I. Purpose of Scripps Community Connect EHR Practices and Procedures

Quality healthcare includes patients' rights and regulatory responsibilities for providers to maintain patients' privacy and confidential information in strict confidence. When patients choose Scripps ACO providers for their care, they often are sharing the very most personal and sensitive information about themselves. It is the responsibility of Scripps ACO providers to protect patient information from being shared with individuals who do not have a need to know. In addition, to help ensure the privacy of patient information, there are various state and federal laws and regulations which mandate protection of such confidential information. In order to fulfill our obligations to our patients and meet regulatory requirements, Scripps has developed certain policies, procedures, standards, rules, regulations, guidelines and recommendations regarding EpicCare EHR, and the privacy and security of patient information (the "Scripps Community Connect EHR Practices and Procedures") to establish effective practices for the management of personal and confidential information.

Scripps Community Connect EHR Practices and Procedures provide specific direction that help to communicate expectations, and ensure compliance with federal and state laws and regulations, licensure requirements and accreditation standards. The Scripps Community Connect EHR Practices and Procedures may be amended, modified, or revised from time-to-time by Scripps. The most current Scripps Community Connect EHR Practices and Procedures will be posted on Scripps ACO Portal.

II. Scripps ACO Community Connect *Authorized User Agreement*

Access to Scripps Community Connect EHR (collectively as the "EpicCare EHR") is contingent upon (electronic) execution the Authorized User Agreement. Key information and requirements for Users included in this agreement include:

1. Scripps or its designee will provide User with a Username and unique password, or ability to select a unique password, ("Log-on Credentials") for access to the EpicCare EHR for the limited and sole purpose of providing healthcare and/or healthcare support services. User's rights to access and use the EpicCare EHR are non-exclusive and non-transferable.
    - User agrees to take appropriate measures to safeguard his/her log-on credentials and will not allow any other individual to access the EpicCare EHR using its log-on credentials. User shall notify Practice and Scripps immediately if User believes his/her log-on credentials have been compromised.
2. User's access to the EpicCare EHR will be recorded electronically, and User consents to having all or any portion of his/her access to and use of the EpicCare EHR recorded, audited and/or reviewed at any time by Practice, Scripps or their respective designees.
3. Information, including Protected Health Information (PHI), that the User accesses from or through the EpicCare EHR is intended solely for the use by User to provide legitimate healthcare or healthcare support services in accordance with Practice's internal business purposes, all as specified in the Software Access Agreement. Access to and/or use of the EpicCare EHR for any other purpose is expressly prohibited.

4. Information, including PHI, User accesses from or through the EpicCare EHR is intended solely for the use by User to provide legitimate healthcare or healthcare support services in accordance with Practice's internal business purposes, all as specified in the Software Access Agreement. Access to and/or use of the EpicCare EHR for any other purpose is prohibited.
5. User agrees to comply with all federal and state laws and regulations governing the privacy and security of personal information and PHI, including without limitation, HIPAA and related regulations (collectively, "Applicable Laws").
6. User agrees to use appropriate safeguards and practices to prevent disclosure or use of PHI other than as expressly permitted by this Agreement.
7. If User becomes aware of any disclosure or use of PHI, or other information, which would violate this Agreement ("Unauthorized Disclosure"), User agrees to:
   - Mitigate, to the extent practicable, any harmful effect that is known to User related to an Unauthorized Disclosure;
   - Immediately report the Unauthorized Disclosure to Practice and Scripps; and
   - Provide full cooperation and assistance to Practice and Scripps or its designee in the investigation and mitigation of the Unauthorized Disclosure.
8. Suspension, Termination, and Disciplinary Action
   - Practice has the right to impose disciplinary actions against a User for any failure to comply with the terms and conditions of this Agreement, including without limitation, requiring User to repeat his/her HIPAA training, restricting or suspending User's access to the EpicCare EHR, and/or termination.
   - Scripps and Practice have the right to immediately suspend User's access to the EpicCare EHR at any time for any reason. Additionally, Practice has the right to immediately terminate this Agreement and discontinue access to the EpicCare EHR at any time for any reason.

III. Privacy & Information Security Key Points:

1. **Access to Patient Accounts:** Access to Scripps Community Connect EHR is a privilege that can be revoked if Scripps EHR Practices and Procedures are not followed.
   - An individual must only access patient records that he/she is authorized to access. Authorized means the individual has an approved need to access, review and/or use the information in order to perform the duties of his or her position, e.g. is related to employer or contractor's practice.
   - Minimum Necessary Restriction - An individual must only access the information actually needed for the business purpose on hand. Health information access under all circumstances should be limited to the amount reasonably necessary to achieve the purpose of the access.
   - If a User is ever unsure about whether to access a patient's record, he/she should ask a supervisor or the practice's privacy official first. Information systems activity and network access is monitored and reviewed on a regular basis as part of the Privacy Program activities.

2. **Violations and Sanctions:** If Scripps determines a privacy violation occurred, the violation will be reported to the practice. Privacy violations may result in termination of the User's account and the practice's ability to access data if repeated violations occur.
3. **Password Protection**: Protect your Scripps computer password; do not share it with any individual or post it anywhere. You are accountable for every action taken under your User Name/password. Your Scripps User Name paired with your password is your electronic signature.
4. **Reporting Lost or Stolen Scripps Computer Equipment, handheld devices and/ or Data Storage Devices:** Immediately notify the Scripps Service Desk at (858-678-7500). Service Desk Analysts are available 24/7 to assist with lost/ stolen devices.
5. **Avoiding Network Security & Email Phishing scams:** These scams send authentic-looking emails that appear try to trick a User into giving away his/her User ID and password. Protect your Scripps User ID and password as follows:
    - Do not follow unsolicited web links in email messages or submit any information to web pages in links.
    - Never enter your Scripps User ID and password within a web link that was embedded in an email.
    - Do not use your Scripps User ID and password for personal email, Facebook, Twitter or other personal accounts.
    - Use caution when opening unfamiliar email attachments.
6. **Immediately report any suspicious events**: this includes (but is not limited to) a phishing attempt (see #5 above), a compromised password, a Ransomware event, or other unusual activity. Report to your supervisor and directly to the Scripps Service Desk (858) 678-7500.
7. **Immediately report any privacy incidents**: this includes a suspected privacy breach, including inappropriate access. Report to your supervisor and directly to the Scripps Privacy Office (858) 678-6819.

Addendum: Regulatory Background Information

Note: this section is intended solely as education, and should not solely be relied upon by the practice to determine whether an incident qualifies as a privacy violation, or be construed as legal advice.

Federal and State Privacy & Information Security Laws: the following section is intended to familiarize the practice with a high-level summary of the sections of Federal and CA law that address breaches of the Federal Privacy Rule, and/or violations of CA law resulting in an unauthorized access, use or disclosure of patient information (collectively referred to as a "privacy violation"), and the required reporting obligations. Hyperlinks to the regulations are included below.

Federal - The HIPAA Privacy Rule contains the federal regulations address the privacy and security of patient information.

> ***Breach*** *(defined in federal law) means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted, by the Privacy Rule, which compromises the security or privacy of the PHI.*

External Notification Requirement - Federal Department of Health and Human Services (DHHS): if an event or privacy violation is determined to be reportable, HIPAA requires reporting to the DHHS Secretary as follows:

a) Breaches affecting less than 500 individuals – DHHS requires reporting within 60 days after the end of each calendar year to the DHHS website
b) A breach affecting 500 or more individuals – the media, as well as the Secretary, and the Attorney General as appropriate, shall be notified within 60-days of determination that an incident meets the Federal Breach Reporting requirements.

Patient Notification- If the privacy violation is deemed reportable under federal law (applies to licensed and unlicensed facilities), the report is required to be made in writing to the patient within 60 days of the discovery of the breach.

a) To meet the federal breach notification requirements written notice to the patient shall include the following elements:
    1. A description of what happened, including date of breach and date breach was discovered, if known;
    2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, account number, diagnosis, disability code, or other types of information where involved);
    3. Any steps the individual should take to protect themselves from potential harm resulting in the breach;
    4. A brief description of the steps Scripps took to investigate the breach, mitigate harm to the individual, and to protect against future breaches.
    5. Contact procedures if the person has additional questions or learn additional information, which must include one of the following: a toll-free phone number, an email address, web site, or postal address. Scripps letter template normally provides the postal address and direct phone numbers of the Privacy Officer and the sender of the letter.

State – There are several California privacy laws including the California Confidential Medical Information Act (CMIA), codified in California Civil Code § 56, which is intended to protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider. The CMIA protects the confidentiality of individually identifiable medical information obtained by a health care provider and includes (but is not limited to) the following:

- ✓ CMIA prohibits a health care provider, health care service plan, or contractor from disclosing medical information regarding a patient, enrollee, or subscriber without first obtaining an authorization, except as specified.
- ✓ CMIA requires a health care provider, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records to do so in a manner that preserves the confidentiality of the information contained within those records.
- ✓ Any person or entity who knowingly and willfully obtains, discloses, or uses medical information in violation of CMIA shall be liable for an administrative fines.

> ***Unauthorized*** *(defined in CA law) means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the CA Confidentiality of Medical Information Act or any other statute or regulation governing the lawful access, use, or disclosure of medical information.*

External Notification Requirement - CA Department of Public Health: Under section CCC unauthorized access is reportable for licensed facilities (at Scripps this includes hospitals and Home Health). If Scripps determines a privacy violation to be reportable to CDPH, Scripps must notify CDPH in writing, that an unlawful or unauthorized access, use or disclosure of medical information has occurred. The law requires that this report be made no later than fifteen (15) business days after detection. The Hospital Risk Manager is responsible for reporting to CDPH.

Patient Notification Requirement: If the privacy violation is deemed reportable to CDPH under CA law (for a licensed facility), the report is required to be made in writing to the patient (at the last known address) no later than fifteen (15) business days after determination that unlawful or unauthorized access, use of disclosure of medical information has occurred.