Scripps

TITLE: Information Systems, Non-Employee Access

IDENTIFIER: S-FW-IM-3004

APPROVED: Executive Cabinet 4/23/19
ORIGINAL: 03/05
REVISED: 04/11, 07/13, 01/15, 03/18, 04/19
REVIEWED:

EFFECTIVE DATE:

☒ **Acute Care:**	**ENC**	**5/7/19**	**GH**	**5/7/19**
	LJ	**5/7/19**	**MER**	**5/7/19**
☒ **Ambulatory:**	**SMF**	**5/7/19**		
☒ **Home-based Care:**	**HH**	**5/7/19**		
☒ **SHAS:**		**5/7/19**		

KEYWORDS: Access, Data, Computer, Emergency, Privacy, Remote, Security, Termination, User Account, Reconfirmation, Identity, Identity Validation, Access Request Form, Non-Employee Access, Approval, Segregation of Duties

I. PURPOSE

This policy and supporting procedures establish requirements, roles and responsibilities, and defines the process to administer non-employee access privileges including the approval, establishment, change, monitoring, periodic reconfirmation, and termination of information resources access privileges. Attachments to this policy may be revised independently of the policy under the direction of IS Executive Leadership and/or Scripps Compliance & Privacy Officer.

II. POLICY

A. All access by non-employees to any Scripps computer and information technology resource is subject to this policy. Scripps computer resources include systems that are administered by Scripps or by a third party contracted by Scripps. Access privileges to Scripps information systems are dependent upon the initial and ongoing satisfaction of the requirements of this policy and procedures as well as *Mandatory Administrative Requirements for Non-employee Access to Scripps Information Systems* established in Attachment A.

B. Types of Non-employees requiring varying degrees of access to Scripps information technology resources include credentialed providers (e.g. SHPS/SMF Contracted Providers), Medical Staff and their office employees, ACO Providers and their office staff, , Service Agreement Contractors, Supplemental Staffing (Contracted Labor), Contract Patient Care staff, Volunteers, Students, Contracted Hospital-Based Physician Medical Groups' Third Party Billing Companies or Staff Members, employees of government agencies, and others as appropriate. See Attachment A of this Policy for *Mandatory Administrative Requirements for Non-employee Access to Scripps Information Systems.*

C. Granting of Non-employee access is permitted only when all the following conditions are met:

1. Clear and justifiably valid Scripps business or clinical need exists.
2. Access is supported by an executed written contract or agreement.
3. Access is approved by an authorized designated Scripps sponsor.
4. Identity of the information technology resource user is validated by Scripps or designated party per contract by inspection of a valid government issued identification document such as an active driver's license or passport.

5. Unique identifier (PIN) for non-employee user is established by:
    a. User providing the last four digits of their social security number (SSN) as a unique identifier and Month/Date of birth as a security question answer for IS Help Desk identity validation for password reset.
    b. Unique 4-digit PIN for employees of government agencies and/or certain contracted vendors who may be instructed by their employers not to provide any part of their SSN. In this case, the Identity and Access Management Team will ask the person being granted access to select a unique 4-digit PIN in lieu of SSN and a security question to be used by IS HelpDesk for authorization in re-setting password.
6. Unique Scripps Corporate IDs will be assigned by the Identity and Access Management Team or HR Central Staffing to identify all non-employee users of Scripps information systems.
7. Approval of Access:
    a. Data/Information Owners are the designated Scripps executives responsible for specific information systems and their data. They or their designees are responsible for defining appropriate role-based access and for authorizing access on an individual basis, when pre-defined roles are not established for a requested access.
    b. Pre-Established Role-Based Access (RBAC) - the implementation of Epic included a robust RBAC program. Standard access by roles were determined with key stakeholders, which were then approved by the Data/Information Owners.
        i. Requests for modifications to standard RBAC are reviewed through Scripps Data Governance processes.
8. All Administrative Requirements per Attachment A have been met (forms, education provided, etc.)
9. Access to Epic will only be granted upon completion of certified training requirements pre-determined by Scripps (outlined in Attachment A).

D. Access levels and entitlements (enabled system privileges and capabilities) are granted in accordance with the following principles:

1. ***Role-based Access****:* The access entitlements to perform certain on-line tasks are assigned to specific pre-defined roles (role matrix) consistent with scope of practice. For example, nurses Nurse Role and Physicians role. Role based access and entitlements are determined and granted based on the following:
    a. The Data/Information Owner has formally approved the role matrix documenting the defined application access roles for employees and non-employees as well as access to other application components such as the database and/or operating system. The role matrix may also define specific groups requiring access to specified roles.
    b. Need to Know: A user is assigned to an Access Role which must be consistent with the individual's job duties establishing an appropriate need to know.
    c. Minimum Necessary: A user is assigned an Access Role that limits the user, to the best of the system's ability, to only information necessary to comply with the user's specific information requirements.

d. Application Intended Use: User’s access to an information resource must be consistent with the application’s intended use.

e. Users Scope of Practice: A user’s access must be consistent with licensure regulations, for example prescription ordering functions for an M.D. versus an R.N.

f. Non Role Based Privileges: When a user requires a type of access that is not covered in the approved role matrix then each individual request for such access shall be formally approved by the Data Owner (or their designee)

2. ***Time-Limited Access**:* Access for non-employees is granted on a time-limited basis which defaults to 90 days. In certain instances a contract/agreement or other standard processes may establish the time limited access to be up to one year. Authorized requestors will be notified by the Identity and Access Management Team when an account is expiring. In addition, the continuation of access will be re-confirmed by the responsible Data Steward with the non-employees’ Scripps designated sponsor at least annually.

3. ***Remote Access**:* Remote access to Scripps information resources is an additional privilege granted to certain non-employee users on a needs basis. Such access is enabled only through Scripps approved secure methods in accordance with the Remote Access Standard S-FW-IM-9031. Specific attestations are required from all remote users related to security safeguards on the computer equipment used to access Scripps Information or technology resource systems.

4. ***Emergency Access*:** When normal role-based access or the established request, approval and documentation procedures are not practical to support patient safety requirements or prevent significant negative impact to critical business operations, a Scripps Director or above may request in writing that the responsible Data Steward temporarily create or modify a user account with escalated privileges. Such emergency access will be documented as required within 24 hours.

E. Logs of Access and Activities: Non-employees granted access to Scripps information systems should be informed by designated requestors that all access to Scripps information systems is logged and user activities are subject to review for investigations and monitoring for compliance with Scripps policies. Information access violations, including unauthorized access outside of role-based privileges, or failure to comply with Scripps policies may result in violations of State and Federal Privacy Regulations. Non-compliance with Scripps policies can result in required reporting to regulatory agencies, suspension or termination of user’s access, and remedies including termination of business relationship with Scripps or legal action.

F. Known or suspected violations, or unauthorized access, must be immediately reported to Scripps. Users should report using one of the two methods listed below, which depends on the type of issue. However if the user inadvertently reports via the wrong mechanism, the Service Desk will notify the Privacy Team and vice versa.

1. Suspected privacy incidents or violations (e.g. inappropriate access of records aka “snooping”) must be immediately reported to the Scripps Privacy Office 858-678-6819

2. Suspected Information Security incidents, including compromised passwords, must be immediately reported via the Scripps Service Desk 858-678-7500 (or tie line 318-7500)

III. RESPONSIBLITIES

A. **Authorized Requestors/Sponsors - as designated in Attachment A:** (such as HR Central Staffing, Medical Staff, ,Centralized Credentialing, Registry Staffing Office, Graduate Medical Education, Volunteer Offices, Director or above) must:

1. Complete access request process in accordance with the mandatory administrative requirements and timeframes established in this policy.
2. If the requested user is unknown to the person making the access request (e.g. outside clinical trial monitor, external auditor or surveyor) the requestor should validate the user's identity by visually inspecting government issued photo identification. (e.g., driver's license or passport).
3. Schedule training for non-employee on the requested system to support proper use of system technology and maintaining data confidentiality and integrity.
4. Upon request from Scripps Privacy Office, review monitoring logs of access activity for the non-employee to validate that patient accounts accessed were appropriate for the specified business purpose and respond within requested timeframe. .
5. Respond timely to annual user reconfirmation requests from Data Stewards to review and confirm whether users under their supervision still require information system access. Send requests for necessary access disablement within two weeks from receipt of reconfirmation notice.
6. Immediately notify the Service Desk 858-678-7500 to terminate user access upon a non-employee user's termination from third party employment or affiliation or termination of the contract/ agreement with Scripps, the Scripps designated sponsor must notify the IS Help Desk 858-678-7500 to terminate user access.
7. Designated authorizing sponsor or cost center director is responsible for ensuring all Scripps computer resources (laptops, desktops, assets issued for home use, handheld devices, removable storage devices, and data files keys, and badges) assigned to a non-employee are returned and collected. Follow all applicable required termination procedures related to non-employees system access in a manner consistent with employees' termination as addressed in the related Scripps policy S-FW-HR-0212 Termination of Employment.

B. **All individuals granted non-employee information systems access privileges must:**

1. Sign a Scripps *Confidentiality and Information Security; Agreement.*
2. If requested, provide a valid government issued identification document, such as an active driver's license or passport.
3. Complete all required administrative requirements as outlined in Attachment A.
4. Not access or attempt to access information above and beyond what is required by their job duties or contracted services, even if the system allows them to do so.

5. Never share their password to any Scripps systems.
6. Immediately report suspected lost or stolen equipment containing Scripps data or suspected unauthorized system access to the IS-Help Desk.
7. Return all Scripps-owned information system related assets and data files upon termination of Scripps contractual relationship.

C. **Identity and Access Management (IAM) Team**

1. Creates unique Corporate IDs for all non-employee users when required documents are completed and authorized as outlined in Attachment A. Exceptions: HR Central staffing for contracted employees and PMA Systems and Reporting Group for referring physicians.
2. Assigns unique PIN numbers and records security question for all non-employee users.
3. Ensures that dormant Scripps Network Accounts are disabled in accordance with Scripps Policy in collaboration with the Windows Computing Platform Group.
4. Maintains official repository of all documents that authorize non-employee access in the Remedy system.
5. Notifies designated requestors regarding accounts scheduled for time-limited deactivation and provides opportunity for re-authorizing before expiration.

D. **Data Owners and Data Steward** responsibilities are outlined in S-FW-IM-3000.

IV. ATTACHMENTS

A. Mandatory Requirements for Non-Employee Access to Scripps Information Systems (revised 02/2020)

B. Epic Connectivity Quick Reference

C. Community Connect EHR Practices and Procedures

V. RELATED PRACTICE DOCUMENTS

A. Business Associate Policy; S-FW-LD-1007

B. Computer, Network and E-mail Usage; S-FW-IM-2001

C. Confidentiality of Information (Patient, Financial, Employee, and Other Sensitive and Proprietary Information); S-FW-IM-0201

D. Health Information, Access, Use and Disclosure; S-FM-IM-0203

E. Information Security Incident Reporting and Response Policy; S-FW-IM-3005

F. Information Systems, Employee Access; S-FW-IM-3002

G. Information Security Program Policy; S-FW-IM-3000

H. Termination of Employment Policy; S-FW-HR-0212

I. Information Security Program Policy; S-FW-IM-3000

J. Access to Patient Care Facilities, Non-Employee Requirements for; S-FW-EC-1157

VI. RELATED FORMS

A. Access Request Form- Non-Employee; SW-IM-3004 A

B. Access Request Form – Multiple Students; SW-IM-3004 B
Student Placement Office may use Department Spreadsheet Equivalent

C. Network Access Release of Liability Waiver; SW-IM-3004 C

D. Personal Computer Access to Scripps Network Security Safeguard Attestation; SW-IM-3004 D

E. Confidentiality and Information Security Agreement for Affiliated Physician Office Staff; SW-IM-3004 H

F. Research Confidentiality and Non-Disclosure Agreement; SW-IM-0201 B

G. Confidentiality and Non-Disclosure Agreement; SW-IM-020s1 C

H. Business Associate Agreement (BAA) and Coversheet; SW-LD-1007

VII. REFERENCES

A. Security and Electronic Standards; 45 CFR Part 142

B. HIPAA Privacy Rule, 45 CFR Parts 160, 162 and 164.

C. California State Privacy Regulations: Health & Code 1280.1, 1280.15, 1280.3 &120755 - 121023; and Civil Code 56.06 & 1789.29

D. Information Systems, Employee Access; S-FW-IM-3002

VIII. SUPERSEDED

Information Systems, Non-Employee Access; S-FW-IM-3004, 3/18

DEVELOPMENT SUMMARY

01/29/2020 Revision Attachment A: approved by K. Lindsey, C. Kegley, G. Soderstrom, M. Hughes, J. Coughlin

7. Community Connect Users
   - Access reconfirmation timeframe to be annual
   - Identifying and communicating termination of access to IAM will be the responsibility of Community Connect Account / Practice Managers**.**

04/19 Revision: Attachment C- Scripps Community Connect EHR (EpicCare EHR) Practices & Procedures added.

Development Workgroup

Representation	Member Name	Member Title/Discipline
Process Owner	Clark Kegley	AVP, Information Services
Workgroup Leader	Jan Coughlin	Corporate Compliance & Privacy Officer
Workgroup Member	Cyrus Bulsara	Manager, Information Security
Workgroup Member	Kristina Lindsey	Director, IS Service Delivery
Workgroup Member	Pedro Ramirez	Manager, IS Service Delivery
Workgroup Member	Paul Soto	IS Support Tech, IAM
Workgroup Member	Brian Leno	Lead, Application Analyst
Workgroup Member	Shane Thielman	AVP, Information Services

ENDORSEMENTS and APPROVALS

Function	Title/Position	Date of Endorsement and Approval
Executive Sponsor	Andy Crowder, Corp. SVP/CIO	4/10/19
Legal Office	Brad Ellis, CVP/ Assistant General Counsel	5/1/19
Executive Cabinet	Chris Van Gorder, President & CEO	4/23/19

ATTACHMENT A: Mandatory Requirements for Non-Employee Access to Scripps Information Systems
Information Systems, Non-Employee Access
Identifier: S-FW-IM-3004 Date: 02/2020 Page: 1 of 7

For questions and additional guidance call the Service Desk at 858-678-7500.

Ref #	User Category	Request Access "Authorized Approvers"	Required Access Request Form	Education and Required Documentation	Access Reconfirmation	Termination
1.	**Non-Employee Supplemental Staffing Labor: Traveler, Registry, Contracted Consultants**	Scripps Supervisor/Manager will contact HR Central Staffing (HRCS). HRCS submits OLS form to IAM via ServiceNow for processing.	Outside Data Labor Sheet.	Supplemental Staffing signs Confidentiality and Non-Disclosure Agreement as part of the HR Central Staffing Process. Access education/training for clinical systems.	Annual Reconfirmation completed by HR Central Staffing through Help Desk.	Notify HR Central Staffing of termination. Call IS Help Desk to obtain list of assets used by Supplemental Staffing and request access termination. Collect Assets. Complete Termination Checklist.
2.	**Non-Employee - Service Agreement Contractors:** **(**e.g., Master Contracts, Children's Hospitals, Radiology Services Technicians, Security Services, Siemens, GE, Phillips, Managed Care provider relations, UCSD)	Director Sponsor verifies that individual is under a written agreement/contract reviewed by Scripps Legal to provide services for Scripps. Director Sponsor provides a copy of **executed** (signed by both parties) contract to IAM Team.	Non-Employee Access Request Form. Confidentiality And Non-Disclosure Agreement.	Contract / agreement reviewed by Scripps Legal. Note: CNDA is usually an included clause in the master Scripps contract. If unsure check with Legal Office. Healthcare check if working on hospital premises. Personal Computer Access to Scripps Network Security Safeguard Attestation. Network Access Release Of Liability Waiver only required if remote/VPN/Citrix access is needed.	Annual Reconfirmation (Identity and Access Management, Data Stewards).	Director Sponsor must: Notify IS Help Desk if individual is relieved, agreement is prematurely severed, or upon termination of relationship or end of volunteer services. Call IS Help Desk to obtain a list of Scripps assets used by contractor. Collect Scripps Assets.

Ref #	User Category	Request Access "Authorized Approvers"	Required Access Request Form	Education and Required Documentation	Access Reconfirmation	Termination
3.	**Non-Employee Credentialed Medical Staff:** **Physicians** **Allied Health Practitioners**	Medical Staff Office validate that physician is an active member of the medical staff or member of the Scripps Clinic or Scripps Costal Medical Center.	AARF is used. NOTE: For temporary privileges, Medical Staff a non-employee access request form must document start and end date.	Confidentiality and Non-Disclosure Agreement. Access education for clinical systems. Healthcare check if working on hospital premises.	Annual Reconfirmation (IAM, Data Stewards).	Medical Staff Manager must: Call IS Help Desk to request Remedy incident to disable access and obtain list of Scripps assets used by physician or allied health practitioner and request access termination. Collect Scripps assets. Complete Termination Checklist.
4.	**Non-Employee Students** **Graduate Medical Education**	Individual must be under an Educational Affiliation Agreement for non-physician students - Personnel in the Staff Development Office to verify. Graduate Medical Education Office for MD Students.	Non-Employee Access Request Form. Automated Non-Employee Access Form (NAARF)	Confidentiality and Non-Disclosure Agreement. Access education /training or clinical systems. Healthcare check if working on hospital premises.	Annual Reconfirmation (IAM, Data Stewards).	Termination is completed by Identity and Access Management (IAT) team who validates termination with the Staff Development Office and GME Office annually. A new Access Request Form is requested to renew access.

Ref #	User Category	Request Access "Authorized Approvers"	Required Access Request Form	Education and Required Documentation	Access Reconfirmation	Termination
5.	**Third Party Billing Companies for Hospital-Based Contracted Physician Groups**	Regional Chief Executive or Chief Operating Executive or and their designee (Director or above). 3-way Contract prepared/approved as to form by Scripps Legal. Sponsor provides a copy of **signed** contract to IAM Team.	Non-Employee Access Request Form With required specific 3-way contract to be executed.	Contract or agreement reviewed by Scripps Legal Office. Forms C and D (Personal Computer Access to Scripps Network and Security Safeguard Attestation. Network Access Release Of Liability Waiver) required.	90 Days (IAM).	Notify Service Desk if individual is relieved, prematurely severs agreement, or upon termination of relationship or end of access requirements. Sponsoring Regional Chief Executive and Backup must notify Service Desk if individual is relieved, agreement is prematurely severed, or upon termination of relationship with Scripps.

Ref #	User Category	Request Access "Authorized Approvers"	Required Access Request Form	Education and Required Documentation	Access Reconfirmation	Termination
6.	**Employees of Physicians on Medical Staff and Employees of Providers Contracted with the ACO**	Epic Care Link - Web-based with limited access to Epic by design, e.g. office staff can only see patient charts associated to the provider they work for. Users with Epic Care Link do not have and account or access to the Scripps network. Epic Care Link can be requested by a sponsoring physician leader or executive and approved by Clinical Leadership Council; IS application director approval for NARF.	Non-Employee Access Request Form (NARF)	Scripps Health Epic Access Agreement (Web Access)- requires push of awareness materials (e.g. user guide) Confidentiality and Information Security Agreement. Personal Computer Access to Scripps Network Security Safeguard Attestation. Network Access Release Of Liability Waiver; only required if remote/VPN/Citrix access is needed.	90 Days (IAM).	Notify Service Desk if individual is relieved, prematurely severs agreement, or upon termination of relationship or end of access requirements.

Ref #	User Category	Request Access "Authorized Approvers"	Required Access Request Form	Education and Required Documentation	Access Reconfirmation	Termination
		Epic Citrix-Based Access – includes access to Scripps Hospital & Ambulatory data, with the ability to enter hospital IP and OP orders and case requests. Epic Citrix-Based access can be requested by Centralized Credentialing Director.	Non-Employee Access Request Form (NARF)	Scripps Health Epic Access Agreement (Citrix Access)- requires completion of classroom training. Confidentiality and Information Security Agreement	90 Days (IAM).	Notify Service Desk if individual is relieved, prematurely severs agreement, or upon termination of relationship or end of access requirements.
		Epic Citrix-Based Access (View Only) – includes access to Scripps Hospital & Ambulatory data, in view only format Epic Citrix-Based Access (View Only) can be requested by Centralized Credentialing Director	Non-Employee Access Request Form (NARF)	Scripps Health Epic Access Agreement (Citrix Access)- requires completion of classroom training. Confidentiality and Information Security Agreement	90 Days (IAM).	Notify Service Desk if individual is relieved, prematurely severs agreement, or upon termination of relationship or end of access requirements.

Ref #	User Category	Request Access “Authorized Approvers”	Required Access Request Form	Education and Required Documentation	Access Reconfirmation	Termination
7.	**Community Connect Users**	ACO Administration *(Sr. Director, ACO Ops or Manager, Patient Outreach)*	Non-Employee Access Request Form (NARF)	Community Connect End-User License Agreement Confidentiality and Information Security Agreement Attachment C- Scripps Community Connect EHR Practices & Procedures (posted on Scripps ACO Portal).	Annual	Users are set up with no termination date specified. Access is handled by Scripps CC Account Managers. CC Account Managers will work with Practice Managers to ensure terminations are communicated to IAM (as required per license agreement) to facilitate the termination of access.
8.	**Federally Qualified Health Care Center or Other Contracted Group Approved by Scripps Legal**	Scripps Legal Office Attorney and Scripps Privacy Officer	Non-Employee Access Request Form (NARF)	Specific Contract Approved as to Form by Scripps Legal Confidentiality and Information Security Agreement	90 Days (IAM).	Notify Service Desk if individual is relieved, prematurely severs agreement, or upon termination of relationship or end of access requirements.

Ref #	User Category	Request Access “Authorized Approvers”	Required Access Request Form	Education and Required Documentation	Access Reconfirmation	Termination
9.	**Employees of government agencies, and other entities that have mandated auditing requirements**: Insurance Payers, Research Monitors	Health Information Director or Manager. Risk Manager COE/CE	Non-Employee Access Request Form.	If not mandatory by regulations, a Contract or agreement reviewed by Scripps Legal Office.	90 Days (IAM).	Notify Service Desk if individual is relieved, prematurely severs agreement, or upon termination of relationship or end of access requirements. Sponsoring Health Information Director and backup and Backup must notify Service Desk if individual is relieved, agreement is prematurely severed, or upon termination of relationship with Scripps.

ATTACHMENT B: Epic Connectivity for Independent Physicians/Staff Quick Reference

Information Systems, Non-Employee Access

Identifier: S-FW-IM-3004 Date: 04/19 Page: 1 of 1

EPIC CONNECTIVITY FOR INDEPENDENT PHYSICIANS/STAFF

	EpicCare Link	**Epic Citrix-Based Access**	**Epic Citrix-Based Access (View Only)**	**Community Connect**
Who	• Independent physicians credentialed at Scripps and their office staff; • Referring physicians	• Independent physicians credentialed at Scripps and their office staff	• Independent physicians credentialed at Scripps and their office staff	• Members of the Scripps Accountable Care Organization (ACO) - as determined by the ACO Board of Directors
Patient Record	Web-based, view-only Portal without the ability to update a patient chart. With EpicCare Link, user has limited access to Epic by design, e.g. office staff can only see patient charts associated to the provider they work for.	Access to Epic with specific role established to support appropriate functionality for office staff.	Access would exist to all patients (identical to full Citrix access) Chart Review with patient look up Dashboard with tip sheets for viewing patient data No service area restrictions	Office EMR – Hospital EMR One Patient / One Record
Orders/Referrals	Enter Radiology, Lab and Referral orders	Enter Hospital Inpatient & Outpatient Orders and Case Requests	No ordering No documentation	Enter All Orders
Lab Results	View Epic Record Order Outpatient/Ambulatory at Scripps	View Epic Record Order Outpatient/Ambulatory at Scripps	View Epic Record	View Epic Record Order All
Private Practice Billing	N/A	Charge Capture Report on Inpatient Work for Office Billing Service	N/A	Each practices maintains independent billing operations or uses a billing services
Notification of Patient Care Changes	Email Notification	Epic *InBasket*	Epic *InBasket*	Epic *InBasket*

ATTACHMENT C: Scripps Community Connect EHR Practices & Procedures

Information Systems, Non-Employee Access

Identifier: S-FW-IM-3004 Date: 04/19 Page: 1 of 5

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.