

INCIDENT RESPONSE POLICY (IRP)

<<insert date>>

Information Security Office
ENTER PRACTICE NAME HERE

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

TABLE OF CONTENTS

I.	Purpose	2
II.	Scope	2
III.	Incident Response Policy	2
IV.	Incident Reporting	4
	Escalation	5
	Mitigation and Containment	5
	Eradication and Restoration	6
	Ongoing Reporting	6
	Notification of Breach	7
	Notification to Individuals	7
	Notification to the Media.....	9
	Notification to the State Offices.....	9
	Notification to the Secretary of DHHS.....	9
	Review.....	10

Revision History

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

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

I. PURPOSE

To establish an incident response policy for all members of the Practice workforce, including management. This policy is a process guide for a response to a computer incident or event impacting the Practice computing equipment, data, or networks.

This policy serves to minimize the negative consequences of information security incidents and to improve the Practice's ability to promptly restore operations affected by such incidents. It ensures incidents are promptly reported to the appropriate Practice officials, that they are consistently and expertly responded to whether suspected or actual, and that serious incidents are properly monitored.

II. SCOPE

This incident response policy applies to all the Practice customers, employees and individuals associated with the Practice, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the Practice, including any Third Party Provider services to the Practice, who create, use or otherwise access or interact with any Practice Information or Practice Information Resource.

This Program applies to all "confidential" information as defined by the Practice Written Information Security Program or "WISP", including all information collected, stored or used by or on behalf of any department and person in connection with Practice operations. In the event that any particular information is governed by more specific requirements under other Practice policies or procedures, the more specific requirements shall take precedence over this Program to the extent there is any conflict.

Managers are responsible for ensuring that its employees are aware of policies and notifying employees of policy change or the creation of new policies that pertain to the department function.

III. INCIDENT RESPONSE POLICY

"Confidential" information must be treated with respect and care by any person with access to this information. This policy will determine the procedure to mitigate all breaches, both willful violations and unintended actions, consistent with guidance described by the [State of Connecticut](#), the [Commonwealth of Massachusetts](#), HIPAA and HITECH rules. The Practice will properly report and respond to breaches when they occur.

Incidents are prioritized based on the following:

- Criticality of the affected resources (e.g., public Web server, user workstation)
- Current and potential technical effect of the incident (e.g., root compromise, data destruction).

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

Combining the criticality of the affected resources and the current and potential technical effect of the incident determines the business impact of the incident—for example, data destruction on a user workstation might result in a minor loss of productivity, whereas root compromise of a public Web server might result in a major loss of revenue, productivity, access to services, and reputation, as well as the release of confidential data (e.g., credit card numbers, Social Security numbers). Refer to the written information security program ("WISP") section X – Breach of Data Security Protocol.

A **"Breach"** means unauthorized acquisition, access, use or disclosure of "confidential" information in a manner not permitted by the information privacy laws of Connecticut, Massachusetts or HIPAA privacy rule, which compromises the security or privacy of that information.

"Access" means the ability to read, write, modify or communicate data in any form or otherwise use any system resource

"Breach" does not mean:

- Unintentional acquisition or use in good faith within the course and scope of employment by someone authorized to access "confidential" material and the information is not further used or disclosed in a way that is inconsistent with the requirements of the information privacy laws of Connecticut, Massachusetts or HIPAA Privacy or Security Rule, or
- Inadvertent disclosure by an authorized person to another authorized person within the same Practice, **Covered Entity or Business Associate** and the information is not further used or disclosed in a way that is inconsistent with the requirements of the privacy laws of Connecticut, Massachusetts or HIPAA Privacy or Security Rule, or
- A disclosure of "confidential" information where the Practice, a **Covered Entity or Business Associate** has a good faith belief that an unauthorized person who receives the information would not reasonably have been able to retain such information.
- Examples of a Breach (this is not an all-inclusive list):
 - Authorized user accesses a patient's information without a functional "need to know" including someone that improperly acquires, accesses, uses, reviews and/or discloses records of any Individual or requests another person do so.
 - Release of patient information to an outside party for any unauthorized purpose – examples may include releases to the media, to relatives or friends of a patient, or sale of "confidential" information
 - Electronic hacking or theft of patient file or database
 - "Dumpster diving" and finds "confidential" information

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

- Unauthorized user using another authorized person's ID/password to access patient information including Stealing or sharing passwords or not reporting a known lost password.
- Persons discussing "confidential" information in any public area where those who have no need to know the information can overhear.
- Someone leaves paper copy of any Individual's health information in a public area.
- Unauthorized access to health records areas and health records.
- Someone leaves a computer unattended in a publicly accessible area with health record information unsecured.
- Failure to log off computer terminal.
- Unauthorized access to "confidential" information, paper or electronic, that is neither protected by encryption nor properly destroyed.
- Introduction of viruses, worms, Trojan horses, or other malicious software into the organization's computer systems.
- Unauthorized access to networks, computer systems, or facilities/equipment rooms housing the computer systems.
- Unauthorized destruction/changing of "confidential" information.
- Improperly discarding "confidential" information (not physically destroying it) whether paper or electronic media.
- Loss or theft of any Mobile Computing Device with "confidential" information that is discoverable and not properly protected/encrypted

Note that some violations may rise to the level of breach as defined by the HITECH Law.

IV. INCIDENT REPORTING

All computer security incidents, including suspicious events, shall be reported immediately (orally or via e-mail) to the department IT manager and/or department supervisor by the employee who witnessed/identified the breach. The "Security Incident Report" form is required for reporting suspected incidents.



E1 Security Incident
Report.doc

Supervisors/managers and/or the "Information Security Coordinator" or ("ISC") shall start from the presumption that the security incident and/or suspected breach that has been identified constitutes a reportable breach under the information privacy laws of Connecticut, Massachusetts or HIPAA/HITECH Act unless they are able to demonstrate and document that there is a low probability that the sensitive, non-public has been compromised. The supervisors/managers and/or the ISC shall conduct the following risk

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

assessment by assessing for specific factors and document the result on the "Security Incident Investigation Report" form:

- i. To whom the information was impermissibly disclosed;
- ii. Whether the information was actually accessed or viewed;
- iii. The potential ability of the recipient to identify the subjects of the data; and
- iv. Whether the recipient took appropriate mitigating action.

Once the initial review by the above supervisor/manager has been completed and documented, the supervisor/manager shall immediately submit the completed "Security Incident Investigation Report" to the **Practice's Privacy Officer**.



E2 Security Incident
Investigation Report

The **Privacy Officer** shall record the security incident to the "Security Incident Report Log"



E3 Security Incident
Report Log.xls

And maintain copies of the "Security Incident Investigation Report" for a minimum of **six (6) years** from the date of the form.

Escalation

The department manager and/or department head needs to determine the criticality of the incident (as stated in section 2.0 Policy). If the incident is something that will have serious impact, senior management will be notified and briefed on the incident.

The **Privacy Officer** or his/her designee will determine if other departments or personnel need to become involved in resolution of the incident. Only the **Privacy Officer and/or designated senior management** will speak to the press about an incident.

Mitigation and Containment

Any system, network, or security administrator who observes an intruder on the Practice network or system shall take appropriate action to terminate the intruder's access. (Intruder can mean a hacker, botnet, malware, etc.) Affected systems, such as those infected with malicious code or systems accessed by an intruder shall be isolated from the network until the extent of the damage can be assessed. Any discovered vulnerabilities in the network or system will be rectified by appropriate means as soon as possible.

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

Information pertaining to investigations of breaches will only be shared with those who have a need to know. Confidentiality of all participants in the reported situation shall be maintained to the extent reasonably possible throughout any resulting investigation. The Practice's Privacy Officer will complete the "Privacy Breach Assessment" to assist in determining the severity. The Privacy Officer and relevant management or staff will conduct the necessary and appropriate investigation commensurate with the level of breach and the specific facts. This investigation may include, but is not limited to, interviewing the individuals involved, interviewing other individuals, obtaining specific facts surrounding the violation/breach and reviewing pertinent documentation.



E4 Privacy Breach
Assmt.doc

Eradication and Restoration

The extent of damage must be determined and course of action planned and communicated to the appropriate parties.

Information Dissemination: Any public release of information concerning a computer security incident shall be coordinated through the **Privacy Officer and designated senior management**.

The **Privacy Officer and/or designated Senior Management** shall manage the dissemination of incident information to other participants, such as law enforcement or legal. After consulting with senior management, **Privacy Officer and/or designated Senior Management** shall coordinate dissemination of information that could affect the public, such as web page defacement or situations that disrupt systems or applications.

Ongoing Reporting

After the initial oral or e-mail report is filed, and if the incident has been determined to be a significant event (such as multiple workstations effected, root compromise, data breach, etc.), subsequent reports shall be provided to the Practice's **Privacy Officer** and appropriate managers. Incidents such as individual workstations infected with malware are considered minor events and need not be followed up with a written report.

The incident reports shall be submitted within 24 hours of the incident. A department may be required to provide reports sooner in accordance with more stringent regulations. For example: HIPAA, SSA and IRS requirements. If this is the case, the more stringent requirements are to be met.

A general report to the Senior Management shall contain the following:

- Point of contact
- Affected systems and locations

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

- System description, including hardware, operating system, and application software
- Type of information processed, such as HIPAA related information
- Incident description
- Incident resolution status
- Damage assessment, including any data loss or corruption
- Organizations contacted
- Corrective actions taken
- Lessons learned

A follow-up report shall be submitted upon resolution by those directly involved in addressing the incident.

- (1) Documentation regarding reported privacy and/or security breaches shall be maintained by the HIPAA-Covered Component, Practice Privacy Officer and ISC, and provided to Senior Management and/or the Security Breach Team where appropriate.
- (2) "Security Incident Investigation Report" shall be maintained by the Practice's Privacy Officer and the HIPAA-Covered Component for a **minimum of six (6)** years from the data of the form.
- (3) All information documenting the process required under HIPAA Privacy and Security and HITECH law regarding the violation or breach will be retained for a **minimum of six (6) years** by the Practice's Privacy Officer and/or the ISC.
- (4) Violations that meet the definition of breach under the HIPAA/HITECH Act as amended shall be reported as required to the Department of Health and Human Services Office of Civil Rights.

Notification of Breach

Where the risk analysis leads the Practice to the determination that a reportable breach has occurred, the Practice will follow appropriate and applicable notification standards.

Notification to Individuals

1. Where appropriate and/or required, the Practice shall notify each Individual whose unsecured sensitive, non-public ("confidential" information) has been, or is reasonably believed by the Practice to have been accessed, acquired, used, or disclosed as a result of a breach. The Practice will provide the required notification without unreasonable delay and in accordance with timelines required by law.
2. The required notification shall be written in plain language and shall include, to the extent possible and/or permitted by law:
 - a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 - b. A description of the types of unsecured "confidential" information that were involved in the breach (such as whether full name, social security

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

- number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- c. Steps Individuals should take to protect themselves from potential harm resulting from the breach;
 - d. A brief description of what the Practice has done/is doing to investigate the breach, to mitigate harm to Individuals, and to protect against any further breaches; and
 - e. Contact procedures for Individuals to ask questions or learn additional information.
3. The required notification to Individuals shall be provided in the following form:
- a. Written notification by first-class mail to the Individual at the last known address of the Individual or, if the Individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.
 - b. If the Practice knows the Individual is deceased and has the address of the next of kin or authorized representative of the Individual, written notification by first-class mail to either the next of kin or authorized representative of the Individual. The notification may be provided in one or more mailings as information is available.
 - c. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the Individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or authorized representative of the Individual. Substitute notice must consist of all of the following:
 - i. E-mail notice, if the person has e-mail addresses for the Individuals to be notified;
 - ii. Conspicuous posting of the notice on the Practice and/or HIPAA-Covered Component's website home page;
 - iii. Notification to major print or broadcast media in geographic areas where the Individuals affected by the breach likely reside; and
 - iv. Include a toll-free phone number that remains active for at least 90 days where an Individual can learn whether the Individual's unsecured "confidential" information may be included in the breach.
 - d. (4) In any case deemed by the Practice to require urgency because of possible imminent misuse of unsecured "confidential" information, the Practice may provide information to Individuals by telephone or other means, as appropriate, in addition to the other forms of notice.

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

Notification to the Media

For a breach of unsecured sensitive, non-public ("confidential" information) involving more than **500 residents of a State or jurisdiction**, the Practice will notify prominent media outlets serving the State or jurisdiction within the timeline required by law. The required notification shall be written in plain language and shall include, to the extent possible:

- (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- (2) A description of the types of unsecured "confidential" information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- (3) Steps individuals should take to protect themselves from potential harm resulting from the breach;
- (4) A brief description of what the Practice is doing to investigate the breach, to mitigate harm to Individuals, and to protect against any further breaches; and
- (5) Contact procedures for Individuals to ask questions or learn additional information.

Notification to the State Offices

A Practice will, in accordance with [Connecticut Act 15-142](#) (Substitute Senate Bill No. 949 "An Act Improving Data Security and Agency Effectiveness) and/or the Security Breach Notifications of [Massachusetts General Law Chapter 93H: "Security Breaches"](#), the ISC shall notify the Connecticut Office of the Attorney General and/or the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office. Refer to Article X of the WISP.

Notification to the Secretary of DHHS

A Practice will, in accordance with the breach notification requirement of the HIPAA/HITECH Act, notify the Secretary of the U.S. Department of Health and Human Services (DHHS) of breach.

For breaches of unsecured sensitive ("confidential" information) involving 500 or more Individuals, the Practice shall provide notification to the Secretary contemporaneously with the notice provided to Individuals and in the manner specified on the HHS Web site.

For breaches of unsecured sensitive ("confidential" information) **involving less than 500 Individuals**, the Practice shall maintain a log and/or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification to the Secretary for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

ENTER PRACTICE NAME HERE

INCIDENT RESPONSE POLICY (IRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

Review

After the initial reporting and/or notification, the IT manager, department/agency managers and CIO shall review and reassess the level of impact that the incident created.