FFT LLC InformationSecurity Policy
(this policy is publicly postedat www.fftcss.com)

I. POLICY

A. It is the policy of FFT LLC that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

B. FFT LLC uses the "CSS system" to track FFT work with client agencies. All CSS documentation, which may be in electronic form, is retained for at least 10 years after initial creation.

C. FFT LLC complies with the EU - U.S. Privacy Shield Principles as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. FFT LLC has certified that it adheres to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. This commitment applies to transfers of all personal data from the UK. To learn more about the Privacy Shield Principles and to view FFT LLC's certification, please visit https://www.privacyshield.gov/

D. These policies are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) as determined by regulation.

II. SCOPE

A. The scope of information security includes the protection of the confidentiality, integrity and availability of information in the CSS system.

B. The framework for managing information security in this policy applies to all FFT employees and independent contractors.

C. This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in INFORMATION CLASSIFICATION.

III. RISK MANAGEMENT

A. A thorough analysis of all FFT LLC CSS system will be conducted on a periodic basis to document any threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection. FFT LLC will do this through its contracted IT vendors.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

B. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

IV. INFORMATION SECURITY DEFINITIONS

Affiliated Covered Entities: Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity for purposes of HIPAA.

Availability: Data or information is accessible and usable upon demand by an authorized person.
Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.
HIPAA: The Health Insurance Portability and Accountability Act, a federal law passed in 1996 that affects the healthcare and insurance industries. A key goal of the HIPAA regulations is to protect the privacy and confidentiality of protected health information by setting and enforcing standards.
Integrity: Data or information has not been altered or destroyed in an unauthorized manner.
Involved Persons: Every worker at FFT LLC-- no matter what their status. This includes employees, contractors, consultants, partners, and researchers.
Involved Systems: The CSS system.
Protected Health Information (PHI): PHI is health information, including demographic information, created or received by the FFT LLC entities which 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 or can be used to identify the individual.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

V. INFORMATION SECURITY RESPONSIBILITIES

A. **Designated Information Security Staff** person works with user management, owners, custodians, and users to, with the guidance of FFT LLC's contracted IT vendor and the company's CEO, to assure appropriate controls Specific responsibilities assuring that the CSS application follows the following standards:

- HTTPS is used for all traffic.
- Application server removes HTTP response headers that disclose application platform information.
- ASP.NET Identity is used for user authentication and authorization.
- User passwords are hashed using PBKDF2 with HMAC-SHA1.
- User accounts are locked after 3 failed login attempts.
- New accounts requests are manually reviewed and approved by an admin before an account is created.
- Password reset links are sent via email. Passwords are never included in any emails.
- Passwords require a minimum length of 6 characters, with at least one numeric, one special character, one uppercase character, one lowercase character.
- User sessions time out after 2 hours of inactivity.
- A number of security roles provide access to various functions of the application. The "Admin" role is the only role permitted to manage user accounts.
- The application provides a single entry point through the login screen. No other actions are permitted without a valid user account.
- ASP.NET MVC filters are used to ensure a valid session and necessary permissions for all non-login actions.
- Security roles and workgroup assignments are used together to determine authorization for application areas.
- SQL Server 2016, running on the application server.
- Entity Framework is used as an ORM framework.
- EF prevents against SQL injection since no SQL queries are generated directly in the code.
- User input is not used in any queries for filtering or data retrieval.

• The staff reports as necessary to the FFT LLC Oversight Committee on entity's status with regard to information security.

B. **Information Owner:** The owner of a collection of information is usually the customers responsible for the creation of that information and the primary user of that information. The owner of information has the responsibility for:

1. Keep logons and passwords, as well as screens, safe.
2. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
3. Reporting promptly to FFT LLC the loss or misuse of FFT LLC information.
4. Initiating corrective actions when problems are identified.
5. Promoting employee and consultant education and awareness by utilizing programs approved by the ISO, where appropriate.
6. Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

C. Custodian: The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:
1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
5. Evaluating the cost effectiveness of controls.
6. Reporting promptly to the ISO the loss or misuse of FFT LLC information.
7. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

D. User Management: FFT LLC- management who supervise users as defined below. User management is responsible for overseeing their employees', consultants, and contracted site's use of information, including:
1. Reviewing and approving all requests for their employees', consultants', and contracted sites' access authorizations.
2. Initiating security change requests to keep employees', consultants', and contracted sites' security record current with their positions and job functions.
3. Promptly informing appropriate parties of employee consultants', and contracted sites' terminations and transfers, in accordance with local entity termination procedures.
4. Providing employees, consultants, and contracted sites with the opportunity for training needed to properly use the computer systems.
5. Reporting promptly to the CEO the loss or misuse of FFT LLC information.
7. Initiating corrective actions when problems are identified.
8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

E. **User:** The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:
1. Access information only in support of their authorized job responsibilities.
2. Refer all disclosures of PHI (1) outside of FFT LLC and (2) within FFT LLC, other than for

treatment, payment, or health care operations, to the CEO.
3. Keep personal authentication devices (e.g. passwords) confidential.
4. Report promptly to the CEO the loss or misuse of FFT LLC information.

VI. INFORMATION CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

A. Protected Health Information (PHI)

1. PHI is information, whether oral or recorded in any form or medium, that:

a. is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or health clearinghouse; and

b. relates to 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

c. includes demographic data, that permits identification of the individual or could reasonably be used to identify the individual.

2. Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious damage to FFT LLC and its patients or

research interests. No PHI will be shared with third parties. Individuals can request their PHI at any point by contacting FFT LLC. There is no onward transfer of information to third parties. If an individual wishes to have their PHI unlisted or have the data be concealed, they can contact FFT LLC.

B. Confidential Information

1. Confidential Information is very important and highly sensitive material that is not classified as PHI. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for FFT LLC, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

C. Internal Information

1. Internal Information is intended for unrestricted use within FFT LLC, and in some cases within affiliated organizations such as FFT LLC business partners This type of information is already widely-distributed within FFT LLC or it could be so distributed within the organization without advance permission from the information owner.

Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

2. Any information not explicitly classified as PHI, Confidential or Public will, by default, be classified as Internal Information.

3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

D. Public Information

1. Public Information has been specifically approved for public release by a designated

authority within each entity of FFT LLC. Examples of Public Information may include marketing brochures and material posted to FFT LLC entity internet web pages as well as lawful requests by public authorities, including to meet national security or law enforcement requirements.
2. This information may be disclosed outside of FFT LLC

VII. COMPUTER AND INFORMATION CONTROL

All involved systems and information are assets of FFT LLC and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. **Ownership of Software:** All computer software developed by FFT LLC employees or contract personnel on behalf of FFT LLC or licensed for FFT Inc. use is the property of FFT LLC and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. **Installed Software:** All software packages that reside on computers and networks within FFT LLC must comply with applicable licensing agreements and restrictions and must comply with FFT LLC acquisition of software policies.

D. **Access Controls:** Physical and electronic access to PHI, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Security Officer and approved by FFT LLC. Mechanisms to control access to PHI, Confidential and Internal information include (but are not limited to) the following methods:

1. **Authorization:** Access will be granted on a “need to know” basis and must be authorized by the immediate supervisor and application owner with the assistance of the ISO. Any of the following methods are acceptable for providing access under this policy:

a. **Context-based access:** Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external” factors might include time of day, location of the user, strength of user authentication, etc.

b. **Role-based access:** An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization’s structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

c. **User-based access:** A security mechanism used to grant users of a system access based upon the identity of the user.

2. **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access PHI, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

a. At least one of the following authentication methods must be implemented:

1. strictly controlled passwords (Attachment 1 – Password Control Standards),
2. biometric identification, and/or
3. tokens in conjunction with a PIN.

b. The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

c. An automatic timeout re-authentication must be required after a certain period of no activity.

d. The user must log off or secure the system when leaving it.

3. Data Integrity: FFT LLC must be able to provide corroboration that PHI, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

a. transaction audit
b. disk redundancy (RAID)
c. ECC (Error Correcting Memory)

d. checksums (file integrity)
e. encryption of data in storage
f. digital signatures

4. **Transmission Security:** Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:
a. integrity controls and
b. encryption, where deemed appropriate

5. **Remote Access:** Access into FFT LLC network from outside will be granted using FFT LLC approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, PHI, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the FFT LLC network

6. **Physical Access**: Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.
The following physical controls must be in place:
a. Mainframe computer systems must be installed in an access- controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
b. File servers containing PHI, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
c. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:
1. Position workstations to minimize unauthorized viewing of protected health information.
2. Grant workstation access only to those who need it in order to perform their job function.
3. Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected health information.
4. Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to PHI.
5. Use automatic screen savers with passwords to protect unattended machines.
d. Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:
1. Contingency Operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
2. Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
3. Access Control and Validation – Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
4. Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

7. **Emergency Access:**
a. Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.
b. Procedures must be documented to address:
1. Authorization,
2. Implementation, and

3. Revocation

E. Equipment and Media Controls: The disposal of information must ensure the continued protection of PHI, Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

1. Information Disposal / Media Re-Use of:

a. Hard copy (paper and microfilm/fiche)

b. Magnetic media (floppy disks, hard drives, zip disks, etc.) and

c. CD ROM Disks

2. Accountability: Each entity must maintain a record of the movements of hardware and electronic media and any person responsible therefore.

3. Data backup and Storage: When needed, create a retrievable, exact copy of electronic PHI before movement of equipment.

F. **Other Media Controls:**

1. PHI and Confidential Information stored on external media (diskettes, cd- roms, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as PHI or Confidential Information. Further, external media containing PHI and Confidential Information must never be left unattended in unsecured areas.

2. PHI and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:

a. Power-on passwords

b. Auto logoff or screen saver with password

c. Encryption of stored data or other acceptable safeguards approved by Information Security Officer

Further, mobile computing devices must never be left unattended in unsecured areas.

3. If PHI or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of FFT LLC Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with FFT LLC.

G. **Oral Communications:** FFT LLC employees and should be aware of their surroundings when discussing PHI and Confidential Information. This includes the use of cellular telephones in public areas. FFT LLC employees and consultants not discuss PHI or Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

H. **Evaluation:** FFT LLC requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection.

I. **Contingency Plan:** Controls must ensure that FFT LLC can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PHI, Confidential, or Internal Information. This will include developing policies and procedures to address the following:

1. Data Backup Plan:

a. A data backup plan must be documented and routinely updated to create and maintain, for

a specific period of time, retrievable exact copies of information.
b. Backup data must be stored in an off-site location and protected from physical damage.
c. Backup data must be afforded the same level of protection as the original data.
2. Disaster Recovery Plan: A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
3. Emergency Mode Operation Plan: A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
4. Testing and Revision Procedures: Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.
5. Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

Compliance [§ 164.308(a)(1)(ii)(C)]

A. The Information Security Policy applies to all users of FFT LLC information including: employees, medical staff, students, volunteers, and outside affiliates. Failure to comply with Information Security Policies and Standards by employees, medical staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable FFT LLC procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with Information Security Policies and Standards by students may constitute grounds for corrective action in accordance with FFT LLC procedures. Further, penalties associated with state and federal laws may apply.
B. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:
1. Unauthorized disclosure of PHI or Confidential Information as specified in Confidentiality Statement.
2. Unauthorized disclosure of a sign-on code (user id) or password.
3. Attempting to obtain a sign-on code or password that belongs to another person.
4. Using or attempting to use another person's sign-on code or password.
5. Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.
6. The intentional unauthorized destruction of FFT LLC information.
7. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

In compliance with the Privacy Shield Principles, FFT LLC commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Private Shield policy should first contact FFT LLC at: holly@fftllc.com.

FFT LLC has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning data transferred from the EU. Their services are provided at no cost to you.
http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

If under certain circumstances the above is not satisfactory, individuals have the ability to invoke binding arbitration before the privacy shield panel.

--- ATTACHMENT 1 ---

Password Control Standards

The FFT LLC Information Security Policy requires the use of strictly controlled passwords for accessing Protected Health Information (PHI), Confidential Information (CI) and Internal Information (II). (See FFT LLC Information Security Policy for definition of these protected classes of information.)
Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for accessing PHI, CI, II:
Users are responsible for complying with the following password standards:
1. Passwords must never be shared with another person, unless the person is a designated security manager.
2. Passwords must, where possible, have a minimum length of six characters.
3. Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
4. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
5. When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc…). A combination of alpha and numeric characters are more difficult to guess.

Where possible, system software must enforce the following password standards:
1. Passwords routed over a network must be encrypted.
2. Passwords must be entered in a non-display field.
3. Sysem software must maintain a history of previous passwords and prevent their reuse.