SUBSCRIBERS MUST READ THIS SUBSCRIBER AGREEMENT BEFORE APPLYING FOR, ACCEPTING, OR USING AN SHC DIGITAL CERTIFICATE. IF YOU DO NOT AGREE TO THE TERMS OF THIS SUBSCRIBER AGREEMENT, A CERTIFICATE WILL NOT BE ISSUED IN YOUR NAME.

1. Scope: THIS SUBSCRIBER AGREEMENT governs your rights, duties, and liabilities as a subscriber of a Certificate issued by Shriners Hospitals for Children (SHC). It is effective on the date you submit a certificate application to SHC whether through a designated Registration Authority (RA) or directly to the SHC Certification Authority (CA). By submitting this Subscriber Agreement (and certificate application), you are requesting that the SHC CA issue a certificate to you and are expressing your acceptance and agreement to the terms of this Subscriber Agreement.

SHC digital certificate services are governed by the SHC Certificate Policy (CP) and the SHC Certification Practice Statement (CPS) as amended from time to time, which are incorporated by reference into this Subscriber Agreement.

SUBSCRIBERS AGREE TO USE THE CERTIFICATE AND ANY RELATED RA SERVICES ONLY IN ACCORDANCE WITH THE CP AND CPS.

2. Certificate Issuance

2.1 Application: The content of a Subscriber certificate is based on information entered on the certificate application form. If you are uncertain whether the information you provided is accurate, you should correct it now. You agree to provide such further information as SHC may reasonably require in connection with your application and the Identification and Authentication process.

2.2 Key Pair Generation: You will generate your own signature key pairs, and the corresponding public keys will be submitted to the SHC CA, incorporated into your certificate, and stored by SHC in its certificate repository. Confidentiality (encryption) key pairs are generated by the CA and downloaded by the Subscriber during the certificate download process.

2.3 Identification and Authentication: Prior to issuing your certificate, SHC will verify the information submitted in your application. You hereby authorize SHC to verify your identity by any reasonable means. SHC may consult internal or external databases or other sources, solely for the purpose of verifying information submitted by you so that SHC can verify your identity. If, based on the information available, SHC is unable to identify and authenticate you and your certificate request to its satisfaction, SHC may refuse to issue you a certificate or seek your permission to obtain additional information. You also authorize SHC to store and use in accordance with this agreement any information generated during the application, Identification and Authentication, and certificate issuance processes. At all times, SHC agrees to protect your privacy in accordance with Section 4.1 below.

2.4 Issuance: If SHC accepts your application for certificate(s) and confirms the information submitted during the application process, the SHC CA will create your certificate(s) and notify you how and where to retrieve your certificate(s). If SHC is unable to confirm your identity, SHC may refuse to approve your application and will not issue you any certificate(s).
2.5 Acceptance: When you enter the activation code, as provided by the SHC CA, in order to download your certificate(s), you will once again be presented with the certificate’s proposed contents. You agree to review the proposed contents of your certificate(s), and immediately notify the PKI Administrator of any errors, defects or problems with your certificate(s). You agree that you will have accepted your certificate(s): (i) when you use your certificate(s) or the corresponding private key after downloading your certificate(s), or (ii) if you fail to notify the PKI Administrator of any errors, defects or problems with your certificate(s) within five business days after downloading it.

2.6 Certificate Lifetime: Your certificate(s), and renewals, will be valid for two years from the date of issuance. You will be notified and given the opportunity to renew your certificate(s) every two years prior to the expiration of your current certificate(s), unless (a) your certificate(s) has been revoked or (b) you have notified the PKI Administrator to cancel this agreement. If you elect to renew, you will be responsible for complying with SHC’s then-current procedures to receive your renewal certificate(s). The terms of this agreement shall apply to each such renewal certificate(s).

3. Your Rights and Responsibilities

3.1 Representations and Warranties By accepting your certificate, you:
   (i) Accept its contents and the responsibilities identified in this agreement, and
   (ii) Represent and warrant to SHC and to all who reasonably rely on the information contained in your certificate that:
       (a) You rightfully hold the private key corresponding to public key listed in your certificate;
       (b) All representations you made and information you submitted to SHC in the application process were current, complete, true and not misleading,
       (c) You have provided all facts material to confirming your identity and to establishing the reliability of your certificate,
       (d) All information in your certificate that identifies you is current, complete, true and not misleading,
       (e) You are not aware of any fact material to the reliability of the information in your certificate that has not been previously communicated to SHC, and
       (f) You have and will keep your private key secret.

3.2 Use of Your Certificate: You agree the certificate(s) will be used exclusively for authorized SHC purposes. You may use your signature keys and certificate to establish your identity with third parties, sign documents and forms, file documents electronically, and obtain access to certificate-enabled resources within the SHC information systems environment. You may use your confidentiality keys and certificate to encrypt and decrypt electronic data. SSL certificates may be used only for authentication of devices.

You may not use your certificate for:
   • Transactions where applicable law prohibits the use of digital signatures or
   • Fraud or any other illegal scheme or purpose.

If you use your certificate for any purpose prohibited in this section, you forfeit all of the rights and protections granted to you by SHC under this agreement.

3.3 Protect Your Private Key: You are responsible for protecting your private key. If you suspect or discover that your private key has been stolen, lost, or otherwise compromised, then you must immediately notify the PKI Administrator, as provided in section 3.5 below (if possible via e-mail signed with your private key), and request that your certificate be revoked. You must then immediately cease all use of your certificate and your private key.

You agree to keep your private key (and any activation data used to protect your private key) secret and secure by:
   • Protecting access to the private key by PIN or password, and
   • Taking other reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, your private key, any activation data and the computer system or media on which your private key is stored or managed.
Failure to notify the PKI Administrator of the theft, loss, compromise, or misuse of your private key, or continued use of the key or certificate after they have been compromised, may cause you serious adverse legal consequences.

3.4 Changes in Certificate Information: If your name or your e-mail address listed in your certificate changes, you should immediately notify the PKI Administrator. If SHC does not have a valid name or e-mail address for you, SHC may not be able to fulfill its obligations to you, including but not necessarily limited to, sending certificate renewal notices, revocation and suspension notices, and providing other information. You may need to know about your certificate and its use. An incorrect e-mail address in your certificate may also prevent you from using it for signing and securing your e-mail, and may cause other technical problems or limitations on the use of your certificate.

3.5 Revoke your Certificate:

When to Revoke Your Certificate: You must immediately request that the PKI Administrator revoke your certificate if:

(i) Your name listed in your certificate is no longer current, complete or true;
(ii) You ever discover or suspect that your private key has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way; or
(iii) Your association with SHC is terminated.

You may also request that the PKI Administrator revoke your certificate at any time for any other reason.

How to Revoke Your Certificate: You can initiate a revocation request by:

(i) Sending a signed e-mail (containing the reason for revocation and using your private key) to pkiadmin@shrinenet.org; or
(ii) Calling the SHC Help Desk at 813-281-8100.

3.6 Cease Using Your Certificate: You must immediately cease using your certificate in the following circumstances:

(i) When you suspect or discover that your private key has been or may be compromised or subjected to unauthorized use in any way;
(ii) When your name listed in your certificate is no longer current, complete or true;
(iii) After you have requested, or been notified by SHC that someone has requested, that your certificate be suspended;
(iv) Upon the revocation or expiration of your certificate; or
(v) Upon termination of this agreement.

3.7 Consequences of Breach: If you act in any manner counter to your obligations under this agreement, you will forfeit any claims you may have against SHC.

3.8 Indemnification: By accepting your certificate, you agree to indemnify and hold SHC and its directors, officers, employees, agents and affiliates harmless from any and all liabilities, costs, and expenses, including reasonable attorneys’ fees, related to:

(i) any misrepresentation or omission of material fact by you to SHC, whether or not such misrepresentation or omission was intentional;
(ii) your violation of this agreement;
(iii) any compromise or unauthorized use of your certificate or your private key that is not caused by SHC, unless prior to such unauthorized use you have appropriately requested revocation of your certificate and proven your authority to request revocation; or
(iv) your misuse of your certificate or your private key, including without limitation any use of your certificate that is not permitted by this agreement; PROVIDED, however, that nothing herein shall require the Subscriber to indemnify SHC for any consequences or damages caused by the fault of SHC, or SHC’s failure to fulfill any of its obligations.

4. SHC's Rights and Responsibilities:

4.1 Your Privacy Is Important: SHC will use reasonable care to ensure that your private information will be kept confidential. SHC will:

(i) Comply with all applicable laws and regulations regarding privacy of information;
(ii) Protect the confidentiality of your private information; and
(iii) Use your private information only for the purpose of providing certificate services and
carrying out the provisions of this agreement.

Your private information will not be sold, rented, leased, or disclosed in any manner to any person
without your prior express consent, except:

(i) As required by law, or
(ii) As may be necessary for the performance of certificate and repository services or for auditing
requirements.

SHC will protect your private information in a manner designed to ensure its integrity and to make
it available to you, following an appropriate request.

However, your certificate and any information contained in your certificates, including your
identity, must be seen by others and is not private. Information that may be disclosed in
your certificate and in SHC's repository includes, but is not limited to:

(i) Your name and e-mail address,
(ii) The public key listed in your certificate; and
(iii) The certificate serial number and expiration date.

However, your address, telephone number and other personally identifying information,
other than name and e-mail address, will not appear in your certificate and will not be
disclosed to third parties except as provided in this agreement.

4.2 Certificate Repository: During the term of this agreement, SHC will operate and maintain an on-
line repository that is available to Relying Parties and that contains:

(i) All current, valid certificates issued by the SHC CA (including, as applicable, your certificate),
and
(ii) A CRL and/or on-line database indicating the status, whether valid, suspended or revoked, of
such certificates.

When you accept your certificate, the CA will publish your certificate in the repository and will indicate its
valid status until it is suspended, revoked or expired, as provided in section 4.3 below. SHC will provide
non-exclusive access to the repository from within the SHC Wide Area Network to Relying Parties to
check the validity and status of your certificate.

4.3 Revocation and Suspension: If you request that your certificate be revoked, the CA will revoke
your certificate through recognized Vettors and update the repository as soon as practical, but not later
than set forth in the Certificate Policy, after the Vettor has adequately confirmed that the person making
the revocation request is authorized to do so. If the request is signed using your private key, the Vettor
will accept the request as valid.

The PKI Administrator may suspend your certificate for period of up to sixty calendar days. If necessary
due to technical requirements, SHC's suspension procedure may be to temporarily suspend and then
reinstate the certificate.

SHC may revoke your certificate without advance notice, and thereafter notify you, if it determines that:

(i) Your certificate was not properly issued or was obtained by fraud;
(ii) The security of your private key has or may have been lost or otherwise compromised;
(iii) Your certificate has become unreliable;
(iv) Material information in your application or your certificate has changed or has become false or
misleading;
(v) You have violated any applicable agreement or obligation;
(vi) You or a third party request revocation or suspension;
(vii) A governmental authority has lawfully ordered SHC to revoke your certificate;
(viii) This agreement terminates; or
(ix) There are any other grounds for revocation.

SHC will notify you when your certificate has been revoked or suspended.
4.4 Representations and Disclaimer of Warranties:

Representations: SHC represents to you, as of the time SHC issues your certificate and as of the time any Relying Party checks the repository for the validity of your certificate, that:

(i) When authenticating your identity and issuing your certificate, the CA, RA and Vettor complied with the requirements of SHC’s policies and procedures governing identification and authentication and issuance of certificates under the SHC Certificate Policy,
(ii) In issuing your certificate, SHC did not exceed any limits of its license as a Certification Authority;
(iii) SHC took reasonable steps to verify the information in your certificate;
(iv) SHC has managed your certificate in accordance with this agreement and SHC’s policies and procedures governing the management of certificates under the SHC CP or SHC CPS.

Disclaimer of Warranties:

SHC DISCLAIMS ANY AND ALL WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, THAT ARE NOT SPECIFICALLY PROVIDED HEREIN, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO THE SERVICES PROVIDED OR THE CERTIFICATE ISSUED HEREUNDER.

5. Governing Law: This agreement shall be governed by and construed under the laws of the State of Florida.

6. Dispute Resolution: In the event of any dispute or disagreement between the parties hereto (“Disputing Parties”) arising out of or related to this agreement or your certificate, the Disputing Parties will use their best efforts to settle the dispute or disagreement through good faith negotiations following notice from one Disputing Party to the other(s). If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties will submit the dispute to the SHC PKI Workgroup for resolution in accordance with the provisions of section 9.13 of the CP.

7. Entire Agreement: This Agreement, together with any other documents referred to and/or incorporated herein, constitute the entire agreement between you and SHC with the respect to your certificate.

8. Third Party Beneficiaries: It is not the parties’ intent that this agreement, or any of the other documents mentioned in the preceding paragraph, should confer, and they shall not confer, any rights on any third party.

9. Amendment: You agree that SHC may modify this agreement from time to time during the term of this agreement. Minor modifications shall become effective when posted to SHC’s Intranet Web site. Any modification to this agreement that substantially alters your rights or obligations will become effective when you renew your certificate after you have received notice of such modification. You will be deemed to have received notice of any modification when

(i) You actually receive written notice of such modification, or
(ii) Notice of such modification is accessible by you at the e-mail address you have provided to SHC.

10. Severability: If any provision of this agreement is found to be invalid or unenforceable, then this agreement will be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this agreement.

11. Survival: Sections governing confidentiality of information, indemnification, SHC’s representations and disclaimer of warranties, governing law and dispute resolution will survive any termination or expiration of this agreement.
SHC Certificate Subscriber Agreement

SUBSCRIBER/SPONSOR:
Name: _________________________________ Date: _______________________________
(Print)
_________________________________ Location: __________________________
(Signature)
Department: ______________________ SHC email: ___________________________
Telephone: ______________________
External email address: ___________________________________
(For non-employee Subscribers that do not actively use SHC email)

Subscriber Classification:
☐ Individual (employee or affiliated person)
☐ Device (must be under SHC control)
☐ Organizational

Reason for requesting certificates: ________________________________________________________
(If device certificate, include name of device)

APPROVAL:
Supervisor: _________________________________ Date: _______________________________
(Print)
_________________________________ Location: ___ __________________________
(Signature)
Department: ______________________ SHC email: ___________________________
Telephone: ______________________

FOR VETTOR AND/OR HR USE ONLY:
☐ Subscriber/Sponsor has AD account and ShrineNET email.
☐ Smart card issued serial number: ____________________________________

Subscriber must be identified by using one of the following methods (select one):
☐ Information from existing database
☐ Two official identification credentials, at least one of which must be a government issued picture ID (e.g. drivers license, passport)
  Type: ________________________________ ID Number: ____________________________
  Type: ________________________________ ID Number: ____________________________

Name of verifier: ______________________________ Date: _______________________________
(Print)
_________________________________
(Signature)