Scripps

TITLE: Confidentiality of Information (Patient, Financial, Employee, and Other Sensitive and Proprietary Information)

IDENTIFIER: S-FW-IM-0201	**EFFECTIVE DATE:**		
	☒ **Acute Care:**	**ENC 08/23/16**	**GH 08/23/16**
APPROVED: Executive Cabinet 07/19/16		**LJ 08/23/16**	**MER 08/23/16**
	☒ **Ambulatory:**	**SMF 08/23/16**	
ORIGINAL: 09/99	☒ **Home-based Care:**	**HH 08/23/16**	**HSPC 08/23/16**
REVISED: 02/01, 02/03, 11/05, 06/07, 11/10, 07/13, 10/13, 07/14, 07/16	☒ **SHAS:**	**08/23/16**	

KEYWORDS: Data Classification, Regulated, Confidential, Internal, Public

I. PURPOSE

To establish policy and direction for practices that protects the confidentiality and security of Confidential Information as defined by Scripps Data Classification System. Confidential Information includes protected health information (PHI), personal financial information (PFI) and other sensitive or proprietary Scripps organizational information. It is an important responsibility of each and every employee, as well as all medical staff members, contractors, volunteers, or other third parties having access to Scripps information, to support the protection of all Confidential Information is as required by Scripps policies and the law. This policy describes the responsibilities of all individuals who have access to any Confidential Information.

II. POLICY

Scripps is committed to safeguarding our patients' privacy, and the confidentiality of records and related information for all patients, employees, donors, and for organizational and operating information. It is the responsibility of every Scripps employee, medical staff member, contractor, volunteer, or other third party having access to Scripps information to follow all of Scripps policies and to safeguard all Confidential Information.

A. **Data Classification –** Scripps has created a data classification system, and all information will be handled in accordance with the designated classification of the data as defined in Attachment A *Data Classification.* Data stored in Scripps Systems will be classified into one of the following categories and the category recorded in the Master Portfolio Index Library (MPIL):

1. **Regulated** - 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). Regulated data may be further classified as **Sensitive (Restricted/ Regulated)** which is a sub-category of Protected Health Information that has further regulatory restrictions and therefore has additional safeguards and process requirements.
2. **Confidential** - 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.

3. **Internal** - Data that is proprietary or potentially sensitive and not intended to be shared with the public.
4. **Public** - Data that may be disclosed to any person regardless of their affiliation Scripps.

B. **Confidentiality and Non-Disclosure Agreement -** access to Scripps computer network, information systems, confidential medical information, personal financial information, and other sensitive or proprietary information is contingent upon execution of a *Confidentiality and Non-Disclosure Agreement*. All employees must review and sign the Scripps *Confidentiality and Non-Disclosure Agreement* at the time of hire (at New Employee Orientation) and annually thereafter as part of their annual performance review. 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.

This agreement includes the following:

1. Appropriate access to and use of information;
2. Incidental disclosure of information;
3. Appropriate disclosure of confidential information;
4. Scripps' surveillance and monitoring practices;
5. Disciplinary actions and sanctions;
6. Passwords, security, and other safeguards; and
7. Obligations for confidentiality while affiliated with, and after disassociation from, Scripps.

C. **Minimum Necessary -** when accessing, downloading, using or disclosing Confidential Information, the individual engaging in the activity must make all reasonable efforts to limit the amount of Confidential Information to the minimum necessary to accomplish the intended purpose of the use or disclosure.

D. **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. Reference Standard Safeguards, V. Procedures, C.

E. **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 indicative of such age (although all persons over 89 may be aggregated into a single category)Telephone numbers
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

F. **Handling of Confidential Information -** all individuals who have access to Confidential Information are prohibited from using, discussing or revealing such information in any unauthorized manner. Unless such information is required by the individual's Scripps related responsibilities, accessing Confidential Information is strictly prohibited. For example, individuals may not:

1. Allow or participate in viewing, accessing, downloading, photographing, using or disclosing Confidential Information for any purpose other than carrying out legitimate job-related responsibilities. This includes information belonging to the individual, other employees, co-workers, family or friends.
2. Shred, destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of any Confidential Information and/or information resources without appropriate authorization.
3. Communicate Confidential Information to any other individual or entity if not required to do so for Scripps business purposes. This includes sharing information regarding coworkers, family or friends.

E. **Violations of Confidentiality -** Scripps shall take appropriate action 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. Violation of this policy represents a failure to meet the professional and ethical standards expected of all employees and non-employees conducting business with or on behalf of Scripps. Conduct need not be deliberate or intentional to violate this policy and includes:

1. Unnecessary or unauthorized disclosure of Confidential Information (e.g., informal dialogue in the cafeteria, open office areas, hallways or elevators)

2. Inadvertent violation of confidentiality, such as accidentally accessing a computer account of the wrong patient,
3. Sharing of information outside of Scripps where there is a reasonable basis to believe that the person could still be identified from that information, e.g. email, social networks.
4. Reproduction, (copy or photography) of Scripps confidential records including patient medical records.

F. **Infractions, Disciplinary Actions, Sanctions and Fines.** Any infraction of this policy shall be subject to corrective action by Scripps, up to and including loss of information system access privileges and/or termination of the employment or business relationship with Scripps. Unauthorized access use, download, or disclosure of confidential information may also result in legal action in respect to violation of federal and state privacy laws.

G. **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.

III. PERSONNEL

This policy applies to Scripps entire workforce, including employees, volunteers, and contracted third parties having access to Scripps information. The policy also applies to medical staff members, residents, fellows and interns, employees of medical groups contracted with the Scripps Medical Foundation and other affiliates that have access to Scripps Confidential Information.

IV. 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). See Procedures - B on page 4.

B. **Professional Licensed Staff** will identify individuals (e.g. 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.

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

1. Determining workforce members' role-based access to Confidential Information to perform their job function in compliance with minimum necessary standards.
2. Developing and applying standard safeguards to department work processes for the security and protection of information to include as appropriate: transport of confidential information i.e., locked bags, trunks of vehicles, and establishing direct transport routes.
3. Establishing that a Business Associate Agreement is in place when required for contractual relationships under their direction.
4. Reporting unauthorized access, use or disclosure of Confidential Information and other policy violations.
5. Following established procedures for appropriate disposal of documents, equipment, removal storage media or other items containing or potentially Confidential Information.
6. Monitoring for compliance with Scripps policies pertaining to confidentiality, privacy and security.
7. Providing on-going education, training, and awareness on privacy and security policies and procedures to all staff, commensurate with relative risks in their job functions.
8. Notifying appropriate departments of any workforce member's termination or transfer and for employees collect all Scripps property in accordance with Scripps *Termination* policy S-FW-HR-0212 and in the case of non-employees with contractual arrangements.
9. Applying corrective actions when policy violations have occurred.

V. PROCEDURES

A. **Confidentiality and Non-Disclosure Agreement.** Each member of the Scripps workforce must execute the Scripps *Confidentiality and Non-Disclosure Agreement* upon hire/credentialing/initiation of service (volunteers and contracted). Signed statements shall be maintained in the appropriate file (i.e. an employee's personnel file, a contract service or credentialing file). All employees must review and sign such agreement annually as part of their annual performance evaluation.

B. **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:

1. Supervisor, Manager, or Department Head or Human Resources Office
2. Scripps Privacy Officer 858 678-7785
3. Audit & Compliance Services 858-678-7203
4. Scripps Compliance & Patient Safety Alertline 1 888-424-2387
5. Scripps Information Services Help Desk 858-678-7500 (for security incidents)

C. **Apply and follow Standard safeguards to clinical and business work processes.**

1. Apply "minimum necessary" standard to all use and disclosure of information.
2. Establish work processes that minimize the occurrence of unintentional disclosure of information, e.g. attention to detail when processing documents

containing PHI and creating redundancy for verification of recipient when disclosing confidential information.

3. Dispose of paper, patient armband, CDs, or other non-electronic items containing confidential information must be placed into Shred-It bins.
4. Apply appropriate information security protection to work processes for information in motion, i.e. encryption of all removable storage devices; protected email.
5. Obtain appropriate authorization for use and disclose of protected health information, i.e. patient authorization, Confidential Data Request Form
6. Apply physical security for the protection of confidential information during use as well as transport, i.e. locked cabinets, medical record security, screen savers and privacy screens, protection of equipment/devices/phones/pagers that contain confidential information.
7. 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.
8. Securely seal and marked as confidential any information, considered confidential, that is being mailed or transported (e.g. mailed or interoffice mailed) making sure that confidential information is not visible through envelope windows.
    a. Departments should implement specific procedures to address the security of such information, for example secure in locked canvas bags, lock information in trunk, and avoid making stops.
9. Report the occurrence of an unintentional disclosure to enable mitigation and appropriate notifications.

VI. DEFINITIONS

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

B. **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 and is expressly permitted by policy and/or procedure or the instructions of his or her supervisor to access, review and/or use the information. Authorized means that the appropriate designee has specifically approved access for an eligible person (has “authorized” access). A signed Designation of Personal Representative form, designating a staff member as the patient’s representative, does **not** permit an individual to access the patient’s electronic medical record.

C. **Business Associate Agreements:** Business Associate Agreement is required in all relationships where any person or entity that is not employed by Scripps performs a function or activity on behalf of Scripps that involves the use and/or disclosure of

protected health information (PHI). This agreement will provide for protection of information in accordance with state and federal law.

D. **Confidentiality**: The obligation to protect the privacy of records and related information of individuals receiving services at Scripps. The principle that information is not made available or disclosed to unauthorized individuals, entities or processes.

E. **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, voice-mail, pagers, text messages, Web Portals, photographs, social media such as *Facebook, Twitter, YouTube, Yelp*) all which are subject to the provisions of this policy.

F. **Disclosure:** The release, transfer, provision of access to, or divulging in any manner of confidential information 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 circumstances, as for public health purposes or as mandated or permitted under the regulations.

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

1. To individuals not involved in the care or treatment of patients,
2. To individuals who are involved or know the patient but have no need to know the information, or
3. In a setting where that information could be overheard by individuals who have no need to know, for example in elevators, lobbies, waiting rooms, hallways, dining rooms, etc., or
4. 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. **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.

I. **Minimum Necessary Restriction**: When a provider requests, uses or discloses protected health information of another provider, reasonable efforts must be made 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.

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

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

L. **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. **Scripps Data:** Scripps maintains a diverse and comprehensive data network and electronic communication system. All data resident within the Scripps computer systems, including personal computers, intelligent work stations, 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 considered to be data-owned by Scripps, and are subject to this policy.

M. **Workforce:** Employees, volunteers, trainees, student, contractors, vendors, and other persons whose conduct, in the performance of work for Scripps, is under the direct control of Scripps, whether or not they are paid by Scripps. Members of the Scripps Medical Staffs and Other Physicians are included as a category of workforce for the purpose of this policy.

VII. ATTACHMENTS

A. Data Classification Matrix

VIII. REFERENCES

B. The Joint Commission Accreditation Standards: RI, IM

C. Health & Safety Code Section 199.20

D. 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.

E. HIPAA Administrative Simplification Regulations Text – 45 CFT Parts 160, 162, and 164. (Unofficial Version, as amended through February 16, 2006)

F. California State Confidentiality of Medical Information Act (Civil Code Section 56.10 et. seq.)

G. California Code of Regulations, Title 22, Section 70707(b)(8)

IX. RELATED POLICIES

A. Business Associate Agreement; S-FW-LD-1004

B. Scripps Compliance Program (Standards of Conduct); S-FW-LD-1003

C. Computer, Network and Email Usage Policy; S-FW-IM-2001

D. Facsimile of Information; Scripps; S-FW-IM-2003

E. Health Information, Access, Use and Disclosure; S-FW-IM-0203

F. Health Information, Accounting of Disclosures; S-FW-IM-0207

G. Information, Disclosure of Patient Directory to Public; S-FW-IM-0208

H. Notice of Privacy Practices, Scripps; S-FW-IM-2004

I. Performance Improvement and Corrective Action; S-FW-HR-0501

J. Record Retention Policy; S-FW-IM-0600

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

L. Termination of Employment; S-FW-HR-0212

M. Equipment and Electronic Media, Disposal, Reuse and Data Sanitization; S-FW-IM-3008

X. RELATED FORMS/ RESOURCES

A. Confidentiality and Non-Disclosure Agreement; 100-8650-061

B. Privacy Program Education and Resources on Inside Scripps

C. Social Network Guidelines; SW-IM-0201 A

XI. SUPERSEDED

Confidentiality of Information (Patient, Financial, Employee, and Other Sensitive and Proprietary Information); S-FW-IM-0201 07/14

DEVELOPMENT SUMMARY
07/16 Revision: Added proper disposal of PHI in Shred-It Bins in Standard safeguard section. Added details to Destruction section of Data Classification Matrix in Attachment A.

Development Workgroup		
Representation	**Member Name**	**Member Title/Discipline**
Workgroup Leader/Author	Jan Coughlin	Sr. Director Corporate Compliance and Privacy Officer
Workgroup Member	Jean Fuller	Asst. VP, Health Information Management Services
Workgroup Member	Kiran Vashishta	Privacy Manager
Workgroup Member	Jane Offerman	Director, Health Information Management
Workgroup Member	Claudia Baker	Sr. Business Analyst Rave/Training
Workgroup Member	Valorie Warner	Manager, Access
Workgroup Member	Margaret Mangin	Corporate Counsel
Workgroup Member	Janice Perez	Manager, Health Information

ENDORSEMENTS and APPROVALS		
Function	**Chair Name/Title/Position**	**Date of Endorsement and Approval**
Executive Sponsor	Dave Cohn, Corporate VP, Revenue Cycle	07/19/16
Privacy Officer	Jan Coughlin, Sr. Director Corporate Compliance and Privacy Officer	07/05/16
Executive Cabinet	Chris Van Gorder, President, CEO	07/19/16

	Regulated	Confidential	Internal	Public
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	Confidential	Internal	Public
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 Committee. Remote access only through Scripps approved and secure technologies (SSL VPN, Terminal Services, Citrix etc.) If approved by the Scripps Data Governance Committee.	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.
	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.			
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	Confidential	Internal	Public
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 and.(c) approved by the Scripps Data Governance Committee. Prohibited to be stored on non-Scripps (personal) computing equipment. Third party processing or storage services are prohibited for storing Prohibited information unless with approved Scripps contracted vendor with signed BAA if required or by the Scripps Data Governance 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 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	Confidential	Internal	Public
Display	Additional controls may be invoked such as 'break 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, CD/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, then 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 Shred-It bins,	Same as Regulated.	If no legal hold requirements, then 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 Shred-It 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	Same as Regulated.	Immediately contact IS Help Desk at 858-678-7500.	No Requirements.