Scripps Care Link Access Request Form

Name	Add name of user requesting access; last name, first name					
Contracted Provider	This is the name of the entity contracted with SHPS					
Contracted Provider Tax ID	This is the number listed on the Contracted Provider's W9					
Contracted Provider NPI	This is the NPI for the Contracted Provider listed in column 3					
Are you a Practitioner?	Are you the Provider or Physician at your facility					
Practitioner NPI	Enter your Practitioner NPI					
Practitioner Specialty	Enter the specialty or the specialty of the provider you are associated with if they are not the same					
User Role	Enter your role: front desk, office admin, billing…etc	Referral Entry	Referral View	Claims View	Eligibility View	Site Administrator
		☐	☐	☐	☐	☐
Address	Office address and phone information. This is the address of the office where you are physically located, . Please note phone number format and this must be your direct line. If you have an extension number, please preceded your extension number with and x as seen in the example below. ***Administrative emails are not accepted. Your email address will be used to authenticate your identity.***					
Phone						
Fax						
Email – **must be an individual work email and not a generic email**						
Confidentiality Agreement	Please complete the Confidentially Agreement and send it along with this access request to ProviderRelations@scrippshealth.org					

Please return completed form attached with the Confidentiality Agreement to: ProviderRelations@scrippshealth.org or fax to 858-260-5851

Scripps Care Link Access Request Form

Information Systems Access Request

Affiliated Providers

1. **Request Type:** **NEW REQUEST / ANNUAL RENEWAL**
2. **Type of Terminal:** Remote Access
3. **TIN #:** _____
4. Last 4 digits off Social Security Number: _____
5. Date of Birth _____

SHPS - Enterprise-wide Data Security Policy

6. **Policy:**

All data, electronic or paper, resident within the many SHPS communications and computer systems, including personal computers, intelligent workstations, telecommunications devices, voice mail, networks, servers, and any storage media, is the sole property of SHPS and/or specifically designated partners and affiliates of these entities. Data and communications pertaining to the daily operation of SHPS, or to their patients, but resident on privately owned personal systems, shall be considered to be data owned by SHPS and, as such, is subject to the policies and regulations set forth in the SHPS Policy and Procedure Number 903 and this and other relevant documents. Permission to access data may be granted to Affiliated Providers under the following conditions:

Guidelines: (each condition must be read and initialed)

_____ Permission to access data may be granted for the purposes of gathering information or updating records only during the normal performance of a Affiliated Providers job. Regular audits of access are conducted on all systems.

_____ Voice mail and messaging systems, including the Internet, are intended as business communications tools. Use of these systems for solicitations, private or public announcements not pertaining to business is prohibited. Profanity, abuse, threats, gossip, or personal information constitutes a misuse of these systems. Affiliated Providers should not expect any privacy in their communications over the Internet or any other communication systems. Unauthorized uses of Internet based services are strictly prohibited.

_____ Affiliated Providers shall not disclose sensitive, confidential information or data, either specific or aggregate, which is owned, controlled, or protected by SHPS without the express permission of the owner, steward, or guardian of that information. Methods of disclosure may include, but are not limited to, data transfer or transmission, verbal or written disclosure, news release, documents left in full or partial view including unattended, connected computer workstations.

_____ Unauthorized access to medical information is prohibited by law (California Civil Code, Section 56). This includes all medical information whether in the medical record or on a computer. Access to one's own medical record must be requested in writing through the Health Information Department.

_____ Access codes, and passwords are strictly confidential and may not be disclosed or shared by anyone.

Please return completed form attached with the Confidentiality Agreement to: ProviderRelations@scrippshealth.org or fax to 858-260-5851

Scripps Care Link Access Request Form

_____ Failure to log off from a terminal when your work is completed allows unauthorized system access by others. Employees with workstations in public areas must invoke password protected video display protection or logoff from their workstations when leaving the immediate area.

SECURITY AGREEMENT: I have carefully read and initialed each condition in the policy stated above and I acknowledge that my signature affixed to this agreement constitutes acceptance of the terms listed therein and an agreement to abide by them. I understand that the agreement applies to all SHPS communications & computer systems and that violation of any of the terms of this agreement may result in actions up to and including termination of my contract agreement with SHPS.

7. **User Signature**: _____

8. **Date**: _____

SUPERVISORY/MANAGERIAL APPROVAL: I certify that this Affiliated Provider is a bona fide representative of the Scripps Clinic under my supervision and has a valid business reason for this request. He/She is duly authorized by me to secure access to the Scripps Clinic System(s) named above.

9. **Supervisor's Name (please print):**_____

10. **Department:**

11. Supervisor's Signature:_____

12. Phone Number:_____

13. Date:_____

Please return completed form attached with the Confidentiality Agreement to: ProviderRelations@scrippshealth.org or fax to 858-260-5851

Scripps

AUTHORIZED AFFILIATE CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

Obligations Regarding Confidentiality and Security of Scripps Data and Information

Confidential Information, *which includes protected health information (PHI), personal financial information (PFI) and other sensitive or proprietary Scripps organizational information, is protected by Scripps' policies and state and federal regulations regarding the privacy and security of patient information*.

I understand that in my capacity as an employee of an Authorized Affiliate, I have been granted access to Scripps Confidential Information within the Scripps Network, including but not limited to the email system, Electronic Health Record (EHR), and Epic.

I UNDERSTAND AND AGREE TO THE FOLLOWING:

- Any Confidential Information (includes any/all patient information) that I may access in the Scripps Network does not belong to me, and I have no right or ownership in such information. Accordingly, Scripps, at its sole discretion, may remove, or in any manner restrict, my access to Confidential Information, or any subset of Confidential Information, at any time and for any reason.
- I will only access, use, download and/or disclose patient information necessary for me to perform my Authorized Affiliate job duties as defined by my employer and Scripps.
- I will not access, view, copy, photograph, or in any other manner obtain, any PHI or PFI not required for performance of my work. <u>This specifically includes any information that pertains to me, or to any member of my family</u>.
- I will take all necessary steps to safeguard Confidential Information, consistent with Scripps policies.
- I will protect my computer passwords and will not share them with anyone or any entity. My user IDs and passwords are my "*electronic signature,*" and I am accountable for all access and actions under my logon.

I AGREE TO REPORT CONCERNS REGARDING PRIVACY OR INFORMATION SECURITY:

- If I believe that I, or any other individual or entity, has inappropriately accessed, used, or disclosed Confidential Information, I will immediately report my belief and any supporting facts to my supervisor, as well as the Scripps Privacy Office at (858) 678-6819.
- I will immediately report any Information Security Incident to the IS Help Desk (858-678-7500). An Information Security Incident includes any lost or stolen computer, handheld device, cell phone, and/or electronic storage media, or any disclosure or misuse of my password.

ACKNOWLEDGEMENT OF MY RESPONSIBILITIES:

I have read and understand this Authorized Affiliate Confidentiality and Non-Disclosure Agreement. My obligations under this Agreement shall survive the termination of my Authorized Affiliate employment. I also understand that any failure to comply with any term of this Agreement will be reported to my employer who, as a result, may take corrective action. I also understand that Scripps may terminate my access to the Scripps Network and its data, now and in the future. By signing below, I understand that I am agreeing to the terms of this Agreement, and that I agree to be bound by them.

Name (Print) and Title | Employer / Practice Name

Signature | Date | Corporate ID# (6-digits)
