SCDC POLICY

NUMBER: GA-06.10

TITLE: HIPAA ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS

ISSUE DATE: November 4, 2019

RESPONSIBLE AUTHORITY: CHIEF LEGAL AND COMPLIANCE OFFICER

OPERATIONS MANUAL: GENERAL ADMINISTRATION

SUPERSEDES: NONE- NEW POLICY

RELEVANT SCDC FORMS/SUPPLIES: 13-53, 13-53A

ACA/CAC STANDARDS: 4-ACRS-4C-22, 4-ACRS-7D-05, 4-ACRS-7E-11, 4-4019, 4-4067, 4-4070, 4-4095, 4-4099, 4-4101, 4-4120, 4-4396, 4-4410, 4-4413, 4-4415

STATE/FEDERAL STATUTES: Health Insurance Portability and Accountability Act (HIPAA), PL-104-191, August 21, 1996, 110 Stat 1936, 65 FR 81321, 45 C.F.R §160.102, 45 C.F.R §164.104, 45 C.F.R §164.306, 45 C.F.R §164.308, 45 C.F.R §164.316, 45 C.F.R §164.502, 45 C.F.R §164.512,

PURPOSE: The intent of this policy is to establish criteria for safeguarding Health Insurance Portability and Accountability Act (HIPAA) information and to minimize the risk of unauthorized access, use, or disclosure. This policy applies to Protected Health Information (PHI), and to Personally Identifiable Information (PII) received, created, used, disclosed, or maintained by SCDC.

POLICY STATEMENT: SCDC's HIPAA privacy polices are applicable to all SCDC employees, including contractors and temporary workers.

TABLE OF CONTENTS

SPECIFIC PROCEDURES:

1. RESPONSIBILITIES:

1.1 SCDC employees are responsible for ensuring that SCDC's HIPAA privacy policies are followed. SCDC's Division of Information Security and Privacy, in conjunction with Health Services, is responsible for the implementation, resolution, and enforcement of all aspects related to SCDC's HIPAA privacy policies.

1.2 The Division of Information Security and Privacy shall be responsible for performing annual risk assessments of the Agency's potential risks and vulnerabilities to the confidentiality, integrity, and availability of both PII (personally identifiable information) and PHI (protected health information).

1.3 The Division of Information Security and Privacy shall work with Health Services and the Division of Resource and Information Management to develop and maintain procedures to regularly perform audits of relevant information system records.

1.4 Exceptions: Any exceptions are listed where appropriate in the policy.

2. HIPAA DATA ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

2.1 SCDC must take reasonable steps to safeguard HIPAA information from any intentional or unintentional use or disclosure that is in violation of SCDC privacy policies. Information to be safeguarded may be in any medium, including paper, oral, visual, and electronic representations of confidential/restricted information.

2.2 Each SCDC workplace must take reasonable and necessary steps to assure that confidential/restricted information cannot be accessed by individuals who do not have a job-related reason for accessing that confidential/restricted information.

2.3 Each SCDC workplace must foster employee awareness of the potential for inadvertent disclosure of confidential/restricted information.

2.4 Safeguarding HIPAA Information: SCDC Information Owner and Workplace Practices:

2.4.1 Paper:

2.4.1.1 Each SCDC workplace will store files and documents containing confidential/restricted information in locked rooms or storage systems when available.

2.4.1.2 In workplaces where lockable storage is not available, SCDC staff must take reasonable efforts to ensure the safeguarding of confidential/restricted information.

2.4.1.3 Each SCDC workplace will ensure that files and documents containing confidential/restricted information that are awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins are appropriately labeled, and are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.

2.4.1.4 Each SCDC workplace will ensure that shredding, burning, or other authorized methods of disposal of files and documents containing confidential/restricted information is performed on a timely basis, is documented, and is consistent with all applicable record retention requirements.

2.4.2 Oral:

2.4.2.1 SCDC employees must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential/restricted information, regardless of where the discussion occurs.

2.4.2.2 Each SCDC workplace should use offices and/or interview rooms available for the verbal exchange of confidential/restricted information, when such rooms are available for that purpose.

2.4.2.3 When conducting telephone conversations that involve the exchange of confidential/restricted information, every reasonable step should be taken to ensure that the conversation will not be overheard by unauthorized individuals.

2.4.2.4 Exception: In work environments structured with few offices or closed rooms, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that SCDC has met the reasonable safeguards and minimum necessary requirements.

2.4.3 Visual:

2.4.3.1 SCDC employees must reasonably ensure that observable confidential/restricted information is adequately shielded from unauthorized disclosure on computer screens and paper documents.

2.4.3.2 Computer screens: Each SCDC workplace must make every effort to ensure that confidential/restricted information on computer screens is not visible to unauthorized persons. Monitors should not face windows, doors, or other areas that permit viewing by others. Users should logoff or lock workstations when they step away from their work area (refer to SCDC Policy ADM-15.05, "Security and Use of Information Technology," section 2.2.7).

2.4.3.3 Paper documents: SCDC staff must be aware of the risks regarding how paper documents are used and handled and must take all reasonable and necessary precautions to safeguard confidential/restricted information.

2.4.3.4 Fax machines, copiers, scanners, and other similar devices: These types of devices should not be located in areas accessible to the public or inmates. All reasonable and necessary precautions should be taken to safeguard confidential/restricted information passing through such devices, including using the secure print feature to reduce the possibility of an inadvertent disclosure.

2.4.4 <u>Electronic</u>:

2.4.4.1 Each SCDC information owner (see SCDC Policy GA-06.05, "Information Security," section 14. Definitions) should request and work with RIM to incorporate safeguards that include, but are not limited to, access control lists, encryption, individualized passwords for access to personal computers, laptops, and other similar devices and password protected screen savers.

2.4.4.2 Each SCDC workplace must take reasonable and necessary steps to ensure that all personal computers, laptops, hard drives, disks, CDs, DVDs, jump drives, and other similar devices on which confidential/restricted information is stored is backed up on a regular basis and stored in a manner consistent with SCDC policy ADM-15.05, "Security and Use of Information Technology." If an area is unsure how its data is backed up, the responsible manager must contact RIM to verify that backups are made or make arrangements with RIM to implement a proper backup method.

2.4.4.3 Each SCDC workplace must take reasonable and necessary measures to assure that all confidential/restricted information stored on personal computers, laptops, hard drives, discs, CDs, DVDs, jump drives, and other similar devices is destroyed on a timely basis, documented, and consistent with all applicable record retention requirements. All such devices must be securely wiped of all confidential/restricted information prior to disposal of the device, in accordance with SCDC Policy GA-06.05, "Information Security."

2.5 Safeguarding HIPAA Information: SCDC Employee Practices

2.5.1 <u>SCDC Databases</u>:

2.5.1.1 SCDC will implement role-based access controls (RBAC) for all SCDC databases.

- RBAC is a form of security allowing access to data baseS on job function in accordance with SCDC security procedures. Employee members shall be assigned the minimum necessary permissions to fulfill their job functions. Supervisors are responsible and accountable for ensuring that their users do not have more access than necessary.

- Implementation of role-based access, "Minimum Necessary Information," will promote administrative safeguards.

2.5.1.2 Other methods may also be developed to assure that employees have access only to information which is necessary to do their jobs for SCDC.

2.5.1.3 Internal security and privacy audits will be conducted periodically to permit SCDC to evaluate the effectiveness of safeguards.

- SCDC managers and supervisors shall comply with ADM-15.05, "Security and Use of Information Technology," and conduct annual reviews to verify that access lists are correct;
- Development and implementation of department-wide security policies will enhance administrative safeguards;
- The Division of Information Security and Privacy shall be responsible for conducting security and privacy audits to ensure that existing controls are effective and to identify any potential additional controls which may be needed.

2.5.2 Email Systems:

2.5.2.1 All communications containing confidential/restricted information using email systems will comply with SCDC Policy ADM-15.05, "Security and Use of Information Technology," and SCDC Policy GA-06.05, "Information Security," regarding "Minimum Necessary Information" and not contain any confidential/restricted information within its caption (i.e., RE: or Subject).

2.5.2.2 All communication containing confidential/restricted information using email, approved text messaging, or other similar systems will contain a verification message or means to confirm recipient.

2.5.2.3 All communication containing confidential/restricted information using email will contain a confidentiality message to assure that if it was inadvertently sent to someone other than the intended recipient that the individual has been warned to return it immediately.

2.5.2.4 All external electronic messages containing confidential/restricted information should be encrypted per SCDC Policy ADM-15.05, "Security and Use of Information Technology," section 3.7.4.

2.5.2.5 Employees should redact confidential/restricted information in an email chain when the information is no longer relevant or necessary to the discussion.

2.5.3 Faxing, Scanning, or Other Similar Methods of Electronic Disclosure of Information:

2.5.3.1 All communications containing confidential/restricted information using faxing, scanning, or other similar methods of electronic disclosure of information will comply with SCDC Policy ADM-15.05, "Security and Use of Information Technology," SCDC Policy GA-06.05, "Informaton Security," and with the "Minimum Necessary" guidelines, and not contain any confidential/restricted information within its caption (i.e., RE: or Subject).

2.5.3.2 All communications containing confidential/restricted information using faxing, scanning, or other similar methods of electronic disclosure of information will contain a verification message or means to confirm recipient.

2.5.3.3 All communications containing confidential/restricted information using faxing, scanning, or other similar methods of electronic disclosure of information will contain a confidentiality message to assure that if it was inadvertently sent to someone other than the intended recipient that the individual has been warned to return it immediately.

2.5.4 Employee HIPAA Privacy Training, Confidentiality Form, and Access Form:

2.5.4.1 Prior to being given access to any confidential/restricted information in the possession of SCDC, all SCDC employees, contractors, and temporary workers are required to:

- Receive the required HIPAA Privacy Training; and
- Sign SCDC Form 13-53, "Confidentiality Agreement," or, for contractors and vendors, sign SCDC Form 13-53A, "Third Party Confidentiality Agreement."

2.5.4.2 All employees, contractors, and temporary workers must complete annual HIPAA Privacy Training.

2.5.4.3 No person provided with an SCDC login ID shall give his/her login ID(s) or password(s) to anyone. No SCDC employee, contractor, temporary worker, or volunteer shall use another person's login ID or password to gain access to any SCDC database or documents which contain PHI or other confidential or restricted information. Doing so constitutes a HIPAA violation and is punishable in accordance with SCDC Policy ADM-11.04, "Employee Corrective Action."

2.5.5 **Safeguarding HIPAA Information: Inmate's or his/her Personal Representative's Waiver**:

2.5.5.1 An inmate or his/her personal representative may expressly waive any or all of the above safeguards as they relate to his/her PHI. This waiver does not and cannot apply to employee access to any SCDC database.

3. INMATE RIGHTS:

3.1 Privacy notices are not required to be posted in correctional facilities or disseminated to inmates during or after incarceration (45 C.F.R. §164.520(a)(3)).

3.2 Inmates shall be permitted to review their medical records, but may be denied the option to receive a copy of his/her PHI if:

- providing or obtaining the copy would compromise the health, safety, security, custody, or rehabilitation of the individual or other inmates ;
- providing or obtaining the copy would compromise the safety of any officer, employee, or person at the correctional institution or the responsible party during the transporting of the inmate;
- those records are psychotherapy notes or contain information compiled by the institution for use in a criminal or administrative proceeding.

3.3 Inmates shall have the right to request that their record be amended if they detect errors.

4. DEFINITIONS: Definitions are included in the body of this policy.

SIGNATURE ON FILE

s/Bryan P. Stirling, Director

Date of Signature

ORIGINAL SIGNED COPY MAINTAINED IN THE OFFICE OF POLICY DEVELOPMENT