TITLE: Information Systems, Non-Employee Access

IDENTIFIER: S-FW-IM-3004

APPROVED: Executive Cabinet 3/13/18
ORIGINAL: 03/05
REVISED: 04/11, 07/13, 01/15, 03/18
REVIEWED:

EFFECTIVE DATE: 3/27/18

☒ Acute Care:	ENC	3/27/18	GH	3/27/18
	LJ	3/27/18	MER	3/27/18
☒ Ambulatory:	SMF	3/27/18		
☒ Home-based Care:	HH	3/27/18		
☒ SHAS:		3/27/18		

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.

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 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 Appendix 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.
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

B. Epic Connectivity Quick Reference

V. RELATED POLICIES

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-0201 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, 1/15

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.

Ref #	User Category	Request Access "Authorized Approvers"	Required Access Request Form	Education and Required Documentation.	Access Reconfirmation	Termination
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.
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.

		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	90 Days (IAM).	Notify Service Desk if individual is relieved, prematurely severs agreement, or upon termination of relationship or end of access requirements.
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.
9.	**Employees of government agencies, and other entities that have mandated auditing requirements:** **Insurance Payors** **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.

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*