European Centre for Information Policy and Security (ECIPS)

ECIPS Information Security Policy

I. POLICY

A. It is the policy of **ECIPS** that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized use, modification, destruction or disclosure throughout its life cycle by unauthorized or authorized personnel **without proper and necessary clearances**. This protection includes an appropriate level of security over the data, information, equipment and software used to process, store, and transmit appropriate information.

B. All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 6 (six) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within **ECIPS**.

C. At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

II. SCOPE

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

B. The framework for managing information security in this policy applies to all **ECIPS** entities and staff, and other Involved Persons and all Involved Systems throughout **ECIPS** as defined below in **INFORMATION SECURITY DEFINITIONS.**

C. This policy and all standards apply to all protected data, hardware, information and 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 **ECIPS** information networks and systems will be conducted on a periodic basis to document the threats to and vulnerabilities of 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.

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 ECIPS research programs.

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.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

Involved Persons: Every worker at ECIPS-- no matter what their status. This includes physicians, residents, students, employees, contractors, consultants, temporaries, volunteers, interns, etc.

Involved Systems: All computer equipment and network systems that are operated within the **ECIPS** environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

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

CLASSIFIED: Classified shall mean all information under section 5775/01 SW/mc 8 ANNEX JUR section 22 page 11: 'If the Council **receives classified information** from third States, from **international organizations** or from other third parties, that information shall be given protection appropriate to its classification and equivalent to the standards established in these regulations for EU classified information, or such higher standards as may be required by the third party releasing the information. Mutual checks may be arranged.''

V. INFORMATION SECURITY RESPONSIBILITIES

A. **Information Security Officer:** The Information Security Officer (**ISO**) for each entity is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of **ECIPS**. Specific responsibilities include:

1. Ensuring security policies, procedures, and standards are in place and adhered to by entity.
2. Providing basic security support for all systems and users.
3. Advising owners in the identification and classification of computer resources. See Section VI Information Classification.
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
6. Providing on-going employee security education.
7. Performing security audits.
8. Reporting regularly to the **ECIPS** Oversight Committee on entity's status with regard to information security.

B. **Information Owner:** The owner of a collection of information is ECIPS. The manager of such information responsible for the creation of that information or the primary user of that information. This role often corresponds with the management

of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may not be shared. The owner may delegate ownership responsibilities to another individual by completing the **ECIPS** Information Owner Delegation Form. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on advice from the **ECIPS**'s Legal Department.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
4. Authorizing access and assigning custodianship.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of ECIPS information.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
9. 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. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.
7. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
8. Reporting promptly to the ISO the loss or misuse of **ECIPS** information.
9. Identifying and responding to security incidents and initiating appropriate **actions when problems are identified.**

D. **User Management: ECIPS** management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

1. Reviewing and approving all requests for their employees access authorizations.
2. Initiating security change requests to keep employees' security record current with their positions and job functions.
3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the ISO the loss or misuse of **ECIPS** 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 or data. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.
2. Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.
3. Keep personal authentication devices (e.g. passwords, Secure Cards, PINs, etc.) confidential.
4. Report promptly to the ISO the loss or misuse of **ECIPS** information.
5. Initiate corrective actions when problems are identified.

F. SECURITY OF INFORMATION (INFOSEC)

INFOSEC relates to the identification and application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional. Adequate countermeasures shall be taken in order to prevent access to ECIPS information by unauthorized users, to prevent the denial of access to ECIPS information to authorized users, and to prevent corruption or unauthorized modification or deletion of ECIPS DATA 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 Information (PI)

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

   a. is created or received by a authority, employer, or university or; 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 ECIPS and its clients or research interests.

B. Confidential Information

1. Confidential Information is very important and highly sensitive material that is not classified as PI. 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 ECIPS, 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 **ECIPS**, and in some cases within affiliated organizations such as **ECIPS** business partners. This type of information is already widely-distributed within ECIPS, 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 PI, Confidential or Public will, by default, be classified as Internal Information.

3. Unauthorized disclosure of this information to outsiders are strictly forbidden and can be prosecuted by ECIPS or any other authority.

D. **Public Information**

1. Public Information has been specifically approved for public release by a designated authority within each entity of **ECIPS**. Examples of Public Information may include marketing brochures and material posted to ECIPS entity internet web pages.

2. This information may be disclosed outside of **ECIPS**.

E. **Non - Public Information**

European Centre for Information Policy and Security, has 4 levels of Security Information, COSMIC (TOP SECRET) , EC-SECRET, EC-CONFIDENTIAL and EC-COMMITTEE.

Notes: Special Clearances

Depending on the level of classification there are different rules controlling the level of clearance needed to view such information, and how it must be stored, transmitted, and destroyed. Additionally, access is restricted on a "need to know" basis. Simply possessing a clearance does not automatically authorize the individual to view all material classified at that level or below that level. The individual must present a legitimate "need to know" in addition to the proper level of clearance.

VII. COMPUTER AND INFORMATION CONTROL

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

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

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

C. **Virus Protection:** Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

D. **Access Controls:** Physical and electronic access to PI, 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 **ECIPS**. Mechanisms to control access to PI, 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 PI, 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 (maximum 15 minutes).

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

3. **Data Integrity: ECIPS** must be able to provide corroboration that PI, 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 **ECIPS** network from outside will be granted using **ECIPS** 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 **ECIPS** 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 PI, 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 (PHI).

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 PI, 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 PI 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 PI before movement of equipment.

F. **Other Media Controls:**

1. PI 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 PI or Confidential Information. Further, external media containing PI and Confidential Information must never be left unattended in unsecured areas.

2. PI 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 PI 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 **ECIPS** Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with **ECIPS**.

G. **Data Transfer/Printing:**

1. **Electronic Mass Data Transfers:** Downloading and uploading PI, Confidential, and Internal Information between systems must be strictly controlled. Requests for mass downloads of, or individual requests for, information for research purposes that include PI must be approved through the Internal Review Board (IRB). All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Applicable Business

Associate Agreements must be in place when transferring PI to external entities (see **ECIPS** policy B-2 entitled "Business Associates").

2. **Other Electronic Data Transfers and Printing:** PI, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PI and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PI that is downloaded for educational purposes where possible should be de-identified before use.

H. **Oral Communications:** **ECIPS** staff should be aware of their surroundings when discussing PI and Confidential Information. This includes the use of cellular telephones in public areas. **ECIPS** staff should not discuss PI 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.

I. **Audit Controls:** Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PI must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for six (6) years.

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

K. **Contingency Plan:** Controls must ensure that **ECIPS** 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 PI, 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. Information Security Policy applies to all users of **ECIPS** 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 **ECIPS** 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 **ECIPS** 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 PI 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. Installing or using unlicensed software on **ECIPS** computers.
7. The intentional unauthorized destruction of **ECIPS** information.
8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

--- ATTACHMENT 1 ---

Password Control Standards

The **ECIPS** Information Security Policy requires the use of **strictly** controlled passwords for accessing Protected Health Information (PHI), Confidential Information (CI) and Internal Information (II). (See **ECIPS** 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 PI, 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. Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity of the information being accessed)
3. Passwords must, where possible, have a minimum length of six characters.
4. 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.
5. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
6. 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. System software must enforce the changing of passwords and the minimum length.
4. System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15 minute timeframe. Lockout time must be set at a minimum of 30 minutes.
5. System software must maintain a history of previous passwords and prevent their reuse.