply or quoted implicitly or explicitly in relation to MaxMD products and services where MaxMD acts as a provider, supplier, beneficiary receiver or otherwise.
Each party, including MaxMD, Subscribers and Relying Parties, irrevocably agree that a tribunal (court or arbitration body) located in New Jersey shall have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CP/CPS or the provision of MaxMD PKI services.

9.15 Compliance with applicable law

This CPS shall be subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. In interpreting this CP/CPS the parties shall also take into account the international scope and application of the services and products of MaxMD as well as the principle of good faith as it is applied in commercial transactions.
The headings, subheadings, and other captions in this CP/CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CP/CPS. Appendices and definitions to this CP/CPS are for all purposes an integral and binding part of the CP/CPS. If/when this CP/CPS conflicts with other rules, guidelines, or contracts, this CP/CPS shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CP/CPS and any other document that relate to MaxMD, then the sections benefiting MaxMD and preserving MaxMD’s best interests, at MaxMD’s sole determination, shall prevail and bind the applicable parties.

9.16.2 Assignment

Parties to this CP/CPS may not assign any of their rights or obligations under this CP/CPS or applicable agreements without the written consent of MaxMD.

9.16.3 Severability

If any provision of this CP/CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CP/CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall remain in full force and effect and shall be interpreted in such manner as to implement the original intention of the parties to the fullest extent possible.
Each and every provision of this CP/CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

MaxMD reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CP/CPS, no delay or omission by any party to exercise any right, remedy or power it has under this CP/CPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach or covenant in this CP/CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. Bilateral agreements between MaxMD and the parties to this CP/CPS may contain additional provisions governing enforcement.

9.16.5 Force Majeure

MaxMD INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.17 Other provisions

This CP/CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CP/CPS applies to. The rights and obligations detailed in this CP/CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CP/CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.