INSTRUCTIONS

The attached form must be completed, signed, and returned before your service provider can create your Direct certificate and use the certificate to securely transmit health care information between providers. Failing to follow these instructions may delay the certificate's issuance.

To complete this form, you must either (a) sign this document using a FBCA Medium or higher assurance certificate issued in your name or (b) bring this document to a notary or trusted agent so they can verify your identity and signature. Your service provider is a trusted agent and will tell you whether a notary or trusted agent is the appropriate choice. Signing with an FBCA Medium or higher assurance certificate is uncommon.

Unless you are signing with a FBCA Medium or higher assurance certificate, you must present, during the verification process, a government-issued photo ID that lists your name and address to verify your identity. A second ID is required if the ID is not a federal government ID or REAL state ID. The second ID does not need to be a government-issued ID. The notary or trusted agent must see you sign this document and attest to the signature. If you have moved within the last year, please attach a copy of a utility bill to confirm your new address.

Examples of acceptable photo ID documents include a passport, driver's license, military ID, permanent resident card, or similar document. Examples of acceptable secondary ID documents include a social security card, birth certificate, school ID, or voter's registration card.

Feel free to call us at 1-800-896-7973 with any questions or concerns. Our support staff is available 24x7 to assist you.

IDENTITY VERIFICATION AND AUTHORIZATION

Applicant	Name:	Telephone:
	Home Address:	Email:
		Date of Birth:

By signing this document, I represent that the information above is correct. I also agree to the direct certificate authorization attached to this document and acknowledge that DigiCert may rely on my adherence to its terms in issuing a digital certificate to my health information service provider.

_____ _____

Applicant Signature Date

INSTRUCTIONS TO NOTARY/TRUSTED AGENT: Please verify the person named in this document using at least one government-issued photo ID. If the ID presented was not issued by the federal government, have the applicant present a secondary form of ID. NOTE: This section is not applicable if the form is signed with an FBCA Medium or higher assurance certificate (uncommon).

ID #1	Type of Document:	Photo: Y N
	Issued By:	Serial #:
	Name on ID#1:	Expiration Date:

ID #2	Type of Document:	Photo: Y N
	Issued By:	Serial #:
	Name on ID#2:	Exp. Date:

ACKNOWLEDGMENT

STATE/COMMONWEALTH OF _____ }
}
COUNTY/PARISH OF _____ }

I certify that at the person named above personally appeared before me and presented the identification listed above.

WITNESSED by _____ and official seal
Notary/Trusted Agent Signs Here

Print Name		Date:
Telephone		Email:

AUTHORIZATION

DigiCert, Inc. ("**DigiCert**") issues X.509 v.3 digital certificates ("**Certificates**") to customers of the health information service provider ("**HISP**") providing this form to you. By signing this document, you agree, on behalf of each Certificate subject you represent, that HISP and DigiCert may provide, on the subject's behalf ("**Applicant**"), certain digital certificate-related duties that are normally reserved for Certificate subjects. These tasks include managing keys, registering devices, authenticating personnel with DigiCert and its Certificate systems, and installing, configuring, and managing issued Certificates. By signing this authorization or signing the declaration of identity form, Applicant hereby agrees and authorizes HISP and DigiCert as follows:

1. Certificates. HISP may request and approve Certificates in Applicant's name and use issued Certificates for Applicant's benefit. DigiCert may issue, refuse to issue, revoke, or restrict access to Certificates in accordance with the instructions provided by HISP and rely on these instructions as if originating from Applicant.

2. Representations. Applicant represents that Applicant 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. Applicant 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 HISP's employees and agents as Applicant's agent for the purpose of requesting, using, and managing Certificates and corresponding private keys. HISP's 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 HISP and its employees to (i) request Certificates for domains and emails owned or controlled by Applicant or Applicant's affiliates, (ii) request Certificates naming Applicant or Applicant's equipment, employees, agents, or contractors as the subject, and (iii) accept terms and conditions related to Certificates issued on Applicant's behalf.

4. Trusted Agent. In addition, the Applicant's accepting this authorization or submitting a signed declaration of identity are hereby appointed as an agent of DigiCert for the purpose of collecting documentation, verifying identities, and providing identity information to DigiCert. Any information must be verified in accordance with instructions provided by DigiCert. The requirements for identity verification are set by the applicable certificate policy and may change without notice, and DigiCert may amend the instructions at any time.

5. Documentation. DigiCert may reuse this information and rely on this authorization for issuing multiple Certificates to HISP 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 or HISP. DigiCert may modify the privacy policy in its sole discretion.

6. Representation. The signer of this document represents that he or she has the authority to execute this authorization 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. 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, and Applicant is responsible for all Certificates requested by HISP on Applicant's behalf. Applicant may revoke the authorization by sending an email message revoking the authorization at 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 to HISP on Applicant's behalf after receiving a verified revocation request from Applicant. DigiCert may also revoke a Certificate issued to HISP on Applicant's behalf for any reason and without notice.

9. Warranty Disclaimers. DIGICERT SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". DigiCert represents that it will provide the services in accordance with its certificate practice statement. 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 or HISP.

10. Limitation on Liability. DIGICERT IS PROVIDING THESE SERVICES TO APPLICANT UNDER AN AGREEMENT BETWEEN HISP AND DIGICERT. DIGICERT'S LIABILITY FOR CERTIFICATES UNDER THIS AUTHORIZATION IS LIMITED TO THE AMOUNT SPECIFIED IN ITS AGREEMENT WITH HISP, WHICH LIMITS APPLY EQUALLY TO THE CERTIFICATES ISSUED UNDER THIS AGREEMENT. APPLICANT ACCEPTS THIS LIMITATION ON LIABLIITY, ACKNOWLEDGES THAT HISP IS RESPONSIBLE FOR ANY USE OF THE CERTIFICATE, AND WAIVES NY RIGHT AGAINST DIGICERT FOR HISP'S 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 HISP. All notices to DigiCert are effective on receipt. HISP is solely responsible for conveying notices to Applicant. DigiCert will deliver notices to Applicant by delivering the notice to HISP. Notices are effective when sent to HISP in accordance with DigiCert's agreement with HISP.

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**.** HISP and DigiCert are express and intended beneficiaries of Applicant's obligations and representations under this authorization.

This authorization is made as of the date below:

APPLICANT **By: _____**
Its:
Date: