Direct-Compliant Certificates

The attached form must be completed, signed, and returned to Health Catalyst Interoperability (HCI) before we can obtain a Direct-compliant digital certificate ("Direct Certificate") on behalf of your organization from DigiCert, Inc. Direct Certificates are used to securely transmit health care information between providers. Any failure to follow the instructions contained herein may result in a delay of the Direct Certificate's issuance.

The attached form contains provisions that are applicable to you personally (as indicated in language referring to "you" or "your"), as well as provisions that apply to your organization (as indicated in language using the capitalized term "Organization"). You must sign the attached form in your personal capacity, indicating your personal agreement to the provisions applicable to "you" or "your." An authorized representative of your Organization must also sign the attached form, on behalf of your Organization.

By signing the Identity Verification, you are also agreeing to the provisions of attached authorization for Direct Certificates applicable to "you" or "your". This authorization, together with your Organization's execution of the attached form, gives HCI permission to request and use Direct Certificates in your Organization's name. HCI will use the Direct Certificates to transfer health care information to your organization in accordance with the Direct Protocol.

After the form is completed, you, a Notary (or Trusted Agent) must send a copy (pdf) of the document (authorization and ID document pages) to HCI at Hispregistration@healthcatalyst.com.

Field Instructions

HCI Customer Name: Enter HCI client name.

Organization: Enter 1) Legal Name of your Organization 2) Telephone 3) Address and 4) preferred Domain Name and 5) HIPAA compliance level.

Authorized Organization Representative: The Applicant or other authorized organization representative should sign and complete all fields after reviewing the authorization agreement.

Applicant: Enter 1) your Name 2) Telephone 3) Home Address 4) e-Mail and 5) Date of Birth. Please do not use your work address to complete this section.

Applicant Signature: The Applicant should complete and sign in front of a Notary.

Identification #1: A Notary (or Trusted Agent) must view and enter your government photo ID information. Examples of acceptable photo ID documents include a passport, driver's license, military ID, permanent resident card, or similar document.

Identification #2: A second ID is required only if your primary ID is not a federal government ID or a "Real ID" approved state driver's license. Examples of acceptable secondary ID documents include a social security card, birth certificate, school ID, work ID, or voter's registration card.

Notary or Trusted Agent: The Notary (or Trusted Agent) will require you to present a government-issued photo ID that lists your name and address. This is to verify your identity. The Notary must see you sign this document and then sign the form.

- You should proceed with contacting a Notary – unless you have been directly informed that a Trusted Agent is available to assist you.

DIRECT IDENTITY VERIFICATION AND AUTHORIZATION

HISP: Health Catalyst
Interoperability

Client	HCI Customer Name: Georgia Health Information Network

Organization	Organization:	Telephone:
	Address:	
	Domain Name:	
	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.	

The undersigned is an authorized officer or other authorized representative of the Organization specified above. The Organization specified above agrees to the provisions of the attached authorization applicable to Organization. The undersigned represents that s/he is duly authorized by Organization to execute this authorization and to bind Organization to such terms.

Organization: _____

Organization Representative Signature: _____

Print Name: _____

Title: _____

Date: _____

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

By signing this document, I hereby agree to the provisions of the attached authorization applicable to me personally (as indicated in language referring to "you" or "your") and request a Direct Certificate and declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

_____ **/ / , :** a.m. ☐ p.m. ☐

Applicant Signature Date and Time

Please have a Notary witness your signature and sign the acknowledgment on the next page. After the form is completed, you or a Notary must send a copy (pdf) of the document (authorization and ID document pages) to HCI at Hispregistration@healthcatalyst.com.

INSTRUCTIONS TO NOTARY/TRUSTED AGENT: Please verify the person signing in the "Applicant Signature" section of this document using at least one government-issued photo ID. If the applicant says they are applying for a medium assurance certificate and the ID presented was not issued by the federal government, have the applicant present a secondary form of ID. Attach a copy of all ID documents to this form. Make sure the information listed in the identification boxes on the first page and below match the identity documents presented during the verification process. **Notaries should sign the Notarial Acknowledgment, leaving the Trusted Agent information blank. Trusted Agents do not need to complete the Notarial Acknowledgment. The identity of the Organization representative does not need to be verified by the Trusted Agent or Notarial Acknowledgment.**

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:

TRUSTED AGENT'S STATEMENT (Not required if notarized)

Trusted Agent			
	I hereby declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that on the date indicated herein, applicant personally appeared before me, signed the foregoing document in my presence, and presented the identification listed above.		
	Name	N/A	
	Organization	N/A	
	Address	N/A	
	Telephone	N/A	Email:

Trusted Agent Signature Date and Time / / , : a.m. ☐ p.m. ☐

NOTARIAL ACKNOWLEDGMENT (Not required if signed by Trusted Agent)

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 / / , : a.m. ☐ p.m. ☐

Print Name		Organization / Employer
Telephone		Email:

DIRECT CERTIFICATE AUTHORIZATION

Health Catalyst, Inc. ("**HCI**") through DigiCert, Inc. ("**DigiCert**"), issues X.509 v.3 digital certificates ("**Certificates**") to customers of its health information service provider ("**HISP**") services. The above described entity ("**Organization**"), as an organization that will be named in a Certificate, is providing this Authorization to assist HCI in performing certain digital certificate-related duties that are normally reserved for Certificate subjects, usually an entity's equipment, personnel, or agents. These tasks include managing keys, registering devices, and authenticating personnel with HCI and its Certificate systems and installing, configuring, and managing issued Certificates. Therefore, Organization and Applicant hereby agree and authorize HCI as follows:

1. Certificates. HCI may request and obtain Certificates in Organization's name and use issued Certificates for Organization's benefit. HCI may further facilitate or refuse to facilitate the issuance of Certificates or restrict access to Certificates in accordance with the terms of this Authorization.

2. Representations. Organization represents that it 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. Organization represents that it will limit its use of the Certificate for purposes required as a HIPAA covered entity, a HIPAA Business Associate or Non-HIPAA Healthcare Entity (HE), defined as an entity that has an appropriate healthcare-related need to exchange Direct messages and which agrees to handle protected health information with privacy and security protections that are equivalent to those required by HIPAA.

3. Authorization. Organization explicitly appoints HCI's employees and agents as its agent for the purpose of requesting, obtaining, using, and managing Certificates and corresponding private keys. HCI's employees and agents are authorized to fulfill all obligations with respect to the Certificates, the management of key sets and Certificates, and to fulfill all roles related to Certificate issuance, such as a Certificate requester and contract signer (as used in the CA/Browser Forum's Extended Validation Guidelines for SSL Certificates). Organization hereby authorizes HCI and its employees to:

   (i) Request Certificates for domains and emails owned or controlled by Organization or its affiliates;
   (ii) Request Certificates naming Organization or its equipment, employees, agents, or contractors as the subject; and,
   (iii) Provide any of the Authorizations, or accept any of the terms that are contained in this Authorization, on Organization's behalf and request any and all necessary acceptance by Organization or Applicant, as applicable, of any additional terms and conditions for utilization of the Certificates that are not set forth herein.

4. Trusted Agent. Where applicable, as determined by HCI, Organization is hereby appointed as an agent of HCI for the purpose of collecting documentation, verifying identities, and providing the identity information that is presented in the Identity Verification. Any information set forth in the Identity Verification must be verified in accordance with instructions provided by HCI. The requirements for identity verification are set by the applicable certificate policy of DigiCert and may change without notice. Therefore, HCI may amend the instructions at any time.

5. Documentation. For each Certificate ordered by HCI under Organization's Authorization, HCI must obtain a personal attestation and a copy of all documentation necessary to verify the individual's identity. HCI may reuse this information in some cases. HCI may rely solely on the information Applicant provides or previously provided when issuing a Certificate or may elect to perform additional verification prior to issuing a Certificate. Applicant agrees to provide, at all times, accurate, complete, and true information to HCI. If any information provided to HCI changes or becomes misleading or inaccurate, then Organization agrees to promptly update the information. Organization consents to (i) HCI's public disclosure of information embedded in an issued Certificate, and (ii) HCI's transfer of personal information presented in the Identity Verification (the "**Identity Verification Data**") to HCI's servers which are located inside the United States. HCI shall follow the privacy policy posted on its website when receiving and using information the Identity Verification Data. HCI may modify the privacy policy in its sole discretion upon thirty (30) days' prior written notice to Organization.

6. Representation. By submitting the Identity Verification Data to HCI, Applicant represents that the Identity Verification Data accurately shows Applicant's name and birthdate and Applicant's address, email address, and telephone number as of the date of the Identity Verification. By submitting the Identity Verification Data, Organjzation represents that Organization: (i) has verified Applicant's, as well as any other named individual's name, address, email address, telephone number, birthdate, and any other information required by and submitted to HCI, in accordance with the instructions that appear in the Identity Verification or as otherwise provided by HCI; (ii) has examined any relied-upon documents for modification or falsification and believes that the documents are legitimate and correct; and, (iii) is unaware of any information presented in the Identity Verification that is reasonably misleading or that could result in a misidentification of the Organization. These representations survive termination of this appointment until all Certificates that rely on the Identity Verification expire.

7. Duration. This Authorization lasts until revoked by Applicant or Organization, and Organization is responsible for all Certificates requested by HCI on Organization's behalf until after HCI receives a clear email message revoking this Authorization. Even after revocation, all representations and obligations herein survive until all Certificates issued under this Authorization expire or are revoked in accordance with this Authorization. HCI may require that Applicant and/or Organization periodically renew this Authorization by resubmitting a copy of this Authorization to HCI.

8. Certificate Revocation and Termination. HCI will revoke any Certificate issued to HCI on Organization's behalf after receiving notice from Applicant or Organization, and after verifying the legitimacy of the revocation request. HCI may also revoke a Certificate issued to HCI on Applicant's or Organization's behalf for any reason and without notice.

9. Warranty Disclaimers/DigiCert Warranty. HCI SERVICES WITH RESPECT TO THE ACTIVITIES DESCRIBED IN THIS AUTHORIZATION ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, HCI DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, WITH RESPECT TO THE ACTIVITIES DESCRIBED IN THIS AUTHORIZATION. HCI DOES NOT WARRANT THAT ANY SERVICES WITH RESPECT TO THE ACTIVITIES DESCRIBED IN THIS AUTHORIZATION WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO SERVICES WILL BE TIMELY OR ERROR-FREE. HCI may modify or discontinue specific service or product offerings at any time. DigiCert warrants that it shall provide the Certificates in accordance with its Certification Practices Statement (the "**CPS**"), as updated from time to time and may be found at http://www.digicert.com/ssl-cps-repository.htm. Notwithstanding the foregoing, nothing herein requires HCI or DigiCert to provide Certificates or other related services to Organization or Applicant.

10. Limitation on Liability. EXCEPT AS SET FORTH IN PARAGRAPH 11 HEREINBELOW, NEITHER APPLICANT. ORGANIZATION, HCI OR DIGICERT SHALL BE LIABLE FOR ANY (INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNATIVE DAMAGES OR ANY LOSS OF PROFIT, REVENUE, DATA, OR OPPORTUNITY, EVEN IF ANY PARTY 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 agreement were breached or proven ineffective.

11. Indemnification. To the extent permitted by law, *Organization* will indemnify and defend HCI and its contractors, agents, employees, officers, directors, shareholders, affiliates, and assigns against all liabilities, claims, damages, and costs (including reasonable attorney's fees) (collectively, "**Damages**") related to HCI's reasonable reliance on (i) the Identity Verification Data, (ii) this Authorization, (iii) the issuance or the use of a Certificate issued under this Authorization, and (iv) any breach by Organization or Applicant of this Authorization. To the extent permitted by law, *HCI* will indemnify and defend Organization and its contractors, agents, employees, officers, directors, shareholders, affiliates, and assigns against all Damages related to (i) HCI's negligence in its transmission to DigiCert of the Identity Verification Data or (ii) HCI's breach of this Authorization in respect to Organization; **provided, however**, that Applicant and Organization agree and acknowledge that HCI expressly disclaims and shall not take on any responsibility or liability of any kind with respect to the accuracy of the Identity Verification Data or any other information provided herein by Applicant or Organization.

12. Enforcement; Severability. HCI, on behalf of its contractors, agents, employees, officers, directors, shareholders, affiliates, and assigns, agrees that to the extent that Applicant's or Organization's conduct gives rise to liability under this Authorization, the aggrieved party shall look solely to Organization for compensation and recoupment of damages, and shall not look to Applicant for such compensation and/or recoupment. If Applicant violates this Authorization, that violation shall constitute a violation of this Authorization by Organization. Organization hereby agrees that it shall indemnify HCI and its contractors, agents, employees, officers, directors, shareholders, affiliates, and assigns from and against, and shall otherwise pay any claims, Damages, expenses, or other costs arising from (i) Organization's violation of a requirement applicable to it under this Authorization and (ii) Applicant's violation of a requirement applicable to Applicant under this Authorization.

    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**.** HCI and DigiCert are express and intended beneficiaries of Applicant's and Organization's obligations and representations under this Authorization.

14. Protection of Personal Data. "**Personal Data**" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Neither HCI nor DigiCert shall (a) use or disclose to any other party or third person, including their affiliates, any Personal Data disclosed to either of them by or on behalf of Organization pursuant to this Agreement except as authorized by this Authorization or any other applicable agreement, unless such disclosure is required by law or the CPS; and (b) use all reasonable security and privacy safeguards to maintain the confidentiality of all such Personal Data in their possession or control, which will in no event be less than the measures each uses to maintain the confidentiality of its own information of similar importance.

15. Notices. All notices and demands required or permitted under this Authorization shall be in writing and may be delivered personally to the other Party, or sent by registered or certified mail, postage prepaid or by an overnight courier service. Any notice or demand mailed or sent by courier as aforesaid shall be deemed to have been delivered on the date of delivery or refusal, as the case may be. Said notices shall be delivered to the addresses set forth in the Identity Verification or to such other address as a Party may designate by written notice to the other Party.

16. Severability. If any provision of this Authorization or the application of such provision to any Party or circumstance shall be held invalid, the remainder of this Authorization, or the application of such provision to Parties or circumstances, other than those as to which it is held invalid, shall not be affected unless such invalidity would materially alter the Party's ability to perform or interfere with the essential purpose of this Authorization.

17. Assignment. Except in connection with dissolution, consolidation, acquisition, or merger, no Party shall assign any of its rights under this Authorization, except with the prior written consent of the other Parties. . Any change of control transaction is deemed an assignment hereunder. Any purported assignment of rights in violation of this paragraph is void.

18. Final Agreement. This Authorization, in conjunction with the Identity Verification, constitutes the complete, final, and exclusive expression of the Parties' agreement, and it supersedes all proposals and other communications made among the Parties concerning the subject matter hereof. This Authorization cannot be modified except by written agreement signed by the Parties.

19. Waiver. A waiver of a default or any term of this Authorization shall not be construed as a waiver of any succeeding default or as a waiver of the provision itself. A Party's performance after the other Party's default shall not be construed as a waiver of that default.

20. Governing Law; Venue. This Authorization, all transactions executed hereunder and the legal relations between the Parties shall be governed and construed solely in accordance with the laws of the State of Utah, without reference to its conflict of laws rule. The Parties, to the fullest extent allowed by law, hereby consent to the exclusive jurisdiction of the state and federal courts situated in Salt Lake City, Utah.