Effective April 26, 2023. This Incident Response Plan supersedes and replaces all prior versions.

Incident Response Plan

This Incident Response Plan is part of Provider's comprehensive effort to protect Client information as well as Provider's own confidential data. The purpose of this plan is to secure and to maintain the integrity of this data during any information security incident (an "Incident").

This plan includes incident notification processes, establishes a team to address Incidents, provides a common definition for determining the significance of an Incident, and outlines a method to assess and investigate Incidents.

PHASE I – REPORT INCIDENT

Any Provider employee or Client who becomes aware of an actual, imminent or potential Incident – an unauthorized disclosure of personal data – should provide notice as set forth below.

Types of Data and Unauthorized Disclosure

Personal Data. Personal data is information that is, or can be, about or related to an identifiable individual. Most of the information Provider collects about its customers and employees is likely to be considered personal data. Some examples of personal data include, but are not limited to:

- Name
- Contact information (address, phone number, e-mail address)
- Social security number or government identifier
- Other identification numbers, including customer or account numbers
- Financial account information
- Driver's license
- Date of birth, mother's maiden name
- Information that could lead to identity theft
- Personnel records
- Racial or ethnic origin
- Medical information (including Protected Health Information (PHI), as defined by federal regulations), Gender or Physical Characteristics
- Other information that an individual would not expect to be disclosed without his or her authorization

Type of Disclosure.

Incidents can result from any of the following, if personal data is potentially involved:

- Intentional and unintentional acts
- Actions of Provider's employees
- Actions of Provider's vendors or customers
- Actions of other, third parties
- External or internal acts

- Credit card fraud
- Potential violations of Provider's Privacy Policy
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism

PHASE II -- TEAM ASSEMBLY AND ORGANIZATION

The Incident Team is responsible for coordinating Provider response to an Incident.

Team Roles and Contacts

The following roles comprise the Incident Team:

Management. An officer or director of Provider has the ultimate responsibility for the decision or action plans to be implemented. Determines the strategy for resolution.

Legal. Provider's corporate or general counsel. Among other duties, determines and remains cognizant of the extent to which Incident Team activities are subject to the attorney-client privilege.

Human Resources. Provider's human resources officer. This individual is to serve as the primary point-of-contact for Provider employees to report an Incident and also is to alert the remainder of the Incident Team following the occurrence of an Incident.

HIPAA Officer. The individual at Provider most familiar with HIPAA and/or other applicable privacy laws and regulations. (This role may be filled by one of the other Incident Team members.)

Response Times

After the occurrence of an Incident, the Incident Team is to assemble for a preliminary meeting within the following response times:

	Definition	Example	Time for Initial Team Meeting
1	A breach of sensitive personal data has occurred	A file containing information subject to HIPAA or other privacy laws or regulations is disclosed.	Within 1 hour
2	A breach of non-sensitive personal data has occurred	Information about Client's account with Provider	Within 5 hours
3	A breach of personal data (sensitive or non-sensitive) is imminent	A disk containing non-encrypted account information is missing	Within 24 hours
4	A breach of personal data (sensitive or non-sensitive) is threatened	A former employee threatens to disclose Provider financial information.	Within 72 hours

Considerations for Initial Incident Team Meeting

The purpose of the initial Incident Team meeting is to assess of the information already available regarding the Incident at issue and to identify real or potential internal and external stakeholders that affect or are or may be affected by the Incident. Among the evaluation criteria that should be considered are:

- Is the information involved in the Incident really personal data?
- If the information already available is accurate, would notice to data subjects or the government be required by law?
- What would be the potential damage to data subjects and/or Provider arising from the misuse of disclosed data and the likelihood of misuse?
- How was the personal data compromised, or how might it be or have been subject to compromise?

In addition, at the initial meeting following the occurrence of an Incident, the Incident Team is to assign responsibility for creation and maintenance of a log to track the progress of the Incident Team's response to the Incident. (This responsibility is best assigned to Legal, whenever possible.)

PHASE III – CONDUCT INITIAL ASSESSMENT

Following the initial meeting, the Incident Team should proceed to conduct an initial assessment of the Incident.

Collect Relevant Information

The Incident Team should search internal information and media sources (if any) and should engage stakeholders to collect the information needed to prepare an appropriate response to an Incident.

Appropriate Questions. Examples of the sorts of questions that the Incident Team should ask in order to gather information are as follow:

- What data/content was breached?
- What data subjects are affected?
- Where are the affected data subjects located?
- What are the potential risks to Provider and to the data subjects?
- Where else are the data/system/supplier used?
- Are there any business continuity implications?
- When did the privacy/data protection breach occur and where?
- Was it reported to law enforcement? If not, should it be reported?
- Is it ongoing?
- Who was the custodian of the information (Provider vs. service provider)?
- Who in Provider is the data owner?
- Which system was compromised?
- Which systems interface with that system?
- Where is the service provider (if any) located?
- Where is the data housed?
- Can the asset/information compromised lead to another breach?
- Is the offender internal or external?
- Was the breach malicious (organized attack or a "mistake")?

Primary Objectives. The primary objectives of the Incident Team's information gathering activities are as follow:

- Determine for each potentially affected individual the specific personal data that may be at risk.
- Determine type of incident. What is the worst possible outcome for Provider and data subjects? What is the best possible outcome?
- Is notice to the data subjects warranted or recommended?
- Notification. The Incident Team is to carefully assess a number of legal considerations concerning notification to data subjects regarding an Incident, including the following:
- Is there a statutory legal obligation to notify?
- Are there other substantive legal considerations regarding notification (e.g., contractual or other liability)?
- Even if there appear to be no statutory or regulatory requirements for notification, consider:
- The nature of the breach and its potential impact on the data subject
- The type of personal data
- Could it lead to identity theft?
- Consider other personal data that an individual may want to be notified if it is accessed (e.g., medical records (including PHI), personnel files, etc.)
- The likelihood of misuse (the extent to which an unauthorized person has had an opportunity to use, access, or further disclose the personal data for illicit purposes)
- The potential damage arising from the misuse
- The tools available to both the company and its customers to identify and address the unauthorized use of customer personal data
- Whether a data subject receiving that notification can take steps to protect himself against identity theft or other fraud (e.g., notifying credit bureau or issuer of driver's license)
- Whether notification to data subjects can be deemed a part of damage mitigation efforts (both the HIPAA Privacy Rule and Security Rule require covered entities to mitigate the known harmful effects of any Privacy/Data Protection incidents)
- Whether notification might result in unnecessary alarm or confusion
- Whether over-notification might result in credit bureaus not being able to promptly respond to affected individuals

<u>Decisions Regarding Next Steps</u>

With the information gathered, the Incident Team is to determine what factors may affect Provider's response to an Incident. Those factors may include the following:

- Review and re-visit stakeholder identification.
- Determine whether notice to the government is required or recommended.
- Determine whether contact with credit bureaus is required or recommended.
- Determine what possible actions could be taken by affected data subjects and the extent to which Provider may be able to mitigate the risk.
- Assess resource needs (e.g., communications to data subjects, media statements, call centers, targeted web sites (public or private)).
- Develop concise, initial statement regarding the incident.

- Determine whether any early warning signals overlooked or ignored.

PHASE VI – INCIDENT CLOSING

Following the delivery of any final reports, the Incident Team should assess the effectiveness of its strategy and processes.

Verify Effectiveness of Response Plan

The Incident Team should closely monitor progress of the resolution plan and re- evaluate the resolution plan if necessary.

Document Lessons Learned

The Incident Team should assign responsibility for documentation and include lessons learned in the incident log.

Recommend Changes

The Incident Team should:

- Determine what, if anything, Provider could have done to prevent the Incident from happening
- Assess changes required to Provider business models, systems, and processes (administration, technology, and/or physical safeguards) to reduce the likelihood of similar instances in the future
- Ensure recommended changes are implemented

Continued Monitoring

Following resolution, the Incident Team should designate at least one team member to have responsibility for monitoring ongoing events and activity and for keeping a close watch on media sources.