Governance, Risk & Compliance	Policy/Procedure Number:	IS.01
Chief Compliance & Privacy Officer	Effective Date:	12/07/2021
	Approval Date:	05/22/2019
Information Security Policy	Revision Date:	08/04/2021
	Replaces/Retires Policy Number:	
	Pages:	**1** of **7**

Our Family of Companies

SCOPE:

This policy applies to all the Family of Companies ("FoC") officers, agents, employees, business associates, contractors, affected vendors, temporary workers, volunteers, and agents who do business with or on behalf of the FoC.

RESPONSIBLE PERSONS:

Responsibility for the content, administration and implementation of the Information Security Policy resides with FoC's Information Security Official and Privacy Official.

BACKGROUND and PURPOSE:

Ensuring the privacy, security, and confidentiality of health information has been a fundamental principle for FoC.

Federal and state laws regulate businesses that electronically maintain or transmit personally identifiable information ("PII"). These laws require each entity to maintain reasonable and appropriate administrative, technical, and physical safeguards for privacy and security.

The purpose of this policy is to outline FoC's standards for information security. Protecting the confidentiality, integrity, and availability of information requires that information be identified by level of sensitivity. Special handling consideration is given to information depending on the level of sensitivity. This document outlines the enterprise-wide information classification standard. Appropriate information security processes and mechanisms can then be applied to adequately protect each level of information.

DEFINITIONS:

A. "**Administrator**" or "**System Administrator**" or "**Security Administrator**" means the individuals responsible for the technical administration of information assets, including networks, systems, applications, and databases.

B. "**Asset**" means any item that is purchased by, owned by, leased to, contracted by, operated by, used by, controlled by, given to, supplied by, or in any other manner connected to FoC. This includes everything from pens and paper to mainframe computing systems and other information assets.

C. "**Confidential Information**" is a subset of Proprietary Information and shall have the same meaning as Proprietary Information.

D. "**Confidentiality**" means the degree to which the privacy or secrecy of something can be trusted.

E. "**Information Security**" means the protection of data against loss, modification, or unauthorized disclosure during its input to, storage in, or processing by a computing resource or at any point thereafter.

F. "**Integrity**" means the degree to which something is free from corruption, i.e., protected from being damaged, altered, added or removed.

G. "**Proprietary Information**" means, any trade secret, know-how, invention, software program, application, documentation, schematic, procedure, contract, information, knowledge, data, process, technique, design, drawing, program, formula or test data, work in progress, engineering, manufacturing, marketing, financial, sales, supplier, customer, client, employee, investor, or business information, whether in oral, written, graphic or electronic form. This information is intended for use within FoC unless authorized for additional distribution.

H. "**Personally Identifiable Information**" or "**PII**" means any information about an individual maintained by the FoC, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as health, educational, financial, and employment information.

I. "**Protected Health Information**" or "**PHI**" means individually identifiable health information that is transmitted by electronic media; maintained in any medium as described in the definition of electronic media; or transmitted or maintained in any other form. PHI excludes individually identifiable health information in education records and student health records covered by the Family Educational Rights and Privacy Act (FERPA), and employment records held by a Covered Entity in its role as employer.

J. "**Workforce**" includes employees, volunteers, trainees and other persons, whose conduct, in the performance of work for the location, is under the direct control of such location, whether or not they are paid by the location. Workforce excludes independent contractors of the location because the location may not exercise direct control over an independent contractor. Workforce also excludes Business Associates or an employee, agent or contractor of a Business Associate.

K. "**Public Information**" means information that has been released to the public by the FoC.

L. "**Security Violation**" means a failure in the physical security and/or Information Security measures resulting in a loss of data, the inability to provide computing services, unauthorized use or modification of information assets, or the unauthorized access to files, data, and services.

POLICY:

The FoC uses on-line information systems to manage business operations and healthcare information. FoC has a duty to protect the confidentiality, integrity, and

availability of medical and business information as indicated or required by best business practices, accepted information security standards, federal and state laws, professional ethics and accreditation requirements.

A. Administrative Controls

1. Information Classifications

   There are three sensitivity classifications for information with separate handling requirements: Confidential, Proprietary, and Public.

   a. Examples of Confidential information include, but are not limited to:

      (1) Protected Health Information (PHI)

      (2) Electronic Protected Health Information (ePHI)

      (3) Personally Identifiable Information (PII)

      (4) Employee personnel files

      (5) Payroll information

      (6) Business strategies

      (7) Quality Assurance documentation

      (8) Clinical Research documentation

      (9) Attorney-client privileged documents

      (10) Attorney work products

      (11) Trade secrets

   b. Examples of Proprietary information include:

      (1) Internal telephone numbers

      (2) Financial information

      (3) Policies and procedures

      (4) FoC intranet website content

   c. Examples of Public information include:

      (1) Job postings

      (2) Annual reports

      (3) FoC internet website content

2. Information Access Management

    a. Each User of ePHI must have an individual UserID and confidential password for accessing that information.

    b. Background checks must be performed on all information asset Users as outlined in FoC's Employee Handbook prior to accessing FoC information assets.

    c. Users must follow the FoC Information Security Policies for gaining access to and for using FoC information assets.

    d. Users must participate in the Information Privacy and Security Awareness Trainings program to ensure their understanding and compliance with the Information Privacy and Security Program.

    e. Users must use FoC information assets as outlined in the FoC Information Security Standards.

    f. Users of FoC information assets shall not assume their actions are private, privileged or protected. FoC reserves the right to monitor Users as outlined in FoC's Employee Handbook. This may include video, audio or electronic monitoring of activities such as:

        (1) Telephone conversations

        (2) E-mail content and destinations

        (3) Internet access and downloading

        (4) Data access

        (5) Key strokes

        (6) Work habits

3. Audit Log Reviews

    System Administrators and/or security Administrators must monitor the security event logs created by the FoC information assets to ensure that inappropriate behavior or potential intrusions are recognized and addressed.

4. Contingency and Disaster Recovery Plan

    The FoC's Contingency and Disaster Recovery Plan is managed by the FoC's Disaster Preparedness Task Force led by the VP, Real Estate & Facilities and the VP, Site Reliability. The intent of this program is to protect the safety of our stakeholders and mitigate potential risk(s) that could materially affect the ability of a location to remain a going concern. The major focus of the plan is for the identification, protection, and recovery of critical information assets in the event of a disaster.

B. Physical Safeguards

1. Facility Access

a. The FoC must implement reasonable appropriate physical safeguards for information systems and related equipment and facilities to protect ePHI.

2. Workstation Use and Security

a. The FoC must implement policies and procedures for granting access to ePHI.

b. The FoC must implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

3. Device and Media Controls

a. The FoC must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility.

C. Technical Safeguards

All information assets must be configured to support the concepts and instructions found in the FoC Information Privacy and Security Program policies and standards.

Administrators of information assets that cannot support the policies and procedures must contact the Information Security Officer prior to using those assets.

1. Areas of Concentration

There are six major areas of information security that must be addressed by administrators of FoC information assets. The content of each of these areas is described below.

a. Local and Remote Access Controls

These controls include provision of mechanisms that permit access by authorized individuals while preventing access by those not properly authorized. Access to PHI and ePHI shall be managed through active application of system controls, physical controls, and reviews.

(1) Desktop, Laptop, and End-User Controls.

You may only access the FoC's network using approved end-user devices that support our current minimum information security standards. Standards for end-user devices may include protective controls and specific configurations, such as multi-factor authentication, anti-virus software, patching levels, and required operating system or other software versions. FoC-owned machines may be configured to automatically receive upgrades. You may be denied remote access using non-FoC owned devices

that do not meet current standards.

Use your own FoC-provided account(s) to access FoC's network and systems, unless you have been specifically authorized to use a device-specific, administrative, or other account (see IS.01.01 Identity and Access Management Standard).

b. Audit Controls

These controls consist of mechanisms employed to increase accountability by recording and supporting examination of system activity.

c. Authorization Controls

These controls include mechanisms for granting access to Confidential or Proprietary information based on the individual's need-to-know as a requisite for performing their job.

d. Data Authentication Controls

These controls relate to the verification that information has not been altered or destroyed through unauthorized methods or access.

e. Entity Authentication Controls

These controls verify an entity and require the use of unique user identifiers, automatic logoffs, and a selection of other identifiers including biometrics, passwords, tokens or PINs.

f. Configuration Management Controls

These controls address the security of information systems in conjunction with the Information Security Policies and Procedures of the organization to create a coherent system of overall security. Configuration management includes:

(1) Documentation of all components of a system's security.

(2) Written procedures for connecting new hardware and software.

(3) Periodic review of system maintenance records.

(4) Periodic testing of the security attributes of the system.

(5) Maintenance of accurate documented inventory records.

(6) Security testing of systems including functional and penetration testing and verification.

(7) Virus checking.

2. Accomplishing Security Goals

Accomplishing FoC's security goals requires information asset Administrators to configure and manage information assets according to the Information Security Standards.

D. Precedence of the FoC Information Security Policies and Procedures

The Information Security Program policies and standards take precedence over other Information Security policies where the Information Security Program policies and standards are more restrictive, unless the need for the divergence is approved and documented.

RELATED POLICIES AND STANDARDS:

- ORM Records Retention Policy
- P&P Sanction Policy
- Privacy Security Program Administration Policy and Standards

REFERENCES:

- Code of Conduct
- Employee Handbook
- Cal. Health & Safety Code section 1280.15. http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC&sectionNum=1280.15. Last visited 7/30/2018.
- 45 C.F.R. § 160 (2013). http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr160_main_02.tpl. Last visited 7/30/2018.
- 45 C.F.R. §164.302-318 (2013). https://www.ecfr.gov/cgi-bin/text-idx?SID=7207be667637709ea58f74c3b51a6129&mc=true&node=sp45.1.164.c&rgn=div6. Last visited 7/30/2018.
- 45 C.F.R. §164.530(f) (2013). http://www.ecfr.gov/cgi-bin/text-idx?SID=59dd34838b48ac113af13d7c46dd06af&node=se45.1.164_1530&rgn=div8. Last visited 7/30/2018.

Our Family of Companies

IT Information Security Policies