

# INFORMATION SECURITY POLICY (ISP)

<<insert date>>

Information Security Office

# INFORMATION SECURITY POLICY

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

## TABLE OF CONTENTS

I.	Purpose .....	2
II.	Scope .....	2
III.	Information Security Policy .....	2
VI.I	Safeguards .....	3
	Safeguarding confidential information – <b>On-site</b> workplace practices: .....	3
	Safeguarding confidential information – <b>Off-site</b> workplace practices: .....	6
VI.II	Internal Risk Mitigation Policies .....	6
VI.III	External Risk Mitigation Policies .....	8

## Revision History

Date of Change	Responsible	Summary of Change
September 2018	TTG SAS	TTG template revision v4

# INFORMATION SECURITY POLICY

**Responsible Office:** <<TBD>>

**Effective Date:** <<insert date>>

## I. PURPOSE

This policy describes the administrative, physical and technical safeguards the Operations and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at , hereinafter, referred to as the "Practice". It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Practice with policies and guidelines concerning the use of Practice technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Practice employees or temporary workers at all locations and by contractors working with the Practice as subcontractors.

## II. SCOPE

This policy document defines common security requirements for all Practice personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the Practice, entities in the private sector, in cases where Practice has a legal, contractual or fiduciary duty to protect said resources while in Practice custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Practice network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Practice in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Practice domain or Virtual Local Area Network (VLAN), either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Practice at its office locations or at remote locales

## III. INFORMATION SECURITY POLICY

The policies outlined on the Safeguards, Internal and External Risks are related to the use of the Practice computer and network resources, and other Practice Information Resources, as well as to Practice requirements and standards concerning the privacy and security of various designated categories of information maintained by the Practice. These policies describe the administrative, technical and physical safeguards employed to protect the security of information maintained by the Practice and to ensure that appropriate information resources are available when needed.

# INFORMATION SECURITY POLICY

**Responsible Office:** <<TBD>>

**Effective Date:** <<insert date>>

All users of the Practice's information and information systems must read and understand their responsibilities under the WISP. Any questions regarding the WISP should be directed to the ISC.

## VI.I Safeguards

The Practice values privacy rights and is committed to safeguarding confidential information. Regulations require that the Practice have reasonable administrative, technical and physical safeguards in place to protect confidential information from any intentional or unintentional use or disclosure and to limit incidental uses or disclosures. We will only collect "confidential" information of clients, customers or employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal, state or local regulations. The Practice will make reasonable efforts to use or disclose only the minimum amount of "confidential" information necessary for business operations.

- (1) ADMINISTRATIVE SAFEGUARDS:** The administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect "confidential" information and to manage the conduct of the Practice workforce in relation to the protection of that information
- (2) PHYSICAL SAFEGUARDS:** The physical measures, policies and procedures to protect and secure all forms of "confidential" information from unauthorized access, accidental or intentional use, disclosure, transmission, or alteration, and inadvertent or incidental disclosure.
- (3) TECHNICAL SAFEGUARDS:** The technology and the policy and procedures relating to electronic storage, maintenance, and transmittal of "confidential" information, including authentication requirements, password controls, audit trails, email encryption, and Internet use.

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing "confidential" information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

To the extent that any of these measures require a phase-in period, such phase-in must be completed on or before <<EFFECTIVE DATE>>.

Safeguarding confidential information – **On-site** workplace practices:

### **Paper**

- A. Each Practice workplace will store files and documents in locked rooms or storage systems.

# INFORMATION SECURITY POLICY

**Responsible Office:** <<TBD>>

**Effective Date:** <<insert date>>

- B. In workplaces where lockable storage is not available, Practice staff must take reasonable efforts to ensure the safeguarding of confidential information.
- C. Each Practice workplace will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.
- D. Each Practice workplace will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

## Mail

- A. Each Practice workplace will ensure that mail is prepared accurately for delivery.
- B. Outgoing mail must include a complete sending address, including first and last name of recipient, agency name, and complete street and city address. If printed labels are not used, write or print legibly. The outgoing mail must also include a complete return address (first and last name of sender, business entity, complete street and city address).

## Oral

- A. Practice staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.
- B. Each Practice workplace shall make enclosed offices and/or interview rooms available for the verbal exchange of confidential information.
- C. Each Practice workplace must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information

## Visual

- A. Practice staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.
  - i. Computer screens: Each Practice workplace must make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.
  - ii. Paper documents: Practice staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

## Computer/electronic

- A. Each Practice workplace must take reasonable and necessary steps to assure that confidential information in electronic form cannot be accessed by individuals who do not have a job-related reason for accessing that particular confidential information. Such reasonable safeguards include but are not limited to individualized

# INFORMATION SECURITY POLICY

**Responsible Office:** <<TBD>>

**Effective Date:** <<insert date>>

password for access to personal computers, laptops, personal digital assistants (PDAs) and other similar devices and password protected screen savers.

- B. Access to records containing "confidential" information shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.
- C. Each Practice workplace must take reasonable and necessary steps to assure that all personal computers, laptops (including hard drives, disks, CDs, tapes, and other similar devices), and PDAs and other similar devices in which confidential information is stored is backed up on a regular basis and stored in a manner not inconsistent with this policy.
- D. Each Practice workplace must take reasonable and necessary measures to assure that all confidential information stored on personal computers, laptops (including hard drives, disks, CDs, tapes, and other similar devices), PDAs and other similar devices is destroyed on a timely basis, documented and consistent with all applicable record retention requirements and all such devices must be completely wiped clean of all confidential information prior to disposal of the device. Written and electronic records containing "confidential" information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.
- E. Current employee user IDs and passwords shall conform to accepted security standards. All passwords shall be changed at least annually, more often as needed (e.g. quarterly).
- F. Each Practice workplace must foster workforce awareness of the potential for inadvertent disclosure of confidential information contained within personal computers, laptops, PDAs and other similar devices.

# INFORMATION SECURITY POLICY

**Responsible Office:** <<TBD>>

**Effective Date:** <<insert date>>

## Safeguarding confidential information – Off-site workplace practices:

- A. All the safeguard requirements for the work place apply equally to any use of confidential information away from or off-site from the Practice work place. Files and records should be securely transported.
- B. Computer/electronic
  - i. Practice staff authorized to use laptop computers off-site are responsible for assuring the security, as well as minimized risk of loss, of the device and its contents.
  - ii. Practice staff working on non-work shared computers should observe security protocols to prevent unauthorized users from accessing confidential information. Shared use of computers with family members or others who are not part of the Practice work force creates a risk of inadvertent disclosure of confidential information.
  - iii. Practice staff are responsible for securing digital camera images. Digital cameras can store confidential information that can be accessed by anyone who has the camera.
- C. Telephone
  - i. Practice staff should ensure care when using telephones outside of the work space. Cell phones, iPhones or other mobile devices require care to protect confidential information.
  - ii. Practice staff should avoid using identifiable information about Practice clients unless staff have taken reasonable efforts to assure the privacy of the call.

## **VI.II Internal Risk Mitigation Policies**

- A. A copy of the WISP's Information Security Policy and Acceptable Use Policy are to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing, by signing the attached sheet, that he/she has received a copy of the afore stated WISP policies and will abide by its provisions. Employees are encouraged and invited to advise the ISC of any activities or operations which appear to pose risks to the security of "confidential" information. If the ISC is him or herself involved with these risks, employees are encouraged and invited to advise any other manager or supervisor or business owner.
- B. A training session for all current employees will be held on <<Insert Date>> to detail the provisions of the WISP.
- C. All employment contracts, where applicable, will be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of "confidential" data as defined by the WISP.
- D. Employees are required to report suspicious or unauthorized use of "confidential" information to a supervisor or the ISC.

# INFORMATION SECURITY POLICY

**Responsible Office:** <<TBD>>

**Effective Date:** <<insert date>>

- E. Whenever there is an incident that requires notification, ISC will follow State and Federal Regulations in reporting the breach. The ISC shall host a mandatory post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard "confidential" information. Refer to Article X of the WISP.
- F. Terminated employees must return all records containing "confidential" data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee
- G. ISC to notify ePHI application(s) and network administrators of any termination immediately or as soon as possible. A terminated employee's physical and electronic access to records containing "confidential" information shall be restricted at the time of termination. This shall include remote electronic access to "confidential" records, voicemail, internet, and email access. All keys, keycards, access devices, badges, Practice IDs, business cards, and the like shall be surrendered at the time of termination.
- H. Disciplinary action will be applicable to violations of the WISP, irrespective of whether "confidential" data was actually accessed or used without authorization.  
All security measures including the WISP shall be reviewed at least annually beginning Nov 2016 to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.
- I. Should our business practices change in a way that impacts the collection, storage, and/or transportation of records containing "confidential" information the WISP will be reviewed to ensure that the policies contained in the WISP are adequate to meet all applicable federal and state regulations, ISC will send a copy of the revised WISP to TTG using ShareFile.
- J. The ISC or his/her designee shall be responsible for all review and modifications of the WISP and shall fully consult and apprise management of all reviews including any recommendations that improve security arising from the review.
- K. The ISC shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which employee possess keys, keycards, or other access devices and that only approved employee have been provided access credentials
- L. The ISC or his/her designee shall ensure that access to "confidential" information in restricted to approved and active user accounts. ISC will review <<(ePHI application(s))>> user access levels on a regular basis to ensure adherence to role based access controls.



# INFORMATION SECURITY POLICY

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

## VI.III External Risk Mitigation Policies

To mitigate external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing "confidential" information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures must be completed on or before <<EFFECTIVE DATE>>:

- A. Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes "confidential" information. Server and Firewall Security logs review process will be performed by TTG every quarter during the scheduled Server Preventive Maintenance.
- B. "Confidential" information shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy.
- C. All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes "confidential" information.
- D. There shall be secure user authentication protocols in place that:
  - i. Control user ID and other identifiers;
  - ii. Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;
  - iii. Control passwords to ensure that password information is secure.
- E. All computer systems must be monitored for unauthorized use of or access to "confidential" information.
- F. To the extent technically feasible, all "confidential" information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.