Department/Program Office of Risk Management	Policy/Procedure Number:	REG.01
Title of Department Leader CAO	Effective Date:	9/16/2019
	Approval Date:	5/22/2019
Privacy Security Administration Policy	Revision Date:	
	Replaces/Retires Policy Number:	
	Pages:	**1** of **6**

Our Family of Companies

SCOPE:

This policy applies to Catalight Foundation and its subsidiaries and affiliates (the "Family of Companies" or "FoC") officers, consultants, employees, business associates, vendors, contractors, temporary workers, volunteers, and any agent who does business with or on behalf of the FoC.

RESPONSIBLE PERSONS:

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

BACKGROUND and PURPOSE:

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

Federal and state laws regulate business, including the FoC 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 ensure the FoC's compliance with all applicable laws and regulations with regards to Health Insurance Portability and Accountability Act ("HIPAA"), as well as any other federal and state laws protecting the confidentiality and privacy of personal information, and principles of general and professional ethics. The FoC also acknowledges its duty and responsibility to support and facilitate the timely and unrestricted flow of health information for lawful and appropriate purposes.

DEFINITIONS:

A. A "**Business Associate**" is a person or entity, other than a member of a Covered Entity's workforce that provides certain functions, activities, or services for or to the Covered Entity involving the Use and/or Disclosure of PII. Business associates include subcontractors that create, receive, maintain, or transmit protected health information on behalf of a Business Associate. Business associates specifically do not include health care providers to whom protected health information is disclosed concerning the treatment of an individual.

B. A "**Disclosure**" means the release, transfer, provision of access to, or divulging of information in any other manner outside the FoC Location holding the information.

C. "**Health Information**" is broadly defined and includes any health information that pertains to a particular individual.

D. The "**Health Insurance Portability and Accountability Act of 1996**" or "**HIPAA**" was enacted by the U.S. Congress and signed by President Bill Clinton in 1996. Title II of

HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for the privacy and security of health data. The Administrative Simplification provisions also address electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

E. The "**Notice of Privacy Practices**" or "**NPP**" is a document that tells clients how a Covered Entity may use and disclose their PII and also informs clients of their legal rights regarding their PII.

F. "**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.

G. "**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.

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

POLICY:

The FoC respects the privacy of every client's health information and the rights clients have with respect to their health information. Protecting the privacy of confidential information in conformity with applicable federal and state laws requires consistent application of administrative policies. The FoC's Information Privacy and Security Programs (**the "Program"**) defines the policies, standards, responsibilities, and authorities designed to protect the health information of clients and afford clients certain rights with respect to their health information, consistent with applicable federal and state law.

This document, along with its subordinate standards, establishes uniform administration of the FoC's Program.

A. Oversight

The FoC's Office of Risk Management ("ORM") will work with the FoC leadership to develop, maintain, and update procedures, guidelines and job aids for protecting PII,

PHI and other confidential information and affording clients their rights with respect to their confidential information.

B. Designation of Information Privacy and Security Officials

1. The FoC designates the Senior Vice President, Compliance and Risk Officer as the Privacy Official.
2. The FoC designates the Chief Technology Officer as the Information Security Official.

C. Designation of an Office to Receive Complaints

The FoC designates the offices of the individuals described above, or their delegates, as the contact persons who will be available to receive complaints regarding the FoC's Program policies and implementation.

1. Complaint and Privacy Security Event Reporting
    a. Complaints and events regarding the FoC's Program may be made in writing, in person, by calling the Compliance Helpline (1-833-44-PROTECT) or as outlined in the Employee Handbook or Code of Conduct.
    b. When privacy and security reports are received, the Office of Risk Management, in collaboration with appropriate leadership, will identify and coordinate resources to document and investigate them as outlined in Privacy Security Event Handling Standard. Documentation must include the resolution of all complaints and incidents, including findings, and, as applicable, corrective actions taken and sanctions imposed.

D. Mitigation

In response to any unauthorized use or disclosure by a member of the FoC's Workforce or any of its Business Associates, the FoC will develop and implement a plan to mitigate any known or reasonably anticipated harmful effects from such unauthorized use or disclosure.

E. Auditing and Monitoring

1. ORM will review the FoC's implementation of this policy during scheduled audits.
2. ORM will be responsible for monitoring the FoC's adherence to this policy.
3. The FoC leaders will be responsible for monitoring the Workforce member's adherence to this policy.

F. Sanctions

The FoC implements sanctions, to the extent practicable, when PII, PHI or other confidential information is used or disclosed in violation of the requirements of federal and state laws and regulations, or the FoC's policies, standards and procedures by members of the FoC's Workforce or its Business Associates.

G. Non-Retaliation

The FoC adheres to a strict policy of non-retaliation, meaning that a workforce member or others will not suffer any negative consequences for making a report or complaint in good-faith or for participating in a subsequent inquiry.

H. Safeguards

The FoC must have appropriate administrative, technical and physical safeguards to protect the privacy and security of PII, PHI and other confidential information. The safeguards will be designed to reasonably protect PII, PHI and other confidential information from any intentional or unintentional use or disclosure that violates the FoC policies and federal and state regulations. The FoC will also put safeguards in place to limit incidental uses or disclosures that are made pursuant to permitted or required uses or disclosures.

I. Waiver of Rights

The FoC may not require any individual to waive his or her rights under state or federal regulations as a condition of treatment, payment or determining eligibility for benefits.

J. Privacy Security Training

The FoC must provide training regarding the FoC's Program in accordance with federal and state law to its Workforce.

1. Training will be provided to new members of the Workforce within 30 days from the date of hire.
2. Each Workforce member whose functions are affected by a material change will be provided additional training within 30 days after the effective date of the change.
3. Training will be ongoing.
4. Training and education can be conducted in a variety of forms.
    a. On-Line Training. Participation in on-line training sessions must be documented and maintained in the FoC's online education system.
    b. Classroom Training. Attendance at classroom training sessions must be documented and maintained in accordance with section 4.d. of this policy.
    c. Training materials must be maintained according to section VI.J. of this policy.
    d. Training completion documentation will include the time, date, place and content of each training session, as well as the Workforce members who attended each training session. The FoC will maintain such documentation and make it available for inspection by regulatory authorities, as appropriate.

K. Policies and Procedures

1. Implementation

   ORM will work with Information Technology, People & Performance and the FoC leadership to develop, maintain, and update operational procedures, guidelines and job aids for protecting PII, PHI and other confidential information and affording clients their rights with respect to their confidential information. The operational procedures are contained in the FoC Policies and Procedures Library on Confluence. The Policies and Procedures Library is available to all the FoC workforce members.

2. Changes in Laws

   ORM will keep abreast of changes in laws, regulations and standards that may affect the Program and will implement changes to affected policies, standards and procedures as necessary. In the event that any the FoC policy, or portion of a policy, is not in accord with such laws, then the provisions of the applicable laws shall control and preempt the policy (or portion of the policy) that is out of compliance until appropriate changes are made to the policy to cause it to conform.

3. Risk Management

   Information privacy and security risk management includes risk assessment, risk reduction, and risk level maintenance. The FoC is responsible for performing risk management procedures. The FoC must amend their procedures as appropriate to manage risk identified through the risk management process.

4. Enforcement

   All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with the People and Performance Policy.

L. Record Documentation and Retention

The FoC's Program policies, standards and procedures must be maintained in written and/or electronic form. Any communications required under the FoC's Privacy and Security Policies and Procedures must be in writing and maintained according to Records Retention Policy.

M. Business Associates and Business Associate Agreements

The FoC may disclose PHI to a Business Associate or allow a Business Associate to create or receive PHI on behalf of the FoC if the FoC obtains satisfactory assurances, memorialized in the form of a Business Associate Agreement, that the Business Associate appropriately safeguards the PHI as required by the HIPAA regulations.

1. The process of entering into business associate an agreement is an integral part of the FoC's Program and is outlined in ORM.VG.01.03 Business Associate and Data Use Agreement Standard.

N. De-identification of Client Information

The Privacy Rule permits the de-identification of PHI in §164.514(a)-(b). The Privacy Rule provides two de-identification methods:

1. A formal determination by a qualified expert; or
2. The removal of specified individual identifiers, in addition to, the absence of actual knowledge by the FoC that the remaining information could be used alone or in combination with other information to identify the individual.

The FoC may only de-identify client information as outlined by this policy and the De-identification of Client Information Standard.

RELATED POLICIES:

- Information Security Policy
- ORM Records Retention Policy

REFERENCES:

- Code of Conduct
- Employee Handbook
- Cal. Health & Safety Code, Division 106 § 123145(a) (1996). http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC&sectionNum=123145.
- Cal. Health & Safety Code section 1280.15. http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC&sectionNum=1280.15.
- 45 C.F.R. § 160 (2013). http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr160_main_02.tpl.
- 45 C.F.R. §164.102-106 (2013). http://www.ecfr.gov/cgi-bin/text-idx?SID=2bc9bff597822b6bfb2d0177444dba8d&mc=true&tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl.
- 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.

ATTACHMENTS:

- Attachment A: REG.01 Privacy Security Administration Standards

Our Family of Companies

Privacy Security Administration Standards

REG.01.01 Privacy Security Event Handling Standard – The purpose of the standard is to provide an organized approach for reporting and responding to privacy security incidents as required under section 164.530(d)(1)(2) of the Privacy Rule and section 164.308(a)(6)(i) of the Security Rule. The growing use of external data communications has increased the likelihood of encountering threats to the security of systems and information. A structured approach is needed to respond to privacy security events and return services and systems to normal operation as quickly as possible.

REG.01.02 Breach Notification Standard – The purpose of this standard is to ensure that affected individuals, the media, the Secretary of Health and Human Services ("HHS") and State Attorney Generals are appropriately notified of any Breach of unsecured personally identifiable information ("PII") protected health information ("PHI") in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and all applicable state and federal regulations and guidance.

REG.01.03 Information Risk Management Program Standard – The purpose of this standard is to provide guidance to management on certain administrative functions and to identify those responsible for controlling and monitoring those functions. The State and Federal laws require certain administrative functions to ensure ongoing guarding of data integrity, confidentiality and availability.

REG.01.04 Disciplinary Guidelines Standard – The purpose of the standard is to establish a consistent procedure to be followed in circumstances where corrective, remedial, or disciplinary action is appropriate to address an employee or contractor's failure to comply with the FoC's Privacy and Security Program policies, the Code of Conduct, the Employee Handbook and applicable state and federal privacy laws. These guidelines were designed to align a "typical" privacy violation with the "normal" disciplinary action consequences.

REG.01.05 – **Information Handling and Physical Safeguards Standard** – Outlines standards, procedures and guidelines supporting the physical security of information and information assets.

REG.01.06 – **Verification of Identity and Authority to Receive Confidential Information Standard** – The purpose of this standard is to inform the FoC workforce members dealing with confidential information of steps for verifying the identity and authority of the requester when disclosing confidential information to individuals.