Scripps

Policy: Confidentiality of Information

Effective: 01/11/22 **Identifier: S-FW-IM-0201**

Acute Care: ENC ☒ GR ☒ LJ ☒ MER ☒ Ambulatory ☒ SHAS ☒

PURPOSE: To establish requirements for the management and safeguarding of confidential information.

I. POLICY

A. **Personnel:** All Scripps Health workforce, including employees, volunteers, contractors, medical staff members, residents, fellows, interns, employees of medical groups contracted with the Scripps Medical Foundation, Authorized Affiliates, and other third parties are required to protect the confidentiality and security of Confidential Information related to protected health information (PHI), personal financial information (PFI) and other sensitive or proprietary Scripps organizational information.

B. **Data Ownership:** All data within the Scripps computer systems, including personal computers, intelligent workstations, networks, servers, and any storage media, are the sole property of Scripps and/or specifically designated partners and affiliates of Scripps and are subject to this policy.

Data pertaining to the organizational operations of Scripps entities, patients, and employees, but resident on privately-owned personal systems, shall be data-owned by Scripps, and are subject to this policy.

C. **Data Classification:** All data will be handled in accordance with the Data Classification System as defined in Attachment A *Data Classification.*

D. **Confidentiality and Non-Disclosure Agreement:**

1. All employees must review and sign the Scripps *Confidentiality and Non-Disclosure Agreement* (Refer to Related Forms) at the time of hire (i.e., at New Employee Orientation) and annually thereafter as part of their mandatory annual training.
2. Non-employees are required to sign this agreement as a condition of conducting business on behalf of Scripps, unless covered by a separate contractual arrangement approved by the Legal Department.
3. Signed statements shall be maintained in the appropriate file (i.e., an employee's personnel file, a contract service or credentialing file).

E. **Safeguarding of Information:** Confidential Information collected and/or generated within Scripps shall be maintained in a manner designed to restrict access to those individuals with a legitimate need to know the information. This includes applying Break the Glass, Minimum Necessary, clean desk policy etc. Refer to section V. Procedures, C, for a more comprehensive list.

F. **Handling of Confidential Information:** Accessing Confidential Information is strictly prohibited unless it is required by the individual's Scripps related responsibilities and abides by the Minimum Necessary standard. All individuals who have access to Confidential Information are prohibited from using, discussing, or revealing such information in any unauthorized manner. For example, individuals may not:

1. Access information belonging to themselves, other employees, co-workers, family, or friends.

2. Share information regarding coworkers, family, or friends unless there is a legitimate Scripps business purpose.

G. **Jeopardize the Integrity of Confidential Information**: Individuals may not interfere with the integrity of Scripps Confidential Information and/or information resources without appropriate authorization. Examples include shredding, destroying, altering, falsifying, dismantling, disfiguring, including preventing rightful access to confidential information (i.e., downloading malware to a Scripps asset).

H. **Violations of Confidentiality:** Scripps shall take appropriate corrective action up to and including loss of information system access privileges and/or termination of the employment or business relationship with Scripps with regard to any employee or non-employee who inappropriately accesses, uses, or discloses Confidential Information in violation of Scripps policies and/ or the law.

Unauthorized access use, download, or disclosure of confidential information may also result in legal action with respect to violation of federal and state privacy laws. Conduct need not be deliberate or intentional to violate this policy.

Examples of violations, which may be done intentionally or unintentionally include:

1. Unauthorized disclosure of Confidential Information (i.e., informal dialogue about a patient in the cafeteria, open office areas, hallways, or elevators; handing/mailing/faxing a patient's record to the wrong individual).
2. Inadvertent violation of confidentiality (i.e., accidentally accessing a computer account of the wrong patient, typing a number incorrectly when faxing patient records causing a mis-directed fax).
3. Sharing information outside of Scripps without a legitimate business purpose or in an unprotected manner (i.e., email that isn't encrypted, posting patient-related and/or confidential information on social networks).
4. Reproduction, (copy or photography) of Scripps confidential records including patient medical records without a legitimate business purpose.

I. **Termination of Employment or Scripps Business Relationship.** Employees who cease their employment or work with Scripps (voluntarily or involuntarily), or non-employees whose Scripps business relationship terminates, continue to be obligated to maintain confidentiality as defined in this policy and as set forth in the Confidentiality Non-Disclosure Agreement.

All such individuals must immediately cease all access to computer and information systems and return all originals and copies of documents containing Confidential Information in their custody or control no later than the last day of work/affiliation with Scripps.

II. RESPONSIBILITIES

A. **All Workforce Members** are responsible for signing the *Confidentiality Non-Disclosure Agreement* annually, complying will all elements of the agreement and:

1. Following all policies related to Confidentiality, Information Security and Management of Information and department specific procedures appropriate to their role and responsibilities.
2. Immediately reporting any substantiated or suspected violation of this policy (inadvertent or intentional). Refer to section V. Procedures, B.

B. **Professional Licensed Staff** will identify individuals (i.e., family/ friends) involved in a patient's care based on patient's expressed desires, clinical situation and patient care needs. The professional patient care staff may disclose relevant health

information unless patient has expressed a restriction on information or as required by law (Refer to Attachment A: Data Classification Matrix).

C. **Department Leadership** are responsible for:

1. Determining workforce members' access to Confidential Information to perform their job function in compliance with minimum necessary standard.
2. Developing and applying standard safeguards unique to the department, based on the department's work processes, for the security and protection of information.
3. Providing on-going education, training, and awareness of privacy and security policies and processes to all staff, as applicable to risks in their job functions.
4. Following established procedures for appropriate disposal of documents, equipment, removable storage media or other items containing Confidential Information.
5. Establishing that a Business Associate Agreement is in place when required for contractual relationships. See *Business Associate Agreement* policy.
6. Monitoring for compliance with Scripps policies pertaining to confidentiality, privacy, and security.
7. Applying corrective actions when policy violations have occurred.
8. Notifying appropriate departments of any workforce member's termination or transfer and to collect all Scripps property from employees in accordance with Scripps *Termination* policy S-FW-HR-0212 and from non-employees as stated within contractual arrangements.

III. PROCEDURES

A. **Reporting concerns or suspected violations.** Each individual must report any suspected violations of confidentiality or concerns through one of the existing compliance reporting channels. These include:

Supervisor, Manager, or Department Head or Human Resources Office	Scripps Privacy Team 858-678-6819 or online Report Form
Scripps Compliance & Patient Safety Alert line 1-888-424-2387 or Web Portal (available on Scripps Connect)	Scripps Information Services Help Desk 858-678-7500 (for security incidents)

B. **Apply and follow Standard safeguards to clinical and business work processes, to include the following:**

1. Apply Minimum Necessary standard to all use and disclosure of information.
2. Take care when in public spaces where conversations can easily be overheard by those that do not have a need to know (i.e., elevators, hallways, cafeteria).
3. Establish work processes and physical safeguards that minimize the occurrence of unintentional disclosure of information. For example: implement a double check method of two or more patient identifiers to ensure documents are being disclosed to the proper recipient; assess waiting areas and check-in areas to identify areas that could be made more private for patient conversations.
4. Dispose of paper, patient armband, DVDs, or other non-electronic items containing confidential information into shredding bins.

5. Apply appropriate electronic information security protection, i.e., encrypting emails and/or password protecting attachments containing PHI; using only encrypted Scripps assets to store PHI; use a Scripps fax cover sheet.
6. Obtain appropriate authorization for use and disclose of protected health information, i.e., Request/Authorization for Health Information (Medical Records), Designation of Personal Representative
7. Apply appropriate physical security for the protection of confidential information during use as well as transport, i.e., locking away devices or documents containing patient information when not in use and not leaving them visible in a parked car.
8. Implement a clean desk process to avoid leaving confidential information unattended, i.e., clean off desk at the end of the day and turn over documents with confidential information if you step away.
9. Securely seal and clearly mark confidential information that is being mailed or transported (i.e., interoffice mailed) making sure that confidential information is not visible through envelope windows.
10. Only use secure texting platforms for protected health information (PHI)
11. Scripps Social Media Guidelines should be followed when posting online about Scripps Health or when involving images and/or videos taken at a Scripps Health site.
12. Apply Break the Glass to a specific patient's entire Epic medical record to provide additional safeguards when requested or deemed appropriate. Refer to the Confidentiality Grid for guidance on the proper use of Break the Glass and related process.
13. Mark a patient's specific encounter in Epic as Private, when requested or deemed appropriate, to restrict the encounter from being visible to workforce that do not have the requisite security. Refer to the Confidentiality Grid for guidance on proper use and the impact of these designations to the patient's record.

IV. DEFINITIONS

Refer to Health Information Management Access, Use and Disclosure; S-FW-IM-0203 for HIPAA, Privacy, and related terminology.

A. **Authorized Affiliate**: Any member of the non-employee workforce that is eligible and authorized by Scripps Health or under contract or agreement to perform services as part of Scripps healthcare operations.

B. **Authorized:**

1. An individual is approved to access, review and/or use information in order to perform the duties of his or her position.
2. The appropriate designee has specifically approved access for an eligible person (has "authorized" access) by completing the appropriate documentation (i.e., NARF).

C. **Confidentiality**: **The obligation to protect the privacy of records and related business information includes not sharing this information with unauthorized individuals or entities.**

D. **Confidential Information** includes, but is not limited to PHI, PFI, patient records, personnel information, information regarding business plans and strategies, information gained from service on organizational or medical staff committees, and information gained from inquiries from families and friends of patients, other employees, the legal department, medical staff, external agencies or media. Confidential Information may be contained via any communication medium, including verbal, written, or electronic (e.g., facsimiles, e-mail, voicemail, pagers, text messages, Web Portals, photographs, social media such as *Facebook, Snap Chat, Tik Tok, Twitter, YouTube, Yelp*) all which are subject to the provisions of this policy.

E. **Data Classification:** Data stored in Scripps Systems will be classified into an appropriate category. Refer to Attachment A: Data Classification Matrix.

F. **Disclosure:** The release, transfer, provision of access to, or divulging in any manner, of PHI outside the entity holding the information. Disclosures require a specific authorization except if the disclosure is related to the provision of health care treatment, payment or healthcare operations of the entity responsible for the PHI, or under a limited data set or other allowable circumstances, as provided under the law.

G. **Inappropriate Disclosure of Protected Health Information**: Disclosing confidential information, regardless of intent, in verbal, written or electronic form can include the following:

1. Disclosing to individuals not involved in the care or treatment of patients,
2. Disclosing to individuals who are involved or know the patient, but have no need to know the information,
3. Disclosures made when in a setting where information can be read or transferred from an unattended computer monitor or through any violation of Scripps's Computer, Network, Email Usage Policy S-FW-IM-2001.

H. Individually Identifiable Health Information (IIHI)
A subset of health information, including demographic information collected from an individual, and:

Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or can be used to identify the individual. Specific identifiers include:

1. Names
2. All geographic designations smaller than a state, including street addresses, city, county, zip code
3. All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 indicatives of such age (although all persons over 89 may be aggregated into a single category)
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses

7. Social Security Numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate and license numbers
12. Vehicle Identifiers and serial numbers (including license plate numbers)
13. Device Identifiers and serial numbers
14. Web Universal Resource Locator (URL)
15. Internet Protocol (IP) address number
16. Biometric identifiers (including fingerprint or voice prints)
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code

I. **Limited Data Set**: Protected Health Information that excludes information that could directly identify an individual, but which could potentially be used to deduce that individual's identity. A Limited Data Set may not contain any of the identifiers under the definition of IIHI. A Limited Data Set may only be requested for research, public health or health care operations purposes.

J. **Minimum Necessary Restriction**: When a provider requests, uses or discloses protected health information of another provider, it must make reasonable efforts to limit the protected health information to the minimum amount of information necessary. Providers must identify those in its workforce who need access to a patient's information and to limit access accordingly. The restriction does not apply to disclosing medical records for treatment.

K. **Password**: A private code conforming to required format, known only to the user, to log in to the Scripps computer network or any Scripps service or application.

L. **Personal Financial Information** includes information such as social security numbers, bank account numbers, credit card numbers, etc.

M. **Protected Health Information (PHI)** is individually identifiable information, including genetic information, that is transmitted or maintained in any form or medium and that relates to the past, present or future physical or mental health or condition of a patient, the provision of health care to a patient, or the past, present or future payment for the provision of health care by a patient. Information is "individually identifiable" if it either identifies an individual or contains enough specific information to do so. ePHI designates PHI that is stored or processed in an electronic format.

N. **Workforce:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Scripps, is under the direct control of Scripps, regardless of whether or not they are paid by Scripps.

V. ATTACHMENTS

Data Classification Matrix

VI. REFERENCES

A. The Joint Commission Accreditation Standards: RI, IM

B. Health & Safety Code Section 199.20

C. 45 CFR – Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule. Federal Register January 25, 2013.
D. HIPAA Administrative Simplification Regulations Text – 45 CFR Parts 160, 162, and 164.
E. California State Confidentiality of Medical Information Act (Civil Code Section 56.10 et. seq.)
F. California Code of Regulations, Title 22, Section 70707(b)(8)

VII. RELATED PRACTICE DOCUMENTS & FORMS

A. Business Associate Agreement; S-FW-LD-1007
B. Computer, Network and Email Usage (Acceptable Use); S-FW-IM-2001
C. Disposal, Transfer, Reuse and Data Sanitization of Equipment, Hard Copy, Electronic Media, and Other Scripps Property; S-FW-IM-3008
D. Facsimile of Information; Scripps; S-FW-IM-2003
E. Health Information, Access, Use and Disclosure; S-FW-IM-0203
F. Disclosure of Hospital Patient Directory to the Public; S-FW-IM-0208
G. Performance Improvement and Corrective Action; S-FW-HR-0501
H. Termination of Employment; S-FW-HR-0212
I. Confidentiality and Non-Disclosure Agreement; SW-IM-0201 A
J. Research Confidentiality and Non-Disclosure Agreement; SW-IM-0201 B
K. Authorized Affiliate Confidentiality and Non-Disclosure Agreement; SW-IM-0201 C
L. Secure Chat Requirements: What You Need to Know; SW-IM-0201 D
M. Confidentiality Grid- Scenarios and Definitions; SW-IM-0201
F. Request/Authorization for Health Information (Medical Records); 100-8700-739SW
G. Designation of Personal Representative; 100-8720-066SW
H. Scripps Social Media Guidelines; SW-IM-2001 A

VIII. SUPERSEDED

Confidentiality of Information (Patient, Financial, Employee, and Other Sensitive and Proprietary Information); S-FW-IM-0201, 06/19

	Regulated Data	**Confidential Data**	**Internal Data**	**Public Data**
Data Classification	Data protected specifically by federal, state, or local laws and regulations: Includes Protected Health Information (PHI), Individually Identifiable Health Information (IIHI), and Personal Financial Information (PFI). **Sensitive (Restricted/ Regulated)** A sub-category of Protected Health Information that has further regulatory restrictions and therefore has additional safeguards and process requirements. This category includes the following only: 1. HIV test results 2. Mental Health records 3. Drug & Alcohol Treatment records 4. Genetic Testing Results 5. Self-Paid Accounts the patient designates NOT to go to 3rd party insurance payer.	Data that, if made available to unauthorized parties, may adversely affect individuals or the business of Scripps. This classification includes data that Scripps is required to keep confidential under contract or a confidentiality agreement with a third party, such as a vendor, payer, or donor.	Data that is proprietary or potentially sensitive and not intended to be shared with the public.	Data that may be disclosed to any person regardless of their affiliation Scripps.
Examples	1. Patient Demographic Information: MRN, Health insurance policy # 2. Social Security Number 3. Biometric identifiers 4. Driver's license # 5. All forms and types of medical information such as (but not limited to) diagnostic test results, progress notes, dictated visit summaries, discharge notes, surgical reports, etc. 6. Privileged attorney client communications 7. Clinical Research records. 8. Credit Card Number 9. Checking account or other Financial account numbers	1. Employment applications 2. Physician applications 3. Personnel files, benefits information, salary, 4. Complete birth date (mm/dd/yyyy) 5. Personal information: phone, address 6. Donor information 7. Budgets, plans, financial information 8. Contracts, Statements of Work (SOW), Memos of Understanding (MOU) 9. Email and phone logs 10. Merger and Acquisition 11. Strategic Plans 12. Litigation documentation	1. Scripps Outlook Directory 2. Telephone numbers 3. People Finder 4. Staff business calendars 5. Non-public Scripps policies and policy manuals 6. Scripps internal memos 7. Meeting minutes	1. Scripps.org 2. Press releases 3. Maps 4. Directory information

	Regulated Data	Confidential Data	Internal Data	Public Data
Access	Granted to as few persons as possible. Access must be obtained based on need to know, minimum necessary, specified job duties, and/or criteria authorized by the Scripps Data Governance Privacy and Security Workgroup. Remote access must be implemented only through Scripps approved and secure remote access technologies (SSL VPN, Terminal Services, Citrix etc.). **Sensitive (Restricted/Regulated)** health information: specific document types that include this type of PHI may be specifically flagged to require "Break-the-Glass" access in systems that have this capability.	Same as Regulated. Remote access must be implemented only through Scripps approved and secure remote access technologies (SSL VPN, Terminal Services, Citrix etc.).	Limited to those with a need to know. Third parties must sign a Confidentiality and Non-Disclosure Agreement. Remote access must be implemented only through Scripps approved remote access technologies.	No Requirements.
Release/ Disclosure	Confidential Information Data Request must be completed and approved prior to disclosure; third parties must sign Confidentiality and Non-Disclosure Agreement and BAA required when applicable. For some types of data specific authorization is required by the patient, Legal Department or other Scripps Management. Disclosures of **Sensitive** (**Restricted/Regulated)** health information is subject to specific authorization via an acknowledgement from the patient/legal representative for disclosures (purpose other than TPO). These data types are filtered out so that they are not included in data sent to Health Information Exchanges (HIEs).	Must be authorized prior to release by an approved Confidential Data Request.	Internal data generally should not be disclosed outside of Scripps without the permission of the person or group that created the data. Third parties must sign Confidentiality and Non-Disclosure Agreement.	No Requirements.

	Regulated Data	Confidential Data	Internal Data	Public Data
Electronic Storage	Prohibited from being stored on Scripps end user computing equipment and any removable storage device or media (e.g., USB, hard drives, CD/DVD, etc.) unless (a) authorized via the Removable Device Request Form and (b) requires encryption per the Encryption Standard. Prohibited to be stored on non-Scripps (personal) computing equipment. Third-party processing or storage services are prohibited from being used to store restricted/regulated information unless there has been an approved Scripps contracted vendor with a signed BAA (if required) or approved by the Scripps Information and Security Risk Committee.	Same as Regulated.	No Requirements.	No Requirements.
Electronic Transmission	Requires encryption when sent outside of Scripps. Email: Third party email services (e.g., Gmail, yahoo, etc.) are not appropriate for transmitting restricted/regulated information. Fax: Must be sent only to an approved and previously verified number and must be accompanied by the Scripps Facsimile Cover Sheet. FTP, EDI, HL7 to external parties must be encrypted.	Same as Regulated.	No special controls required when sent via a public network (i.e., outside the Scripps network).	No Requirements.

	Regulated Data	Confidential Data	Internal Data	Public Data
Display	Additional controls may be invoked, such as 'Break the Glass,' to record additional justification for viewing data in addition to the standard audit logging. Masking of some of the characters of a data element may be required, for example, displaying only the last 4 digits of the social security number. The amount of regulated information displayed on any screen or report should be the minimum necessary for the intended use. Credit Card number may not be displayed in any form.	Same as Regulated.	No Requirements	No Requirements.
Routine Handling	When not in use, must be stored in a closed container, such as a locked filed cabinet, locked drawer, locked room or an area controlled by a guard, cipher lock, badge reader or other physical security control that provides adequate protection and prevents unauthorized access.	Same as Regulated.	When not in use, must be stored in a closed container, such as a locked filed cabinet, locked drawer, locked room or an area controlled by a guard, cipher lock, badge reader or other physical security control that provides adequate protection and prevents unauthorized access by members of the public.	No Requirements.
Transportation	Direct delivery of encrypted media (hard drive, USB, DVD). Package tracking and receipt signature required, sealed envelope/package clearly marked as Confidential.	Same as Regulated.	No Requirements.	No Requirements.

	Regulated	Confidential	Internal	Public
Destruction	If no legal hold requirements, information should be managed in accordance with the Record Retention, Storage, Retrieval, and Destruction policy (S-FW-IM-0600). For equipment or electronic media, use only approved destruction methods as described in the secure destruction controls outlined in the Disposal, Transfer, Reuse and Data Sanitization of Equipment and Other Scripps Property Policy S-FW-IM-3008. If no legal hold requirements on confidential paper and/or paper containing protected health information (to include patient armbands) destruction is via shredding bins.	Same as Regulated.	If no legal hold requirements, information should be managed in accordance with the Record Retention, Storage, Retrieval, and Destruction policy (S-FW-IM-0600). For equipment or electronic media, use only approved destruction methods as described in the secure destruction controls as outlined in the Disposal, Transfer, Reuse and Data Sanitization of Equipment and Other Scripps Property Policy S-FW-IM-3008 - If no legal hold requirements on confidential paper and/or paper containing protected health information (to include patient armbands) destruction is via shredding bins.	No Requirements.
Improper Release	Contact the Privacy Office at (858) 678-6819 or if desired to be anonymous call the Scripps Compliance & Patient Safety Alertline at 1-888-424-2387 or via the online web portal on Scripps Connect.	Same as Regulated.	Immediately contact IS Help Desk at 858-678-7500.	No Requirements.