CAROLINA FAMILY HEALTH CENTERS, INC.
POLICY & PROCEDURE

MANUAL: Volume III	**SUBJECT POLICY:** **SUBJECT PROCEDURE:** Confidential Data
NUMBER: IS-09 Page **1** of **4**	**EFFECTIVE DATE:** April 2014
SECTION: Information Systems **REFERENCE POLICY:** N/A **REFERENCE PROCEDURE:**	**REVIEWED:** 10/14; 08/16
RESPONSIBILITY: Chief Financial Officer	**APPROVAL:** APPROVED **DATE:** 8-23-16
CEO APPROVAL: N/A **DATE:**	**BOARD APPROVAL:** N/A **DATE:**

I. PURPOSE

The purpose of this policy is to detail how confidential data, as identified by IS-5 Data Classification Policy, should be handled by Carolina Family Health Centers, Inc. (CFHC, Inc.). This policy lays out standards for the use of confidential data, and outlines specific security controls to protect this data.

II. PROCEDURE

CFHC, Inc.'s confidential data will be stored and transmitted in a way that ensures the security of the information.

Examples of Confidential Data

The following list is not intended to be exhaustive, but provides a guideline the type of information that is typically considered to be confidential. Confidential data can include:

- Employee or customer social security numbers or personal information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Customer data
- Company financial data
- Product and/or service plans, details, and schematics
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party

MANUAL: Volume III	**SUBJECT POLICY:** **SUBJECT PROCEDURE:** Confidential Data
NUMBER: IS-09 Page **2** of **4**	**EFFECTIVE DATE:** April 2014
SECTION: Information Systems **REFERENCE POLICY:** N/A **REFERENCE PROCEDURE:**	**REVIEWED:** 10/14; 08/16

Use of Confidential Data

- Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential."
- Users must only access confidential data to perform his/her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.
- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information.
- If confidential information is shared with a third party, the company must indicate to the third party how the data should be used, secured, and, destroyed.

Treatment of Confidential Data

Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key.

Transmission

Strong encryption must be used when transmitting confidential data, regardless of whether such transmission takes place inside or outside the company's network. Confidential data must not be left on voicemail systems, either inside or outside the company's network, or otherwise recorded.

When sending confidential information through email users are required to follow all guidelines in the *IS-3 Email Policy*. The company provides email encryption services to all employees. Please see the email encryption guide on the company intranet at http://local.cfhcnc.org/misforms.html.

MANUAL: Volume III	**SUBJECT POLICY:** **SUBJECT PROCEDURE:** Confidential Data
NUMBER: IS-09 Page **3** of **4**	**EFFECTIVE DATE:** April 2014
SECTION: Information Systems **REFERENCE POLICY:** N/A **REFERENCE PROCEDURE:**	**REVIEWED:** 10/14; 08/16

Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.
- Storage media (CD's, DVD's): If re-writable, these media may be re-formatted. Otherwise physical destruction is required. Contact the IT department if assistance is needed.
- Storage media (Flashdrives) – Must be re-formatted.
- Hard Drives/Systems/Mobile Storage Media: physical destruction is required. Contact the IT Manager.

Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. CFHC, Inc. requires that the following guidelines are followed:

- Computer screens must be positioned where information on the screens cannot be seen by outsiders.
- Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.
- Users must log off or shut down their workstations when leaving for an extended time period, or at the end of the workday.
- Strong Encryption. Strong encryption must be used for confidential data transmitted internal or external to the company. Confidential data must always be stored in encrypted form, whether such storage occurs on a user machine, server, laptop, or any other device that allows for data storage.
- Network Segmentation. The company must use firewalls, access control lists, or other security controls to separate the confidential data from the rest of the corporate network.
- Authentication. Two-factor or Two-step authentication must be used for access to confidential data.
- Physical Security. Systems that contain confidential data, as well as confidential data in hardcopy form, should be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data.
- Printing. When printing confidential data the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.

MANUAL: Volume III		**SUBJECT POLICY:** **SUBJECT PROCEDURE:** Confidential Data
NUMBER: IS-09	Page **4** of **4**	**EFFECTIVE DATE:** April 2014
SECTION: Information Systems **REFERENCE POLICY:** N/A **REFERENCE PROCEDURE:**		**REVIEWED:** 10/14; 08/16

- Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.
- Emailing. Confidential data must not be emailed inside or outside the company without the use of strong encryption.
- Mailing. If confidential information is sent outside the company, the user must use a service that requires a signature for receipt of that information. When sent inside the company, confidential data must be transported in sealed security envelopes marked "confidential."
- Discussion. When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.
- Confidential data must be removed from documents unless its inclusion is absolutely necessary.
- Confidential data must never be stored on non-company-provided machines (i.e., home computers).
- If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

III. Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities. Refer to *RM-08 Incident Reporting*.