

MedAllies Registration Policy (RP)

Version 1.0

Date 20 Mar 2015

## Revision History

|  |  |  |
| --- | --- | --- |
| DocumentVersion | DocumentDate | Revision Details |
| MedAllies Registration Policy | 1.0 | Initial version |
|  |  |   |

Approved by: ­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pete Palmer, Chief Security Officer, CISSP, CPHIMS

Published by

MedAllies, Inc

300 Westage Business Center Drive

Suite 320

Fishkill, NY  12524

[www.medallies.com](http://www.medallies.com/)

MedAllies, Inc.

Proprietary and Confidential

This document is proprietary and confidential information of MedAllies, and may not be reproduced or distributed without the express written consent of MedAllies

Contents

[Revision History 2](#_Toc442354017)

[1 Introduction 8](#_Toc442354018)

[1.1 Overview 8](#_Toc442354019)

[1.1.1 Relationship Between this Document and the Kantara Program 8](#_Toc442354020)

[1.2 Document Name and Identification 9](#_Toc442354021)

[1.3 RA Participants 9](#_Toc442354022)

[1.3.1 Registration Authorities (RAs) 9](#_Toc442354023)

[Trusted Agent (TA) 10](#_Toc442354024)

[1.3.2 Subscribers 11](#_Toc442354025)

[1.3.3 Relying Parties 11](#_Toc442354026)

[1.3.4 Other Participants 11](#_Toc442354027)

[1.4 Policy Administration 11](#_Toc442354028)

[1.4.1 Organization Administering the Document 11](#_Toc442354029)

[1.4.2 Contact Person 11](#_Toc442354030)

[1.4.3 Person Determining Registration Practices Statement Suitability for the Policy 12](#_Toc442354031)

[1.4.4 Registration Practices Statement Approval Procedures 12](#_Toc442354032)

[1.5 Definitions and Acronyms 12](#_Toc442354033)

[1.5.1 Acronym 12](#_Toc442354034)

[1.5.2 Definitions 12](#_Toc442354035)

[2 Publication and Repository Responsibilities 15](#_Toc442354036)

[2.1 Repositories 15](#_Toc442354037)

[2.2 Publication of Identity Information 15](#_Toc442354038)

[2.2.1 Publication of Identity 15](#_Toc442354039)

[2.2.2 Publication of RA Information 15](#_Toc442354040)

[2.3 Frequency of Publication 15](#_Toc442354041)

[2.4 Access Controls on Repositories 15](#_Toc442354042)

[3 Identification and Authentication 16](#_Toc442354043)

[3.1 Naming 16](#_Toc442354044)

[3.1.1 Meaningful Names 16](#_Toc442354045)

[3.1.2 Anonymity or Pseudonymity of Subscribers 16](#_Toc442354046)

[3.1.3 Uniqueness of Names 16](#_Toc442354047)

[3.1.4 Recognition, Authentication, and Role of Trademarks 16](#_Toc442354048)

[3.2 Initial Identity Validation 16](#_Toc442354049)

[3.2.1 Authentication of Individual Identity 16](#_Toc442354050)

[3.2.2 Change of Personal Information 20](#_Toc442354051)

[3.2.3 Non-verified Subscriber Information 21](#_Toc442354052)

[3.2.4 Validation of Authority 21](#_Toc442354053)

[3.2.5 Criteria for Interoperation 21](#_Toc442354054)

[3.3 Identification and Authentication for Revocation Requests 21](#_Toc442354055)

[4 Credential Life-Cycle 22](#_Toc442354056)

[4.1 Application 22](#_Toc442354057)

[4.1.1 Submission of Credential Application 22](#_Toc442354058)

[4.1.2 Enrollment Process and Responsibilities 22](#_Toc442354059)

[4.2 Credential Application Processing 22](#_Toc442354060)

[4.2.1 Performing Identification and Authentication Functions 22](#_Toc442354061)

[4.2.2 Approval or Rejection of Credential Applications 22](#_Toc442354062)

[4.2.3 Time to Process Certification Applications 23](#_Toc442354063)

[5 Facility Management and Operations Controls 24](#_Toc442354064)

[5.1 Physical Controls 24](#_Toc442354065)

[5.1.1 Site Location and Construction 24](#_Toc442354066)

[5.1.2 Physical Access 24](#_Toc442354067)

[5.1.3 Power and Air Conditioning 25](#_Toc442354068)

[5.1.4 Water Exposure 25](#_Toc442354069)

[5.1.5 Fire Prevention and Protection 25](#_Toc442354070)

[5.1.6 Media Storage 25](#_Toc442354071)

[5.1.7 Waste Disposal 25](#_Toc442354072)

[5.2 Procedural Controls 25](#_Toc442354073)

[5.2.1 Trusted Roles 25](#_Toc442354074)

[5.2.2 Number of Persons Required Per Task 27](#_Toc442354075)

[5.2.3 Identification and Authentication for Each Role 27](#_Toc442354076)

[5.2.4 Separation of Roles 27](#_Toc442354077)

[5.3 Personnel Controls 28](#_Toc442354078)

[5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements 28](#_Toc442354079)

[5.3.2 Background Check Procedures 28](#_Toc442354080)

[5.3.3 Training Requirements 28](#_Toc442354081)

[5.3.4 Retraining Frequency and Requirements 28](#_Toc442354082)

[5.3.5 Job Rotation Frequency and Sequence 29](#_Toc442354083)

[5.3.6 Sanctions for Unauthorized Actions 29](#_Toc442354084)

[5.3.7 Independent Contractor Requirements 29](#_Toc442354085)

[5.3.8 Documentation Supplied to Personnel 29](#_Toc442354086)

[5.4 Audit Logging Procedures 29](#_Toc442354087)

[5.4.1 Types of Events Recorded 29](#_Toc442354088)

[5.4.2 Frequency of Processing Log 31](#_Toc442354089)

[5.4.3 Retention Period for Audit Logs 32](#_Toc442354090)

[5.4.4 Protection of Audit Logs 32](#_Toc442354091)

[5.4.5 Audit Log Backup Procedures 32](#_Toc442354092)

[5.4.6 Audit Collection System (internal vs. external) 32](#_Toc442354093)

[5.4.7 Notification to Event-Causing Subject 32](#_Toc442354094)

[5.4.8 Vulnerability Assessments 32](#_Toc442354095)

[5.5 Records Archival 32](#_Toc442354096)

[5.5.1 Types of Events Archived 32](#_Toc442354097)

[5.5.2 Retention Period for Archive 33](#_Toc442354098)

[5.5.3 Protection of Archive 33](#_Toc442354099)

[5.5.4 Archive Backup Procedures 33](#_Toc442354100)

[5.5.5 Requirements for Time-Stamping of Records 33](#_Toc442354101)

[5.5.6 Archive Collection System (Internal vs. External) 34](#_Toc442354102)

[5.5.7 Procedures to Obtain & Verify Archive Information 34](#_Toc442354103)

[5.6 Compromise and Disaster Recovery 34](#_Toc442354104)

[5.6.1 Incident and Compromise Handling Procedures 34](#_Toc442354105)

[5.6.2 Computing Resources, Software, and/or Data Are Corrupted 34](#_Toc442354106)

[5.6.3 Business Continuity Capabilities after a Disaster 34](#_Toc442354107)

[5.7 Not used 34](#_Toc442354108)

[5.8 RA Termination 34](#_Toc442354109)

[6 Technical Security Controls 36](#_Toc442354110)

[6.1 Computer Security Controls 36](#_Toc442354111)

[6.1.1 Specific Computer Security Technical Requirements 36](#_Toc442354112)

[6.1.2 Computer Security Rating 36](#_Toc442354113)

[6.2 Life-Cycle Security Controls 36](#_Toc442354114)

[6.2.1 System Development Controls 36](#_Toc442354115)

[6.2.2 Security Management Controls 36](#_Toc442354116)

[6.2.3 Life Cycle Security Ratings 37](#_Toc442354117)

[6.3 Network Security Controls 37](#_Toc442354118)

[6.4 Time Stamping 37](#_Toc442354119)

[7 Compliance Audits and Other Assessments 38](#_Toc442354120)

[7.1 Frequency and Circumstances of Assessment 38](#_Toc442354121)

[7.2 Identity/Qualifications of Assessor 38](#_Toc442354122)

[7.3 Assessor’s Relationship to Assessed Entity 38](#_Toc442354123)

[7.4 Topics Covered by Assessment 38](#_Toc442354124)

[7.5 Actions Taken as a Result of Deficiency 38](#_Toc442354125)

[7.6 Communication of Results 39](#_Toc442354126)

[8 Other Business and Legal Matters 40](#_Toc442354127)

[8.1 Fees 40](#_Toc442354128)

[8.1.1 Identity Proofing Fees 40](#_Toc442354129)

[8.1.2 Fees for other Services 40](#_Toc442354130)

[8.1.3 Refund Policy 40](#_Toc442354131)

[8.2 Financial Responsibility 40](#_Toc442354132)

[8.2.1 Insurance Coverage 40](#_Toc442354133)

[8.2.2 Other Assets 40](#_Toc442354134)

[8.2.3 Insurance/Warranty Coverage for End-Entities 40](#_Toc442354135)

[8.3 Confidentiality of Business Information 40](#_Toc442354136)

[8.3.1 Scope of Confidential Information 40](#_Toc442354137)

[8.3.2 Information not within the scope of Confidential Information 40](#_Toc442354138)

[8.3.3 Responsibility to Protect Confidential Information 40](#_Toc442354139)

[8.4 Privacy of Personal Information 41](#_Toc442354140)

[8.4.1 Privacy Plan 41](#_Toc442354141)

[8.4.2 Information Treated as Private 41](#_Toc442354142)

[8.4.3 Responsibility to Protect Private Information 41](#_Toc442354143)

[8.4.4 Notice and Consent to Use Private Information 41](#_Toc442354144)

[8.4.4.1 Compliance with FICAM Privacy Policies 41](#_Toc442354145)

[8.4.5 Disclosure Pursuant to Judicial/Administrative Process 42](#_Toc442354146)

[8.4.6 Other Information Disclosure Circumstances 42](#_Toc442354147)

[8.5 Intellectual Property Rights 42](#_Toc442354148)

[8.6 Representations and Warranties 42](#_Toc442354149)

[8.6.1 RA Representations and Warranties 42](#_Toc442354150)

[8.6.2 RA Representations and Warranties 42](#_Toc442354151)

[8.6.3 Relying Parties Representations and Warranties 42](#_Toc442354152)

[8.6.4Representations and Warranties of Affiliated Organizations 42](#_Toc442354153)

[8.6.5 Representations and Warranties of Other Participants 42](#_Toc442354154)

[8.7 Disclaimers of Warranties 42](#_Toc442354155)

[8.8 Limitations of Liabilities 43](#_Toc442354156)

[8.9 Indemnities 43](#_Toc442354157)

[8.10 Term and Termination 43](#_Toc442354158)

[8.10.1 Term 43](#_Toc442354159)

[8.10.2 Termination 43](#_Toc442354160)

[8.10.3 Effect of Termination and Survival 43](#_Toc442354161)

[8.11 Individual Notices and Communications with Participants 43](#_Toc442354162)

[8.12 Amendments 43](#_Toc442354163)

[8.12.1 Procedure for Amendment 43](#_Toc442354164)

[8.12.2 Notification Mechanism and Period 43](#_Toc442354165)

[8.13 Dispute Resolution Provisions 43](#_Toc442354166)

[8.14 Governing Law 44](#_Toc442354167)

[8.15 Compliance with Applicable Law 44](#_Toc442354168)

[8.16 Miscellaneous Provisions 44](#_Toc442354169)

[8.16.1 Entire Agreement 44](#_Toc442354170)

[8.16.2 Assignment 44](#_Toc442354171)

[8.16.3 Severability 44](#_Toc442354172)

[8.16.4 Enforcement (Attorney Fees/Waiver of Rights) 44](#_Toc442354173)

[8.16.5 Force Majeure 44](#_Toc442354174)

[8.17 Other Provisions 44](#_Toc442354175)

# 1 Introduction

This Registration Policy (RP) addresses the policies related to the identity proofing of individuals seeking level-3, 2-factor non-PKI identity credentials as defined under NIST Special Publication 800-63, the Kantara Identity Assurance Framework and the US Federal Identity Credentialing and Access Management (FICAM) programs. The proofing performed under this policy is done to verify to the maximum feasible extent in accordance with NIST and FICAM requirements that the individual seeking a credential is actually the person they purport to be. Specific steps required as part of the proofing process are included in Section 3.2 of this policy. In addition, the policies described herein comply with the identity proofing requirements of the US Federal Public Key Infrastructure (FPKI).

The terms and provisions of this document shall be interpreted under and governed by applicable Federal and State laws and regulations.

## 1.1 Overview

This document describes the requirements under which the MedAllies Registration Authority identity proofing process operates. MedAllies operates its RA in the United States of America and may provide services in all 50 states.

The MedAllies Program Manager has responsibility for approving this policy and any updates to it. Any use of or reference to this policy outside the context of MedAllies is completely at the risk of the relying party.

### 1.1.1 Relationship Between this Document and the Kantara Program

Kantara has the responsibility to determine that the MedAllies policies and processes are comparable to one or more of the Kantara trust framework models. This process provides assurance to all Relying Parties (RPs) of the validity, and thus dependability, of the MedAllies identity proofing process.

The determination is performed by a Kantara Registered Assessor and is based on the Kantara Trust Framework (KTF model) at the required levels of assurance. During this assessment, the following information is reviewed:

1. **Identity proofing policies** that establish the degree of certainty an identity service provider has about a user’s legal identity.
2. **Security policies** that establish the degree to which the integrity and confidentiality of identity information is protected**.**
3. **Privacy policies** that establish the degree of control a user has over how their identity information is used and shared.
4. **Survivability policies** that establish the degree to which a user’s identity data remains both portable and protected.

The Kantara Trust Framework has been certified by the US Federal Identity, Credentialing and Access Management (FICAM) program as being Trust Framework Provider for US ICAM LOA 1, 2, and 3.

Kantara provides a trust framework against which identity service providers can operate and be certified in order to issue US FICAM credentials at one or more levels of assurance. Once certified, service providers shall be placed on a “White List” of approved non-PKI Credential issuers for the FICAM community.

The FICAM White List shall be used by Relying Parties to confirm that the service provider has been certified to issue non-PKI Credentials to the LOA to which they are certified. This profile defines the assurance level claims that indicate trust within the FICAM community at the corresponding level of assurance (LOA):

* Assurance Level 1

http://idmanagement.gov/icam /2009/09/imi\_1.0\_profile#assurancelevel1

* Assurance Level 2

http://idmanagement.gov/icam /2009/09/imi\_1.0\_profile#assurancelevel2

* Assurance Level 3

http://idmanagement.gov/icam /2009/09/imi\_1.0\_profile#assurancelevel3

## 1.2 Document Name and Identification

This RP defines the requirements for identity proofing of applicants for MedAllies non-PKI, 2-factor authentication credentials issued at NIST levels of assurance 1-3.

## 1.3 RA Participants

The following are roles relevant to the administration and operation of this service.

### 1.3.1 Registration Authorities (RAs)

Registration Authorities (RA) operate identity management systems (IdMs) and collect and verify Subscriber information on MedAllies behalf. MedAllies may act as its own RA or may delegate or subcontract the collection of identity proofing to an agent that has executed an RA agreement. There shall be a clear contractual trust relationship between the RA and the managing credential service provider. Mutual service provision obligations and requirements shall be clearly delineated in the contract between the entities. All communications between component service providers shall be secure and encrypted.

RAs collect and verify identity information from Subscribers using procedures that implement the identity validation policies set forth in this document. When MedAllies delegates RA activities to a Local Registration Authority (LRA), it monitors their compliance with this document and the MedAllies Registration Practices Statement (RPS) under which the RA operates.

A client Trusted Agent (TA) may be appointed by MedAllies to carry out these roles. The TA is legally bound by their organization to carry out actions pertaining to identity proofing as a proxy for the RA. MedAllies clients sign legal contracts and identify the parties responsible for providing such services and the mechanisms for determining their trustworthiness according to this policy.

The first Registration Authorities (RAs) within the system must be vetted by MedAllies, per the process described for all RAs.

MedAllies RAs shall enroll in person. Organizational LRAs/TAs shall enroll in person or via videoconference call with a MedAllies RA. The authentication for these Subscribers is documented by a signed declaration by the Trusted Role personnel that they personally verified the identity of the Subscriber.

This declaration must be maintained by the MedAllies RA.

##### Local Registration Authorities/Trusted Agents

Within subscriber organizations, the Trusted Role is the Local Registration Authority (LRA), which acts as the RA for that organization.

The Trusted Agent (TA) performs a more limited role as defined below.

The LRA and TA shall be enrolled utilizing the same process as the RA, defined above.

### Trusted Agent (TA)

A Trusted Agent is a person who is accountable for Subscriber Identity verification during the registration process. The TA is generally authorized to serve a limited population of Subscribers, based on logical or geographical organization.

##### End User Subscribers

Similar to LRAs, end user Subscribers will enroll in person with the appropriate RA/LRA/TA for their organization. MedAllies clients are responsible for implementing the MedAllies Trusted Agent Policies as described in the MedAllies Trusted Agent Agreement and must participate in a MedAllies developed Trusted Agent Training.

### 1.3.2 Subscribers

A Subscriber is the entity whose name appears as the subject in a credential and who signs a Subscriber Agreement with MedAllies. Subscriber Agreements shall be reaffirmed at periodic intervals but no less than every five years.

### 1.3.3 Relying Parties

A Relying Party uses a Subscriber’s credential to verify the identity of the Subscriber. A Relying Party is the entity that relies on the validity of the binding of the Subscriber’s name to a credential. The Relying Party is responsible for deciding whether or how to check the validity of the credential.

### 1.3.4 Other Participants

The RA will work in support of a full service Credential Service Provider (CSP) which may be MedAllies itself or a third party. The RA may also work in support of a component service Token Manager that provides the actual token to the Subscriber. If the RA and TM/CSP are remotely located and communicate over a network, the entire registration transaction between the RA and TM/CSP shall occur over a mutually authenticated protected session. In all cases, Approved cryptography is required.

## 1.4 Policy Administration

### 1.4.1 Organization Administering the Document

The MedAllies Registration Authority (RA) is responsible for this document. MedAllies may amend this Policy, or any part thereof, at any time, at its discretion. Prior to any amendment of this RP, MedAllies will provide notice of any proposed change in writing to all using clients and its Credential Service Provider and may specify a review period in any such notice.

### 1.4.2 Contact Person

Questions regarding this policy should be directed to:

Pete Palmer, CISSP, CPHIMS

Chief Security Officer

MedAllies, Inc.

300 Westage Business Center Drive

Suite 320

Fishkill, NY  12524

Work - 845.896.0191 Cell - 845-264-4087

ppalmer@medallies.com

### 1.4.3 Person Determining Registration Practices Statement Suitability for the Policy

The MedAllies program manager shall approve the RPS.

The determination of the compliance of the RPS to this Policy shall be based on an independent compliance auditor’s results and recommendations.

### 1.4.4 Registration Practices Statement Approval Procedures

MedAllies submits the RPS to a compliance analysis and audit against this Policy as described in Section 7. MedAllies will not declare conformance between this Policy and the RPS until the compliance analysis and audit is complete and any discrepancies are resolved.

## 1.5 Definitions and Acronyms

### 1.5.1 Acronym

|  |  |
| --- | --- |
| **Acronym** | **Meaning** |
| ID  | Identity |
| ONC HIT | Office of the National Coordinator for Health IT |
| RP | Registration Policy |
| RPS | Registration Practice Statement |
| RAPP | Registration Authority Proofing Policy |
| POC  | Point of Contact |
| RA | Registration Authority |

### 1.5.2 Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Applicant | A party undergoing the process of registration and identity proofing.  |
| Authentication | Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information. [NS4009] |
| Credential | A credential is an object that authoritatively binds an identity to a token possessed and controlled by a Subscriber. Credentials are used to validate the token used by the Subscriber and establish the identity of the Subscriber. |
| Face-to-face | To identify an individual, and confirm by means of their proof of identity documents that they are who they claim to be, through an in-person meeting between the individual and a trusted registration agent.  In most major companies, a person-to-person meeting will be part of the employment process (e.g., performed by the Human Resources, Information Technology (security) or Medical Staff credentialing functions within the company), and is an allowable antecedent process for identity-proofing purposes. |
| I&A | Identification and Authentication: A process for the establishment of the identity of an end-user to the assurance level specified in the NIST 800-63 standard. |
| Identity Proofing | The process by which an Issuer and an RA validate sufficient information to uniquely identify a person.  |
| Relying Party (RP) | A relying party is an organization that uses your credential to verify your identity and to authenticate you to their websites or applications.  |
| Registration Authority (RA)  | A trusted entity that establishes and vouches for the identity of a Subscriber to an Issuer. The RA may be an integral part of an Issuer, or it may be independent of an Issuer, but it has a relationship to the Issuer.  |
| Subscriber | A parity who has received a Credential and token from an Issuer.  |
| Token | Something that the Subscriber possess and controls (e.g. a key, OTP device, password, etc.) used to authenticate the Subscriber’s identity.  |
| Trusted Agent | A Trusted Agent is a person who is accountable for Subscriber Identity verification during the registration process. |

# 2 Publication and Repository Responsibilities

## 2.1 Repositories

The MedAllies RA shall operate repositories in support of operations required by this Policy.

The mechanisms supported and operated are detailed in the MedAllies RPS.

Repositories holding identity status data are operated 24 hours a day, 7 days a week with a minimum of 99% availability overall per year.

## 2.2 Publication of Identity Information

### 2.2.1 Publication of Identity

The MedAllies RA shall maintain a repository containing the artifacts of the identity proofing process. In some cases, this repository may be maintained by a MedAllies client that uses the Trusted Agent process for identity proofing. In such cases, the maintaining entity is responsible for compliance with the terms of this policy and such compliance shall be assured under terms of the contract for service between MedAllies and the client. The client entity shall be subject to the same periodic audit requirements under this policy as MedAllies.

### 2.2.2 Publication of RA Information

The MedAllies RA shall publish information necessary to support its operation and use. Information on how to obtain a copy of this Policy shall be provided to any party with legitimate interest.

## 2.3 Frequency of Publication

An updated version of this Policy, and any ensuing changes, shall be made available on the MedAllies website within 30 days of incorporation of changes.

## 2.4 Access Controls on Repositories

The MedAllies RA shall protect repository information not intended for public dissemination or modification. The RA shall provide unrestricted read access to its repositories for legitimate uses and implement logical and physical controls to prevent unauthorized write access to such repositories.

# 3 Identification and Authentication

## 3.1 Naming

### 3.1.1 Meaningful Names

For LOA 2 and LOA 3 Credentials, the RA shall record the actual Subscriber’s name in a manner that can be unequivocally associated with the credential and the identity that it asserts. All names associated with a Subscriber shall be meaningful, i.e., names used in credentials must be understandable, human readable and unambiguous by relying parties.

### 3.1.2 Anonymity or Pseudonymity of Subscribers

For LOA 2 and LOA 3 Credentials, MedAllies shall not support anonymous or pseudonymous names.

### 3.1.3 Uniqueness of Names

RAs shall ensure that each Subscriber’s identity is unique and uniquely associable with the tokens and/or credentials issued to that identity.

### 3.1.4 Recognition, Authentication, and Role of Trademarks

Subscriber registration is under the auspices of the MedAllies RAs and Organizational LRAs.

MedAllies shall resolve any name collisions or disputes regarding identities verified under this Policy brought to its attention. MedAllies will not verify an identity knowing that it infringes upon the trademark of another organization. The RA must reject any application or require revocation of any credential that is part of a trademark dispute.

## 3.2 Initial Identity Validation

In order to obtain a Credential, all Subscribers shall apply for a credential, and identify and authenticate themselves to the MedAllies RA or the appropriate organizational LRA. This section covers the identity proofing requirements for each LOA. Multiple types of identity credentials may be issued to end user subscribers through one identity-proofing event. The identity-proofing performed shall meet the level of assurance of the higher credential issued. Specific procedures are identified in the RPS.

### 3.2.1 Authentication of Individual Identity

3.2.1.1 Authentication of Human Subscribers

**For Level of Assurance 1 (LOA 1)**

There are no identity-proofing requirements.

**For Level of Assurance 2 (LOA 2)**

The identity may be established by in-person proofing before a Registration Authority or Trusted Agent. The applicant must be in possession of a valid current primary Government Picture ID that contains Applicant’s picture, and either address of record or nationality of record (e.g. driver’s license or Passport) shall be required. The RA/TA shall inspect the photo-ID, compare picture to Applicant, and record ID number, address and date of birth (DOB). If the photo ID appears valid and the photo matches Applicant and if the ID confirms the address of record, the RA authorizes the CSP shall issue credentials and notice shall be sent to the address of record; OR if ID does not confirm address of record, the CSP shall issue credentials in a manner that confirms the claimed address. The ID may also be established remotely by verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases.

In both person to person and remote processes the TA/RA shall confirm that: name, Date of Birth (DoB), address and other personal information in records are consistent with the application and sufficient to identify a unique individual.

Examples of documents accepted for identity proofing are included in Exhibit 1.

A Registration Agent (either RA, LRA or TA) shall record the information set forth below for issuance of each verified identity:

* The identity of the Registration Agent performing the identification;
* A signed declaration by the Registration Agent that he or she verified the identity of the Subscriber. This declaration shall use the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable format under non-US law;
* Unique ID number(s) provided by the Subscriber, or other unique ID number(s) that are linked directly to the Subscriber, and the names of the databases from which the number(s) were verified;
* The date and time of the verification; and
* A declaration of identity signed by the Subscriber using a handwritten signature and performed in the presence of the person performing the identity authentication using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or a comparable procedure under local law.

Identity shall be established through the initial identity-proofing process at least once every fifteen (15) years.

**For Level of Assurance 3 (LOA 3)**

Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or National Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. Credentials required are either one National Government-issued Picture I.D., or two Non-National Government I.D.s, one of which shall be a photo I.D. (e.g., Driver’s License). Any credentials presented shall be unexpired.

Examples of documents accepted for identity proofing are included in Exhibit 1.

A Registration Agent (either RA, LRA or TA) shall record the information set forth below for issuance of each verified identity:

* The identity of the Registration Agent performing the identification;
* A signed declaration by the Registration Agent that he or she verified the identity of the Subscriber. This declaration shall use the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable format under local law;
* A unique identifying number(s) from the ID(s) of the Subscriber (or some other trusted source of information on the Subscriber), or a facsimile of the ID(s);
* The date and time of the verification; and
* A declaration of identity signed by the Subscriber using a handwritten signature and performed in the presence of the person performing the identity authentication using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or a comparable procedure under local law.

Identity shall be established through the initial identity-proofing process at least once every nine (9) years.

**For Both LOA 2 and LOA 3**

Identity shall be established no more than 30 days before initial credential issuance.

An entity certified by a National or State Government as being authorized to confirm identities may perform person-to-person identity-proofing on behalf of the RA or LRA. The certified entity, TA, or the applicant shall forward the information collected directly to the RA or LRA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such identity-proofing does not relieve the RA and LRA of its responsibility to verify the presented data.

In-person identity proofing may be supported using video teleconferencing if the following criteria are met:

* the video resolution is sufficient to allow the Trusted Agent to view and copy the identifying information from the proffered identity document without assistance from the applicant;
* the persons communicating must simultaneously see and speak to one another; the signal transmission must be live and in real time; and
* the signal transmission must be secure from interception by persons other than the persons communicating.

Exhibit : Acceptable Identification Credentials

**U.S. BASED -LIST OF ACCEPTABLE DOCUMENTS**

Identity Proofing

(All Documents MUST be Unexpired)

|  |  |  |
| --- | --- | --- |
| **List A****Documents that establish both identity & employment eligibility** | **List B****Documents that Establish Identity** | **List C****Documents that Establish Employment Eligibility** |
| **1.** U.S. Passport (unexpired or expired) | **1.** Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address | **1.** U.S. Social Security card issued by the Social Security Administration *(other than a card stating it is not valid for employment)* |
| **2.** Permanent Resident Card or Alien Registration Receipt Card (FormI-551) | **2.** ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address | **2.** Certification of Birth Abroad issued by the Department of State *(Form FS-545 or Form DS-1350)* |
| **3.** An unexpired foreign passport with a temporary I-551 stamp | **3.** School ID card with a photograph | **3.** Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal |
| **4.** An unexpired Employment Authorization Document that contains a photograph(Form I-766, I-688, I-688A, I-688B) | **4.** Voter's registration card | **4.** Native American tribal document |
| **5.** An unexpired foreign passport with an unexpired Arrival-Departure Record, Form I-94, bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, if that status authorizes the alien to work for the employer | **5.** U.S. Military card or draft record | **5.** U.S. Citizen ID Card *(Form I-197)* |
|  | **6.** Military dependent's ID card | **6.** ID Card for use of Resident Citizen in the United States *(Form I-179)* |
|  | **7.** U.S. Coast Guard Merchant Mariner Card | **7.** Unexpired employment authorization document issued by DHS *(other than those listed under List A)* |
|  | **8.** Native American tribal document | **For persons under age 18 who are unable to present a document listed above:** |
|  | **9.** Driver's license issued by a Canadian government authority | **10.** School record or report card |
|  |  | **11.** Clinic, doctor or hospital record |
|  |  | **12.** Day-care or nursery school record |

**Illustrations of many of these documents appear in Part 8 of the Handbook for Employers (M-274)**

### 3.2.2 Change of Personal Information

Any changes to personal information (e.g., name change due to marriage/divorce) shall be authenticated by review of documentation substantiating the change. The TA/RA shall review and process such information according to provisions of the RPS and shall notify the TM/CSP if approved changes for credential revision if necessary.

### 3.2.3 Non-verified Subscriber Information

All Subscriber information included in a MedAllies credential must be verified and a credential issued within 30 days of completion of verification.

### 3.2.4 Validation of Authority

The MedAllies RA must validate individuals who are authorized to represent the Client during the application process by ensuring that the individual is the POC for that Client.

### 3.2.5 Criteria for Interoperation

This RP shall be mapped to and conform to the Kantara Service Assessment requirements. The Interoperating TM/CSP shall adhere to the following requirements:

* Operate a credential issuance service that has undergone a successful compliance audit.
* Provide SAML authentication assertions compliant with the ICAM profiles.

## 3.3 Identification and Authentication for Revocation Requests

Revocation requests shall be authenticated.

# 4 Credential Life-Cycle

## 4.1 Application

MedAllies or a Subscriber official credential signing request must provide sufficient information as required for a MedAllies credential in order to:

* Establish the applicant’s authorization from the employing or sponsoring organization to obtain the credential;
* Establish and recording the identity of the applicant;

### 4.1.1 Submission of Credential Application

MedAllies or a Subscriber shall create the credential request based on input received from the Subscriber as validated by the MedAllies RA during the identity verification process.

### 4.1.2 Enrollment Process and Responsibilities

A Subscriber is responsible for providing accurate information about himself and his organization during identity verification. The MedAllies RA is responsible for ensuring that the identity of each Applicant is verified in accordance with this RP and its corresponding RPS prior to the issuance of a credential. The MedAllies RA authenticate and protect all communication made during the credential application process.

## 4.2 Credential Application Processing

The MedAllies RA is responsible for verifying that the information in a credential request is accurate and reflects the information presented by the Subscriber.

### 4.2.1 Performing Identification and Authentication Functions

The identity verification of Subscribers is performed MedAllies RA as specified in [section 3.2](#_3.2_Initial_Identity) using procedures detailed in the applicable registration practices statement (RPS). The RA, LRA or TA shall verify new or updated Subscriber personal information. For example, if an individual’s name changes (e.g., due to marriage), then proof of the name change shall be validated using the initial identity proofing processes as defined in Section 3.2.. The RA, LRA or TA shall securely notify the TM/CSP and confirm the validation result prior to the modification of the credential

### 4.2.2 Approval or Rejection of Credential Applications

A credential application may be rejected by the MedAllies RA due to missing or inaccurate information. The RA retains the right to reject MedAllies credential applications if, in its judgment, the requesting individual or organization does not have a legitimate reason to possess a MedAllies credential.

### 4.2.3 Time to Process Certification Applications

All Subscriber information placed in a MedAllies credential is verified and a credential is issued within 30 days of completion of verification.

# 5 Facility Management and Operations Controls

## 5.1 Physical Controls

The MedAllies RA equipment is protected from unauthorized access at all times.

### 5.1.1 Site Location and Construction

The location and construction of the facility housing the RA equipment must be consistent with facilities used to house proprietary and sensitive computer systems and networks. The location and construction provides robust protection against unauthorized access to the RA equipment and records. At all times, all personnel gaining access to the facility must pass through the building’s security checkpoint.

### 5.1.2 Physical Access

The RA equipment must always be protected from unauthorized access with appropriate access control mechanisms. Entry must be restricted to only those trained individuals that require it for their job responsibilities. All doors to the facility are monitored with cameras. The doors are equipped with proximity card readers.

The MedAllies RA facility shall be secured in a two-person control manner. A locked cabinet/rack houses the RA Server. The two-person control is attained by separation of access responsibilities. The Trusted Roles present whenever the RA is accessed must sign the “secure access list” which is checked by the auditor during the weekly audits and retained as part of the logs available during the annual Compliance audit.

Both the Administrator and Officer must remain in the room while access to RA equipment is unlocked. The Officer may never be left in the room without escort.

All access into and out of the RA equipment room shall be recorded in a manual log.

A security check of the facility housing the RA equipment or remote workstations used to administer the RA shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

* The equipment is in a state appropriate to the current mode of operation.
* Any security containers are properly secured.
* Physical security systems (e.g., door locks, vent covers) are functioning properly.
* The area is secured against unauthorized access.

At least two individuals must be assigned for each Trusted Role (Auditor, Officer and Administrator).

### 5.1.3 Power and Air Conditioning

The RA equipment may be attached to redundant UPSs to allow for a graceful shutdown in the event of power failure. The data center should have a backup generator that can run on fuel for three days. Should excessive heat build-up occur in the physical surroundings of the RA equipment, procedures must be in place to prevent equipment damage through alerts and fire deterrent systems.

### 5.1.4 Water Exposure

RA equipment shall be installed such that it is not in danger of exposure to water. Water exposure from fire suppression systems is excluded from the requirement.

### 5.1.5 Fire Prevention and Protection

RA equipment shall be protected from fire by certified dry chemical fire prevention/suppression systems at the hosting center.

### 5.1.6 Media Storage

RA media must be stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information shall be duplicated on redundant disks and stored in a secure location separate from the RA equipment. This storage is restricted to authorized custodians.

### 5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed by a commercial disposal company. De-commissioned hard drives shall be stored in a locked room until they are handed over to the commercial disposal company. Chain of custody documents shall be maintained describing who had possession of the media until its final destruction.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security or operational incidents if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles are responsible for the integrity of the MedAllies RA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The MedAllies RA defines its trusted personnel in terms of four roles.

1. Administrator – authorized to install, configure, and maintain the RA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. Officer – authorized to request or approve credentials and credential revocations.
3. Auditor – authorized to maintain audit logs.
4. Operator – authorized to perform system backup and recovery.

Some roles may be combined. The following subsections provide a detailed description of the responsibilities for each role.

#### 5.2.1.1 Administrator

The administrator role is responsible for:

 Installation, configuration, and maintenance of the RA,

 Establishing and maintaining RA system accounts,

 Configuring credential profiles or templates and audit parameters.

#### 5.2.1.2 Officer

The officer role is responsible for issuing credentials, that is:

 Verifying the identity of Subscribers and accuracy of information included in credentials,

 Approving the issuance of credentials, and requesting and approving the revocation of credentials.

#### 5.2.1.3 Auditor

The auditor role is responsible for:

 Reviewing, maintaining, and archiving audit logs, and

 Performing or overseeing internal compliance audits to ensure that the RA is operating in accordance with the RPS.

#### 5.2.1.4 Operator

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

### 5.2.2 Number of Persons Required Per Task

At least two people are trained for each task but only one is required to execute each task. To best ensure the integrity of MedAllies equipment and operation, no individual will be assigned more than one Trusted Role, with the exception of Operator. Since an Administrator is required to gain access to the MedAllies RA facilities, at least one of the participants will always be an Administrator.

Only an Officer has access to the locked racks containing RA equipment. Therefore, both an Administrator and an Officer are required for any task associated with MedAllies RA activation and backup.

Under no circumstances does MedAllies RA perform its own auditor function.

### 5.2.3 Identification and Authentication for Each Role

A person occupying a trusted role must authenticate himself to the RA system using MedAllies credential.

At the operating system level, authentication is done by system logon controlled by account authentication in Active Directory. Trusted Roles are given role-based access control on the system enforced by security groups in Active Directory. Administrators have local and domain administrator rights on the systems (with separate accounts providing those rights).

Officers are also identified and authenticated by the RA database via accounts assigned to the Officer role.

### 5.2.4 Separation of Roles

Any individual may assume the Operator role. No one individual assumes both the Officer and Administrator roles. The operator role may be assumed by the Administer. Audit log data is generated automatically by MedAllies for all RA activities.

## 5.3 Personnel Controls

### 5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles must be selected on the basis of loyalty, trustworthiness, and integrity. All trusted roles are required to be held by persons who are legally eligible to work in the United States.

Personnel security procedures must be in place, which include separation of duties, least privilege, and individual accountability to mitigate internal security risks due to the actions of personnel as outlined in [NIST SP 800-53].

### 5.3.2 Background Check Procedures

RA personnel shall pass a background check in the following areas:

* Employment;
* Education;
* Place of residence;
* Law Enforcement; and
* References.

These checks are repeated every 5 years for RA personnel.

### 5.3.3 Training Requirements

Persons in a Trusted Role shall receive comprehensive training in all aspects of the role they perform. All persons have a reasonable understanding of PKI principles and operations.

Training shall be conducted, and training records maintained, in the following areas:

* RA security principles and mechanisms;
* All software versions in use on the RA system;
* All RA duties they will perform;
* Disaster recovery and business continuity procedures; and
* Stipulations of this RP and associated RPS.

### 5.3.4 Retraining Frequency and Requirements

Individuals responsible for Trusted Roles must be made aware of changes in RA operation. Any significant change to the operations has a training (awareness) plan, and the execution of such plan is documented. Examples of such changes are MedAllies RA software or hardware upgrades, changes in automated security systems, and relocation of equipment. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

### 5.3.5 Job Rotation Frequency and Sequence

No stipulation.

### 5.3.6 Sanctions for Unauthorized Actions

MedAllies shall take appropriate administrative and disciplinary actions against personnel who violate this RP.

### 5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the RA must meet the personnel requirements set forth in this RP.

### 5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role. If there are changes made to that role, that person will be notified in a secure manner.

## 5.4 Audit Logging Procedures

Audit log files are generated for all events relating to the security of the RA. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits. Audit entries must be clearly labeled with date/time period information of the data contained in the record. System clocks shall be kept synchronized via a trusted time server. System logs shall be automatically time stamped.

Formal audit and accountability policies and procedures have been developed and documented, and are periodically updated.

### 5.4.1 Types of Events Recorded

A message from any source received by the MedAllies RA requesting an action related to the operational state of the RA is an auditable event. At a minimum, each audit record must include the following (either recorded automatically or manually for each auditable event):

 The type of event,

 The date and time the event occurred,

 A success or failure indicator, where appropriate,

 The identity of the entity and/or operator (of the MedAllies RA) that caused the event,

Detailed audit requirements are listed in the table below. All security auditing capabilities of the RA operating system and RA applications required by this RP are enabled. As a result, most of the events identified in the table are automatically recorded. Where events cannot be automatically recorded, the MedAllies RA implements manual procedures to satisfy this requirement.

|  |  |  |
| --- | --- | --- |
|  | Manual | Automatic |
| **SECURITY AUDIT** |  |  |
| Any changes to the audit parameters, e.g., audit frequency, type of event audited | **X** |  |
| Any attempt to delete or modify the audit logs |  | **X** |
| AUTHENTICATION TO SYSTEMS |  |  |
| Successful and unsuccessful attempts to assume a role |  | **X** |
| The value of maximum number of authentication attempts is changed |  | **X** |
| Maximum number of unsuccessful authentication attempts reached during user login |  | **X** |
| An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts |  | **X** |
| An administrator changes the type of authenticator, e.g., from a password to a biometric | **X** |  |
| LOCAL DATA ENTRY |  |  |
| All security-relevant data that is entered in the system |  | **X** |
| REMOTE DATA ENTRY |  |  |
| All security-relevant messages that are received by the system |  | **X** |
| DATA EXPORT AND OUTPUT |  |  |
| All successful and unsuccessful requests for confidential and security-relevant information |  | **X** |
| CREDENTIAL REGISTRATION |  |  |
| All credential requests, including issuance and renewal | **X** |  |
| CREDENTIAL REVOCATION |  |  |
| All credential revocation requests | **X** |  |
| RA CONFIGURATION |  |  |
| Any security-relevant changes to the configuration of a RA system component | **X** |  |
| ACCOUNT ADMINISTRATION |  |  |
| Roles and users are added or deleted | **X** |  |
| The access control privileges of a user account or a role are modified |  | **X** |
| MISCELLANEOUS |  |  |
| Appointment of an individual to a Trusted Role | **X** |  |
| Installation of an Operating System | **X** |  |
| Installation of a RA Application | **X** |  |
| System Startup | **X** | **X** |
| Logon attempts to RA Application | **X** | **X** |
| Attempts to set passwords | **X** | **X** |
| Attempts to modify passwords |  | **X** |
| Backup of the internal RA database |  | **X** |
| Restoration from backup of the internal RA database | **X** |  |
| All credential compromise notification requests | **X** |  |
| CONFIGURATION CHANGES |  |  |
| Hardware | **X** |  |
| Software | **X** |  |
| Operating System | **X** | **X** |
| Patches | **X** | **X** |
| PHYSICAL ACCESS / SITE SECURITY |  |  |
| Known or suspected violations of physical security | **X** |  |
| ANOMALIES |  |  |
| System crashes and hardware failures |  | **X** |
| Software error conditions |  | **X** |
| Software check integrity failures |  | **X** |
| Network attacks (suspected or confirmed) |  | **X** |
| Equipment failure |  | **X** |
| Violations of a CP or CPS | **X** |  |
| Resetting Operating System clock | **X** | **X** |

### 5.4.2 Frequency of Processing Log

Audit logs must be reviewed and monitored regularly to ensure that any irregularities are identified and handled properly. Review of this log must occur once every two months.

### 5.4.3 Retention Period for Audit Logs

Security audit log data is available on the RA equipment for a minimum of two months. Audit logs shall be retained on-site until reviewed, in addition to being archived as described in section 5.5. Audit logs shall be stored onsite until the next audit (weekly) then moved to the Interim Storage Area.

### 5.4.4 Protection of Audit Logs

Only authorized personnel who require access for the performance of their job responsibilities may have access to the logs, and the right to archive the logs. Access rights management systems and processes enforce these requirements.

RA system configuration and procedures shall be implemented together to ensure that only authorized people archive or delete security audit data.

### 5.4.5 Audit Log Backup Procedures

Security audit data should be backed up monthly and stored off-site in a secure location.

### 5.4.6 Audit Collection System (internal vs. external)

All security audit processes shall be invoked at RA startup and cease only at shutdown. Should it become apparent that an automated security audit system has failed; the RA ceases all operation except for revocation processing until the security audit capability can be restored.

### 5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited.

### 5.4.8 Vulnerability Assessments

The RA shall be subjected to the same vulnerability assessments as other critical systems. External vulnerability assessments should also be performed.

### 5.5 Records Archival

### 5.5.1 Types of Events Archived

RA archive records must be sufficiently detailed as to verify that the RA was properly operated as well as to verify the validity of any credential throughout its validity period. At a minimum, the following data must be archived:

1. Any accreditation of the MedAllies RA,

2. All applicable RP and RPS versions,

3. Contractual obligations and other agreements concerning the operation of the RA,

4. System and equipment configurations, modifications, and updates,

5. Credential and revocation requests,

6. Identity authentication data,

7. Subscriber Agreements,

9. Any data or applications necessary to verify an archive’s contents,

10. Compliance auditor reports,

11. Any attempt to delete or modify audit logs,

12. Appointment of an individual to a trusted role,

13. Remedial action taken as a result of violations of physical security, and

14. Violations of the RP or RPS.

### 5.5.2 Retention Period for Archive

RA archives must be kept for a required period of 20 years and 6 months.

### 5.5.3 Protection of Archive

Only authorized individuals shall be permitted to add to or delete from the archive. Archive media must be stored in a separate, safe, secure storage facility.

The contents of the archive shall not be released except as determined by MedAllies or as required by law.

### 5.5.4 Archive Backup Procedures

The applicable RPS shall describe how the archive records are backed up, and how these backups are managed.

### 5.5.5 Requirements for Time-Stamping of Records

Records must be clearly labeled with date/time period information of the data contained in the record. System clocks shall be kept synchronized via a trusted time server. System logs shall be automatically time stamped.

### 5.5.6 Archive Collection System (Internal vs. External)

The archive information shall be collected by the Auditor, who (using a checklist) is responsible for assuring that all records required for archive are correctly filed.

### 5.5.7 Procedures to Obtain & Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store the RA archive information shall be published in the applicable RPS.

## 5.6  Compromise and Disaster Recovery

### 5.6.1 Incident and Compromise Handling Procedures

If a hacking attempt or other form of potential compromise of the MedAllies RA becomes known, it shall be investigated in order to determine the nature and the degree of damage.

In the event of a suspected compromise, MedAllies shall notify interested parties, including Kantara and subscriber organizations to make them aware of the situation and the ongoing investigation. Once impact has been determined MedAllies will provide this information to the same parties and will provide remediation actions as well as schedule for these actions to be completed.

### 5.6.2 Computing Resources, Software, and/or Data Are Corrupted

The MedAllies RA shall maintain backup copies of system, databases, and private keys in order to rebuild the RA capability in case of software and/or data corruption. Prior to resuming operations, the RA must ensure that the system’s integrity has been restored.

### 5.6.3 Business Continuity Capabilities after a Disaster

In the case of a disaster in which the RA equipment is damaged and inoperative, the RA operations shall be reestablished as soon as possible.

## 5.7 Not used

## 5.8 RA Termination

In the event the MedAllies RA terminates operations, credentials based on MedAllies ID proofing must be revoked.

MedAllies will continue to protect all collected and maintained PII in a secure manner for the required period of seven years post credential expiration or revocation.

Entities shall be given as much advance notice as circumstances permit, and attempt to provide alternative sources of interoperation will be sought in the event the MedAllies RA is terminated.

# 6 Technical Security Controls

## 6.1 Computer Security Controls

### 6.1.1 Specific Computer Security Technical Requirements

The MedAllies RA shall configure its 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 RA shall authenticate and protect all communications between a trusted role and its RA system using a PIN Entry Device. All communication between the Remote PED and the RA shall be transmitted within an AES-256 encrypted channel using session keys based on secrets shared out-of-band via the Remote PED role.

### 6.1.2 Computer Security Rating

No stipulation.

## 6.2 Life-Cycle Security Controls

### 6.2.1 System Development Controls

The RA software shall be developed using FIPS-certified libraries. The software shall be maintained in a controlled development environment with modern source code control. All RA hardware and software must be dedicated to performing RA tasks. Hardware and software updates shall be tested and installed in a professional and controlled manner. As part of the configuration management methodology, MedAllies will develop an Annual Release Plan for use in controlling configuration.

### 6.2.2 Security Management Controls

The configuration of the RA system as well as any modifications and upgrades shall be documented and controlled. A formal configuration management methodology will be used for installation and ongoing maintenance of the RA system. As part of the configuration management methodology, MedAllies will develop an Annual Release Plan for use in controlling configuration.

### 6.2.3 Life Cycle Security Ratings

The MedAllies RA operates under standard maintenance.

## 6.3 Network Security Controls

Information transferred from the RA shall be done through dedicated removable media or secure networks. The RA should employ appropriate security measures to ensure it is guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers.

## 6.4 Time Stamping

System clock time for the RA systems must be derived from an external trusted time service. Asserted times shall be accurate to within three minutes.

# 7 Compliance Audits and Other Assessments

The MedAllies RA shall have a compliance audit mechanism in place to ensure that the requirements of this RP and the applicable RPS are being implemented and enforced. This practice does not impose a requirement for any particular audit assessment methodology—it may be an internal audit process or it may use a compliance auditor that is independent from the entity being audited.

## 7.1 Frequency and Circumstances of Assessment

The compliance audit should occur annually. The MedAllies RA must arrange, initially and annually, for independent inspections and compliance audits to validate that the MedAllies RA is operating in accordance with the security practices and procedures described in this RP.

## 7.2 Identity/Qualifications of Assessor

Every compliance auditor must demonstrate competence in the field of compliance audits. The RA compliance auditor must be thoroughly familiar with the requirements which the RA imposes on the performance of identity proofing.

## 7.3 Assessor’s Relationship to Assessed Entity

The Compliance Auditor must be independent from MedAllies. This contracted individual will provide an unbiased, independent evaluation of the MedAllies facility and operations. To ensure further objectivity, the Compliance Auditor must not have served MedAllies in developing or maintaining the MedAllies facility, operations, or this RP or the applicable RPS.

## 7.4 Topics Covered by Assessment

MedAllies RA must undergo compliance audits to ensure that the applicable RPS is in conformance with this RP. The compliance audit will address all aspects of the MedAllies RA for a given year.

## 7.5 Actions Taken as a Result of Deficiency

The MedAllies RA may not be granted the right to claim conformance with reference to this RP unless they are in full compliance with its provisions and requirements.

## 7.6 Communication of Results

An Audit Compliance Report shall be provided to the entity responsible for RA operations. The Compliance Auditor must notify MedAllies of the results of the compliance audit within 24 hours of the audit’s completion. Results of the audit shall be maintained securely and protected against loss for a minimum of 36 months after completion.

# 8 Other Business and Legal Matters

## 8.1 Fees

### 8.1.1 Identity Proofing Fees

No stipulation

### 8.1.2 Fees for other Services

No stipulation.

### 8.1.3 Refund Policy

No stipulation.

## 8.2 Financial Responsibility

### 8.2.1 Insurance Coverage

No stipulation.

### 8.2.2 Other Assets

No stipulation.

### 8.2.3 Insurance/Warranty Coverage for End-Entities

No stipulation.

## 8.3 Confidentiality of Business Information

### 8.3.1 Scope of Confidential Information

The RA shall specify what constitutes confidential information in its RPS.

### 8.3.2 Information not within the scope of Confidential Information

The MedAllies RA treats any information not listed as confidential in its RPS as public information.

### 8.3.3 Responsibility to Protect Confidential Information

The RA shall contractually obligate employees, agents, and contractors to protect confidential information. The RA may provide training to employees on how to handle confidential information.

### 8.4 Privacy of Personal Information

### 8.4.1 Privacy Plan

The RA shall develop, implement and maintain a privacy plan. The privacy plan shall document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

### 8.4.2 Information Treated as Private

The RA shall protect all subscriber’s personally identifying information from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by RAs operating under this policy shall not be released except as allowed by the privacy plan.

Information included in credentials is not deemed private.

### 8.4.3 Responsibility to Protect Private Information

The MedAllies RA shall store private information securely.

### 8.4.4 Notice and Consent to Use Private Information

The MedAllies RA shall use private information only as dictated by the agreements with its Subscribers.

### 8.4.4.1 Compliance with FICAM Privacy Policies

Although the strict FICAM requirements related to privacy, i.e., adequate notice, minimalism and activity tracking, apply more fully to the Credential Service Provider, the MedAllies RA Subscriber Agreement shall include the following provisions to comply with FICAM Privacy requirements:

##### 8.4.4.1.1 Termination

The Subscriber agreement shall include language regarding how the RA will protect and manage personally identifiable information (PII) collected during identity proofing. This information will also be included in a formal privacy plan for the RA

##### 8.4.4.1.2 Opt In

The Subscriber agreement shall include an explanation of the PII collected during identity proofing with an explanation of its use and purpose for collection. The Subscriber shall be offered the option to opt in/out but must be informed that failure to opt in will result in cessation of credential processing.

### 8.4.5 Disclosure Pursuant to Judicial/Administrative Process

The MedAllies RA must not disclose private information unless allowed by agreements with its Subscribers or unless required to by law.

### 8.4.6 Other Information Disclosure Circumstances

No stipulation.

## 8.5 Intellectual Property Rights

The MedAllies RA will not knowingly violate the intellectual property rights held by others.

## 8.6 Representations and Warranties

### 8.6.1 RA Representations and Warranties

The MedAllies RA must represent to Subscribers, and Relying Parties that they comply, in all material aspects, with the RPS, the related RP, and all applicable laws and regulations. The MedAllies RA operates under the legal provisions of the State of New York.

### 8.6.2 RA Representations and Warranties

The MedAllies RA must require RAs operating on their behalf to represent that they have followed this RP and the applicable RPS) when participating in the issuance and management of credentials.

### 8.6.3 Relying Parties Representations and Warranties

No stipulation.

### 8.6.4Representations and Warranties of Affiliated Organizations

No stipulation.

### 8.6.5 Representations and Warranties of Other Participants

No stipulation.

## 8.7 Disclaimers of Warranties

No stipulation.

## 8.8 Limitations of Liabilities

The MedAllies RA limits its liability to any extent not otherwise prohibited by the applicable RPS, provided that it remains responsible for complying with this RP.

## 8.9 Indemnities

No stipulation.

## 8.10 Term and Termination

### 8.10.1 Term

This credential policy becomes effective when approved. This credential policy has no specified term.

### 8.10.2 Termination

Termination of this credential policy may occur if approved.

### 8.10.3 Effect of Termination and Survival

The assertions made within registration policy remain in effect through the end of the archive period of the last credential issued.

## 8.11 Individual Notices and Communications with Participants

No stipulation.

## 8.12 Amendments

### 8.12.1 Procedure for Amendment

This RP may be amended.

### 8.12.2 Notification Mechanism and Period

No stipulation.

## 8.13 Dispute Resolution Provisions

In the event of any dispute related to this credential policy, a statement of guidance may be issued and published on the MedAllies website if approved through the MAPA consensus process.

## 8.14 Governing Law

The laws of the United States of America shall govern this Policy.

Where an inter-governmental dispute occurs, resolution shall be according to the terms of the MOA.

## 8.15 Compliance with Applicable Law

All PKI participants must comply with applicable laws.

## 8.16 Miscellaneous Provisions

### 8.16.1 Entire Agreement

No stipulation.

### 8.16.2 Assignment

No stipulation.

### 8.16.3 Severability

Should it be determined that one section of this credential policy is incorrect or invalid, the other sections of this credential policy remains in effect until the certification practice statement is updated.

### 8.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

### 8.16.5 Force Majeure

No stipulation.

## 8.17 Other Provisions

No stipulation.