



**DECLARATION OF IDENTITY (DOID) FORM**

**FOR DIRECT IDENTITY VERIFICATION AND AUTHORIZATION**

|  |  |  |  |
| --- | --- | --- | --- |
| *Service Provider* | HISP Name: Orion Health on behalf of Mass HIway | Telephone: +1 800 905 9151 |  |
|  |  |  |
| Address: Evans Office Complex, Building C, Suite C-100, 7350 | Account #: 080088 |  |
| East Evans Rd, Scottsdale, Arizona 85260 |  |  |
|  |  |
|  |  |  |  |
|  |  |  |
| *Organization* | Organization (legal Business Name): | Main Telephone: |  |
|  |  |  |
| Address: |  |  |
|  |  |  |
| HIPAA Compliance: |  |  |
| ⎕ | HIPAA covered entity |  |  |
|  ⎕ | HIPAA Business Associate |  |  |
| ⎕ | Other HIPAA Entity - Health-care organization that treats protected health information with privacy and |  |
|  | security protections that are equivalent to those required by HIPAA. |  |
| *Applicant* | Applicant Name: | Personal Telephone: |  |
|  |  |  |
| Home Address: | Personal Email: |  |
|  |  |  |  |
|  |  |  |
| Date of Birth: |  |  |
|  |  |  |  |
|  Work Address: |  Work Phone:  |  |
|  Title:  |  Work Email:  |  |

By signing this document, I hereby 1) state that I am the Access Adminstrator (in accordance with Section 7 of the [Mass HIway Policies and Procedures](http://www.masshiway.net/HPP/cs/groups/hpp/documents/document/cgfu/zhbz/~edisp/hiway_pandps_v4.pdf)) or an authorized Officer of the Organization listed above; and 2) agree to the attached authorization, request a Direct Certificate and declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **/** | **/** | **,** | **:** | am/pm |
| Applicant Signature | Date and Time |  |  |  |

**To the Applicant: Please have a notary witness your signature on page 1 of this document. The notary also must complete and sign the acknowledgement on page 2. Pages 1 and 2 of the completed form should then be returned to the Mass HIway in accordance with the enclosed instructions.**

**SEE PAGE 3 FOR IMPORTANT INSTRUCTIONS TO THE NOTARY AND APPLICANT FOR COMPLETING THIS SECTION AND THE IDENTITY VERIFICATION PROCESS**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *Identification #1* | Type of Document: |  |  | Photo: | Y | N |  |
|  |  |  |  |
|  |  |  |  |  |  |  |
| Issued By: |  | Serial #: |  |  |  |
|  |  |  |  |  |  |
| Name on ID#1: |  | Expiration Date: |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| *Identification #2* | Type of Document: |  |  | Photo: | Y | N |  |
|  |  |  |  |
|  |  |  |  |  |  |  |
| Issued By: |  | Serial #: |  |  |  |
|  |  |  |  |  |  |
| Name on ID#2: |  | Exp. Date: |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |
| **NOTARIAL ACKNOWLEDGEMENT****Notary must sign, date, and stamp this section.** |  |
| STATE/COMMONWEALTH OF \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ } |  |  |  |
|  |  | } |  |  |  |  |  |
| COUNTY/PARISH OF \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | } |  |  |  |  |  |

I hereby certify under penalty of perjury under the laws of the United States of America that at the above-indicated date and time, personally appeared before me, the above-named Applicant, who signed the foregoing document in my presence, and who presented the identification listed above, affixed hereto, which I did review for authenticity.

|  |  |
| --- | --- |
| WITNESS my hand \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | and official seal |
|  |  |  | Notary Signs Here |  |  |  |
| Date and Time | **/** | **/** | **,** | **:** |  | am/pm |
|  |  |  |  |  |  |  |  |
| Print Name |  |  |  |  |  |  | Organization / |
|  |  |  |  |  |  |  | Employer |
| Telephone: |  |  |  |  |  |  | Email: |
|  |  |  |  |  |  |  |  |

**INSTRUCTIONS TO APPLICANT/NOTARY:**

Required identification consists of one original, unexpired Federal Government‐issued Photo I.D. (List A)- OR- two unexpired Non‐Federal Government I.D.s (List B and C), one of which must be a Photo I.D. (List B).

List A ‐ Acceptable Federal Photo IDs include: a current passport, a permanent resident card, Global Entry or passport card, employment authorization document (Form I‐766), a REAL ID driver’s license/ID card, or a military ID card. *Driver’s licenses and ID cards from non‐REAL‐ID‐Act compliant* *states are allowed only under List B. See https://www.dhs.gov/real‐id‐enforcement‐brief*.

List B ‐ Acceptable Other Photo IDs, when presenting two unexpired non‐Federal Government IDs

(one of which must be a photo ID), include: a non‐REAL‐ID‐Act‐compliant Driver’s License/state issued

ID Card, a driver’s license/ID card issued by a Canadian government authority, a School ID

card with a photograph, a military dependent’s ID card, Native American tribal ID card, or other ID

card issued by a federal, state or local government agency, provided that it contains a photograph.

List C – Acceptable Secondary Forms of ID include, in addition to a photo ID on List B, include: a

social security card, birth certificate, a recent utility bill, a recent financial account statement

(redaction allowed), a carry permit, voter registration card, or other similar identity document.

Unacceptable forms of secondary ID include: any club/organization membership card (Elks, Sam’s

Club/Costco), library card, marriage license (except to establish new surname).

**NOTE TO THE APPLICANT:**

Only pages 1-2 of this Form will need to be submitted to the Mass HIway. You will not need to submit copies of your identity documents to the Service Provider. These documents are for use by the notary only.

**IMPORTANT INFORMATION FOR THE NOTARY:**

**DIGICERT MUST SPEAK WITH THE NOTARY DIRECTLY WITHIN 30 DAYS OF THE NOTARIZED DATE FOR VERIFICATION.**

Please note the following:

* Please complete organization/employer, telephone, and email. Digicert is required to contact you at your place of business to get a verbal confirmation of your signature and seal.
* The telephone number should be listed on a trusted third party source for ease of verification of the notary by Digicert.
* Digicert will attempt to contact you by phone at least once a day for 30 days from the date above from the following number: 801-701-9600.
* Digicert may use email for notary verification only if the email address is verified on one of these two ways: 1) it is listed on a trusted third-party source; OR 2) if a contact reached by Digicert at a verifiable number for the organization/employer listed gives the email address for the notary directly.

****

**AUTHORIZATION FOR ISSUANCE OF GROUP CERTIFICATE(S)**

DigiCert, Inc. **(“ DigiCert”**) issues X.509 v.3 digital certificates **(“ Certificates”**) for the Direct Trust program

(https://www.directtrust.org/). Group Certificates are issued under the Direct Trust program either as “Address

Certificates” or as “Organizational Certificates”. By signing the declaration of identiy form, you agree, for each Certificate issued to you or your organization **(“ Applicant”** or **“Organization”**), that your Direct Trust service provider **(“ Service Provider”**) may perform joint‐custodian certificate‐related duties that are normally performed directly by Certificate subjects. These tasks include managing keys, registering devices, authenticating personnel with DigiCert and its certificate systems, and installing, configuring, and managing Certificates. By signing the declaration of identity form, Applicant hereby agrees and authorizes DigiCert as follows:

1. Certificates. Service Provider may request and approve Certificates in Applicant’s name and manage Certificates for Applicant’s benefit. DigiCert may issue, refuse to issue, revoke, or restrict access to Certificates in accordance with the instructions provided by the Service Provider and rely on these instructions as if originating from Applicant.
2. Representations. Applicant represents that the Organization is a HIPAA Covered Entity, a HIPAA Business Associate, or a health‐care organization that treats Protected Health Information with privacy and security protections that are equivalent to those required by HIPAA, HITECH, and implementing regulations (“HIPAA”). The Organization must protect any information transferred via Direct Exchange using this Certificate in accordance with privacy and security protections that are equivalent to those required by HIPAA.
3. Authorization. Applicant explicitly appoints Service Provider’s employees and agents as Applicant’s agent for the purpose of requesting, using, and managing Certificates and corresponding private keys. These employees and agents are authorized to fulfill all obligations imposed by DigiCert with respect to the Certificates, communicate with DigiCert regarding the management of key sets and Certificates, and fulfill all roles related to certificate issuance. Applicant hereby authorizes these agents to (i) request Address Certificates and Organizational Certificates for Direct addresses and domains owned or controlled by the Organization or its affiliates, (ii) request Certificates naming the Organization or its equipment, employees, agents, or contractors as the Certificate’s subject, and (iii) accept terms and conditions related to Certificates issued on Applicant’s behalf.
4. Trusted Agent. In addition, an Applicant submitting a signed declaration of identity is hereby appointed as a “Trusted Agent” of DigiCert for the purpose of collecting documentation, verifying identities, and providing identity information to DigiCert. Any identity information provided by other applicants for Certificates must be verified by Trusted Agents in accordance with instructions provided by DigiCert. The requirements for identity verification are set by the applicable certificate policy, which may change, and DigiCert will amend the instructions provided to its Trusted Agents at such time if necessary.
5. Documentation. DigiCert may rely on this authorization and accompanying information to issue subsequent Certificates on Applicant’s behalf. DigiCert is solely responsible for determining what information and documents are required to issue a Certificate. Applicant agrees to provide, at all times, accurate, complete, and true information to DigiCert. If any information provided to DigiCert changes or becomes misleading or inaccurate, then Applicant agrees to promptly update the information. Applicant consents to (i) DigiCert’s disclosure of information embedded in an issued Certificate, and (ii) DigiCert’s transfer of Applicant’s information to DigiCert’s servers, which are located inside the United States. DigiCert shall follow the privacy policy posted on its website when receiving and using information from Applicant. DigiCert may modify the privacy policy in its sole discretion.
6. Representation. The signer of the declaration of identity form represents that he or she has the authority to provide this authorization as the Organization’s Access Administrator in accordance with Section 7 of the [Mass HIway Policies and Procedures](http://www.masshiway.net/HPP/cs/groups/hpp/documents/document/cgfu/zhbz/~edisp/hiway_pandps_v4.pdf) or as an authorizedOfficer of the Organization and, if applicable, bind the signer’s represented Organization by its terms. By submitting documentation to DigiCert, Applicant represents to DigiCert that (i) Applicant has verified any named individual’s name, address, email address, telephone number, birthdate, and any other information required by DigiCert and in accordance with any instructions provided by DigiCert, (ii) Applicant has examined any relied upon documents for modification or falsification and believes that the documents are legitimate and correct, and (iii) Applicant is unaware of any information that is reasonably misleading or that could result in a misidentification of the verified entity or person. These representations survive termination of this authorization until all Certificates that rely on documentation provided by Applicant expire.
7. Duration. This authorization lasts until revoked by Applicant. Applicant may revoke the authorization by sending an email message revoking the authorization to: legal@digicert.com. Even after revocation, all representations and obligations relied on for Certificates issued prior to DigiCert’s receipt of the revocation survive until the Certificates expire or are revoked by DigiCert. DigiCert may require that Applicant periodically renew this authorization by resubmitting a copy of this authorization to DigiCert.
8. Certificate Revocation and Termination. DigiCert will revoke any Certificate issued on Applicant’s behalf after receiving a verified certificate revocation request from Applicant. DigiCert may also revoke a Certificate issued for any reason and without notice.
9. Warranty Disclaimers. DIGICERT SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE”. DIGICERT EXPRESSLY DISCLAIMS ALL OTHER EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON‐INFRINGEMENT. DigiCert may modify or discontinue specific service or product offerings at any time. Nothing herein requires DigiCert to provide Certificates or other related services to Applicant.
10. Limitation on Liability. DIGICERT IS PROVIDING THESE SERVICES TO APPLICANT UNDER AN AGREEMENT BETWEEN THE SERVICE PROVIDER AND DIGICERT. DIGICERT’S LIABILITY FOR CERTIFICATES UNDER THIS AUTHORIZATION IS LIMITED TO THE AMOUNT SPECIFIED IN ITS AGREEMENT WITH THE SERVICE PROVIDER, WHICH LIMITS APPLY EQUALLY TO THE CERTIFICATES ISSUED UNDER THIS AGREEMENT. APPLICANT ACCEPTS THIS LIMITATION ON LIABLIITY, ACKNOWLEDGES THAT THE SERVICE PROVIDER IS RESPONSIBLE FOR ANY USE OF THE CERTIFICATE, AND WAIVES ANY RIGHT AGAINST DIGICERT FOR USE OF DIGICERT’S SERVICES, INCLUDING THE ISSUANCE OR USE OF CERTIFICATES. DIGICERT IS NOT LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNATIVE DAMAGES OR ANY LOSS OF PROFIT, REVENUE, DATA, OR OPPORTUNITY, EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this authorization were breached or proven ineffective.
11. Notices . Applicant must send all notices (i) in writing, (ii) with delivery confirmation via first class mail, commercial overnight delivery service, facsimile transmission, email, or by hand, and (iii) addressed to DigiCert, Inc., Attn: Legal Department, 2600 West Executive Parkway, Suite 500, Lehi, Utah 84043, email: legal@digicert.com, fax: 1‐866‐842‐0223. DigiCert may change its address for notices by sending notice of the change to the Service Provider. All notices to DigiCert are effective on receipt. The Service Provider is solely responsible for conveying notices to Applicant. DigiCert will deliver notices to Applicant by delivering the notice to the Service Provider. Notices are effective when sent to the Service Provider in accordance with DigiCert’s agreement with the Service Provider.
12. Severability. The invalidity or unenforceability of a provision under this authorization, as determined by an arbitrator, court, or administrative body of competent jurisdiction, does not affect the validity or enforceability of the remainder of this authorization. The parties shall substitute any invalid or unenforceable provision with a valid or enforceable provision that achieves the same economic, legal, and commercial objectives as the invalid or unenforceable provision.
13. Intended Beneficiaries . The Service Provider and DigiCert are express and intended beneficiaries of Applicant’s obligations and representations under this authorization.