Scripps
Health Plan Services

Please **complete** all three (3) pages provided. Please follow the instructions below:

- Box 4 – User Name **Last**, **First**, **Middle Initial**
- Box 5 – User E-mail Address (**Please do NOT provide a personal email address)**
- Box 6 – User Provider Address & your Department
- Box 7 – Circle all that apply to **user**
- Box8 – Phone and Fax Numbers (with area code), and Tax ID Number
- Box 9 – **Last 4** Digits of Social Security Number (**REQUIRED)**
- Box 10 – User Date of Birth **(Month/Day)**
- Box 11 – User Signature
- Box 12 – Date
- Box 13 – Supervisor's Name
- Box 14 – Department **Supervisor** works in
- Box 15 – Supervisor's Title
- Box 16 – Supervisor's Signature
- Box 17 – Supervisor's Phone Number
- Box 18 – Date

*** If form is not complete Scripps Health Plan Services will resend incomplete form back to providers for correct completion, which will delay user access.

*** **Access will not be granted until all three pages are complete.**

*** For **questions** on completing this form contact Elvia Cabrera @ **858-927-5452.**

*** Please **fax** back to: 858-260-5851, Attn: Elvia D. Cabrera - Contracts & Provider Relations

Scripps
Health Plan Services

Information Systems Access Request
Affiliated Providers

1. Request Type: ☒ **Add**	2. Type of Terminal: ☒ **Remote Access**	3. Systems to be accessed: **https://www.cerecons.com/scripps/physician/login.aspx**
4. Name (Last, First, Middle Initial): Supply ALL information & Print Clearly		5. Email Address:
6.Provider / Practice Name and Address: Department:		**7.** Business Reason for Access: (**Circle at least one)** **View enrollment and copay information, enter and track referrals, check claim status**
8. Phone Number: Fax Number: **TIN:**	9. Last 4 digits off Social Security Number:	10. Date of Birth

SHPS - Enterprise-wide Data Security Policy

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**.

_____ 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.

11. **User Signature:**	12. **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.

13. **Supervisor's Name (please print):**	**14. Department:**	**15. Title:**
16. **Supervisor's Signature:**	17. **Phone Number:**	18. **Date:**

Related Form to Policy S-FW-IM-0201

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 the law.*

I understand that in my capacity as an employee, medical staff member, contractor, volunteer, or other third party having access to Scripps information, I may see or hear Confidential Information. This Confidential Information, which may exist in any form (e.g., written, electronic), includes, but is not limited to:

- Patient information (e.g., patient records, test results, treatment plans, conversations regarding patient status or outcome, personal financial information);
- Scripps business information, including, but not limited to, strategic plans, budgets, internal financial reports, contracts, vendor quotes, PFI, personnel or employment information or records, or other proprietary information.

I UNDERSTAND AND AGREE TO THE FOLLOWING:

- Any confidential Information that I may receive or learn from any source during the course of my work at Scripps does not belong to me, and I have no right or ownership in such information. Accordingly, Scripps, at its sole discretion, may remove, in any manner restrict, my access to Confidential Information, or any subset of Confidential Information, at any time and for any reason.
- I will not misuse any Confidential Information, and will only access such information as is necessary for me to do my job.
- I will not use, download, or disclose any Confidential Information at any time, or for any purpose, unless required to do so for the performance of my Scripps-related duties.
- I will not access, view, copy, photograph, or in any other manner obtain, any PHI or PFI that is not required for performance of my work for Scripps. This specifically includes any information that pertains to me, or to any member of my family.
- I will take all necessary steps to safeguard Confidential Information at all times in accordance with the law and Scripps policies including Scripps policies regarding record retention and authorized record destruction.
- I will protect my computer passwords and will not share them with any individual. I understand that my user ID's and passwords are my "*electronic signature*" and I am accountable for all access and actions under my logon.
- On termination of my employment or engagement with Scripps, or at any other time that I am requested to do so, I will immediately return to Scripps all documents or property containing any Confidential Information in my possession, custody and control.

I AGREE TO REPORT CONCERNS REGARDING CONFIDENTIALITY SAFEGUARDS:

- If, at any time, I believe that I, or any other individual or entity has inappropriately accessed or disclosed Confident Information, I will immediately report my belief and any supporting facts to my supervisor and/or Audit & Compliance Services, and/or the Scripps Ethics & Compliance Alert Line (1-888-424-2387). I understand that Scripps will not tolerate retaliation against me for making any such good faith report.
- 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 misuse of my password.

ACKNOWLEDGEMENT OF MY RESPONSIBILITIES:

I have read and understand this Confidentiality and Non-Disclosure Agreement. I understand that my obligations under the Agreement shall survive the termination of my employment or engagement with Scripps. I also understand that any failure to comply with any term of this Agreement may result in corrective action, up to and including termination of employment, or any other relationship with Scripps, as well as appropriate legal action. By signing below, I understand that I am agreeing to the terms and conditions of this Agreement, and that I agree to be bound by them.

_____	_____
Name (Print)	Title
_____	_____
Signature	Date

Personal Computer Access to Scripps Network Security Safeguard Attestation

In today's rapidly changing technical world it is important to use safeguards to protect your personal computers and for Scripps to minimize risks when your computers are remotely connected to our resources. These required safeguards are basic precautions to protect the confidentiality and availability of our patients' data. To that end, we require that all non-Scripps owned computers that connect to the Scripps corporate network have the following mechanisms enabled:

- ✓ **Antivirus Software (AV)**
  - Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware). (e.g. Norton, McAfee, Symantec, CA, etc.)
- ✓ **Latest Operating System Patches (OS)**
  - An operating system (OS) is the computer program that manages all other programs on the machine. Updates address known issues and help protect against known security threats. (e.g. Windows latest update)
- ✓ **Personal Firewall**
  - A personal firewall is a piece of software installed on an end-user's PC which controls communications to and from the user's PC, permitting or denying communications based on a Security Policy. (e.g. Windows Service Pack 2, Zone Alarm, etc.)

I attest that prior to connecting my personal computer or laptop to the Scripps corporate network; it will have the above mechanisms enabled and operational. In addition, my AV and OS updates will be set to automatically update when new signature files or patches are available and otherwise maintained current.

Signature: _____ Date: _____

Print Name: _____ Phone: _____

Facility: _____