ID Experts® Breach Services

Incident Response Plan (IRP)

Ownership

The material comprising this Incident Response Plan, including all text, graphics, charts, and other content; all modifications, improvements, or derivative works based on or derived from the same; and all copyright, trademark, and other intellectual property and proprietary rights associated therewith, is the sole and exclusive property of ID Experts, and all right, title, and interest in and to the foregoing are and shall remain ID Experts'.

Use Restrictions

You may use this Incident Response Plan solely for your internal business purposes. You may not distribute, transmit, sell, lease, loan, or otherwise transfer or provide, electronically, in print, or otherwise, this Incident Response Plan (or any modification, improvement, or derivative work of this Incident Response Plan), in whole or in part, to any individual outside your organization or to any other entity (whether or not affiliated with your organization) for any purpose whatsoever.

You may reproduce a reasonable number of copies of this Incident Response Plan for use by your employees for your internal business purposes only.

You may modify this Incident Response Plan by incorporating your information into the blank fields within this Incident Response Plan, by adding your own definitions, by revising the sample materials, or by making other similar changes to suit your business needs, but any modified version or derivative work of this Incident Response Plan will automatically be the sole and exclusive property of ID Experts.

Introduction

Purpose

This Incident Response Plan (IRP) is designed for your organization to execute when a privacy-related incident is reported. While each privacy-related incident has unique aspects, this plan gives the Incident Response Team (IRT) overall guidelines for its responsibilities and actions. The plan contains instructions, worksheets and sample materials that can be used by the Incident Response Team to streamline the response process.

Objectives

The Incident Response Plan will enable your organization to respond to most privacy-related incidents in an efficient and cost-effective manner that:

- Avoids or minimizes damage to individuals whose personal information may have been compromised
- Avoids or minimizes short and long-term business losses resulting from a privacy-related data breach
- Meets industry and regulatory requirements and avoids breach-related penalties
- Avoids or minimizes risk of class-action litigation resulting from a breach
- Avoids or minimizes risk of similar breaches in the future

IRP Requirements

The following requirements must be met to help ensure the effectiveness of the IRP:

- The IRP must be approved by executive management.
- Incident Response Team members must be trained in their IRP roles and responsibilities.
- The IRP must be tested and reviewed regularly.
- The IRP must cover all foreseeable data breach incidents/types.
- The IRP must outline how to assist managers, employees, clients, partners, vendors and customers in the event of a data breach.
- The IRP must also cover interactions with vendors, contractors and strategic partners.

Prerequisites

To mount an effective and timely response to a privacy-related incident, the following information and processes should be in place:

- An established process for reporting suspected privacy breach incidents, with immediate notice to the Incident Response Team leader and designated privacy/security officer
- A data breach risk assessment and a Personally Identifiable Information or Protected Health Information (PII/PHI) inventory
- On-going evaluation of risk management and data security monitoring programs

- Knowledge of applicable regulations

Overview of Incident Response Process

There are three potential phases in responding to a privacy-related incident, as shown in Figure 1.

Figure 1: The Incident Response Process

The three phases are typically executed as follows:

- **DISCOVERY** occurs whenever an incident is reported. During this phase, the Incident Response Team leader notifies the designated privacy/security officer and appropriate members of the executive team, then convenes the Core Incident Response Team (IRT) to quickly confirm the likelihood of an actionable data breach, as defined by in the breach policies and definitions section. (See Tab 2.) Your data breach services provider can refer you to additional needed resources, such as forensics experts. The Core IRT also takes whatever steps are necessary to try to contain the possible breach. If a breach can be ruled out, response may end here.

- **INVESTIGATION** occurs when the Discovery phase establishes the likelihood of an actionable data breach. During this phase, the Core Incident Response Team works with other IRT members as appropriate to investigate what Personally Identifiable Information or Protected Health Information (PII/PHI) was breached, evaluate the business and privacy risks associated with loss of that information, and plan a risk-appropriate response that protects the organization and the individuals whose information was breached and that complies with applicable regulations. This is the appropriate time to contact your data breach services provider to discuss the requirements for and advisability of notification, special notification needs, etc. Decisions about notification, remediation and other possible responses will also depend on your organization's culture and risk tolerance. If investigation establishes that there has been a breach of PII/PHI but that the risk does not justify further action, the incident response may end here.

- **RESPONSE** occurs when a data breach has occurred and is judged to require further response to protect the organization and/or the individuals whose personal information has been compromised. Certain types of response are required to ensure the organization complies with applicable regulations. Depending on the nature of the breach, response may include notification of the incident to individuals and agencies, identity protection services for individuals, legal action, public relations efforts, establishment of new security systems or processes to prevent future breaches, and other actions. Your data breach services provider can manage all elements of notification.

The exact details and actions taken in each phase depend upon your industry and the nature of the privacy-related incident. The rest of this document contains guidelines, worksheets and other materials for the Incident Response Plan.

Tab 1: Incident Response Team and Other Contacts

Overview

The Incident Response Team (IRT) typically operates under the authority of the Chief Information Officer (CIO), Chief Privacy Officer (CPO) or Chief Security Officer (CSO), or another executive operating in one of those roles. The team is responsible for all phases of response to a privacy-related incident. The team is divided into two bodies: the Core IRT, which handles immediate response ("triage") during the Discovery phase, and the Extended IRT, which includes the Core IRT plus team members from the various functional areas who may be involved during the Investigation and Response phases. (The Core team may call on other team members during Discovery as needed.)

To be successful, the IRT members must have the expertise and training to respond to and manage privacy-related incidents, they must have the full support of the executive team, and they must have access to relevant data, tools and incident reports.

Roles and Responsibilities

The overall responsibilities of the Incident Response Team are to:

- Identify the incident and what occurred
- Escalate issues to the executive team as required
- Provide training and guidance to staff who are involved in handling the incident
- Provide training and guidance to other internal employees as needed
- Manage or conduct investigation, evidence gathering and preservation of all documents and materials
- Manage and/or execute the incident response
- Assist law enforcement as appropriate or applicable
- Submit written progress reports to the executive team and other stakeholders regularly during the response process
- Recommend new systems, policies and procedures to avoid similar incidents in the future
- Submit a final incident report and recommendations and to conduct a debriefing with appropriate management and stakeholders, upon resolution of the breach incident
- Plan for implementation of recommendations and arrange for testing and on-going monitoring of new systems, polices and processes

The roles and responsibilities of the team members are outlined in Tables 1 and 2. The tables list the essential IRT members. Other experts and stakeholders may be brought on to the team, and outside experts will be called in, depending on the nature and severity of the incident.

Core IRT Member	Department	Role	Responsibilities
IRT Leader	Office of CSO/CPO/ CIO	Program manager for Incident Response Process	• Convenes team and chairs IRT meetings • Oversees the incident response process • Submits progress reports to executive staff and stakeholders • Submits final report and oversees debriefing • Tracks and reports on operations changes resulting from incident
Legal Representative	Office of Corporate Counsel	Legal advisor to the IRT and liaison to Corporate Counsel	• Provides information on privacy-related legislation that may affect incident response decisions • Provides information on major contracts and other obligations that may be relevant to the breach impact assessment • Oversees discovery and investigation from an evidentiary perspective • Recommends steps to mitigate legal liability in case of a data breach • Coordinates with internal and external legal teams as needed
Information Technology Representative	Office of CIO	IT advisor to the IRT and liaison to the IT organization	• Provides assistance in determining the existence, cause and extent of an IT-related incident (e.g., reviews firewall logs for correlating evidence of unauthorized access) • Coordinates with IT organization to stop or contain an IT-related breach (e.g., implements new firewall rules to close security holes) • Coordinates with IT organization to provide needed information during the Investigation phase • Coordinates with IT organization to plan and implement actions to prevent similar future incidents
Quality Assurance and Compliance Representative	Office of CCO/CSO/ CPO	Authority on privacy-related regulations and compliance requirements	• Provides information on privacy-related regulatory requirements • Oversees discovery and investigation from a compliance perspective • Recommends steps for compliance and to mitigate the risk of penalties • Oversees mandatory or discretionary reporting to

			government agencies and/or industry groups • Coordinates with legal representative

Table 1: Core IRT Team Roles and Responsibilities

Table 2: Extended IRT Roles and Responsibilities

Extended IRT Member	Department	Role	Responsibilities
Financial Representative	Office of the CFO	Financial risk analyst, liaison to Finance organization	• Helps evaluate financial liability and business risks related to a breach incident • Helps conduct cost/benefit analysis for breach response planning • Helps gain budget approval for response
Marketing Representative	Office of the CMO	Public relations advisor, liaison to Marketing organization	• Advises team on consumer privacy issues, and best privacy and breach response practices within industry and from other companies • Creates and/or maintains breach response PR procedures • If an actionable breach occurs, immediately notifies the Public Relations Director • Coordinates with the IRT, executive and legal team on the timing, content and method of notification • Prepares and issues press releases or statements, as needed
Customer Service/Sales Representative	Senior Executive of Sales	Customer and sales advocate, liaison to Sales and Customer Service organizations	• Advocates for customers, customer service and sales in incident response planning • Coordinates with customer service team and sales to prepare for customer response after notification and/or PR announcement • If a breach occurs due to problems with customer-facing systems or processes, works with IT, HR and other appropriate departments to plan and implement change to avoid future similar incidents
Human Resources Representative	Senior Executive of HR	Employment law advisor, employee advocate, and liaison to Human Resource organization	• Provides assistance in determining the existence, cause and extent of an employee data-related incident • If employee personal data is compromised, handles communications with business area managers and employees • If employee performance is a factor in the incident, works with appropriate managers and employees to

			correct performance or improve processes or training • If employee misconduct is a factor in the incident, works with appropriate HR and business managers, legal representatives and others to take appropriate employment action (e.g., termination of employment) and legal action

Sample Worksheets

See *Tab 9: Worksheet Templates* for worksheets to copy and fill out.

Core IRT Roles and Responsibilities Worksheet

Core IRT Contacts	Office Phone	Mobile Phone	Email
IRT Leader:			
Alternate:			
Legal Representative:			
Alternate:			
IT Representative:			
Alternate:			
QA and Compliance Representative:			
Alternate:			

Extended IRT Roles and Responsibilities Worksheet

Extended IRT Contacts	Office Phone	Mobile Phone	Email
Financial Representative:			
Alternate:			
Marketing Representative:			
Alternate:			
Customer Service/ Sales Representative:			
Alternate:			
HR Representative:			
Alternate:			

External IRT Contacts Worksheet

Outside experts selected to help the IRT as needed with Discovery, Investigation and Response.

External IRT Contacts	Name	Phone/Fax	Email
Data Breach Services Provider Contacts	ID Experts		
Public Relations Vendor Contacts			
IT Security Consultant Contacts			
Outside Legal Contacts			
Regulatory Agency Contacts			
Law Enforcement Contacts (if any)			

Third-party PII/PHI Contacts Worksheet

Key vendors and business partners with whom your organization shares PII/PHI, such as payment processors, marketing agencies, business partners or third-party service providers.

Third-party PII/PHI Contacts	Name	Phone/Fax	Email

Tab 2: Policies and Definitions

Definitions

The following definitions are used to determine whether a privacy-related incident or data breach has occurred.

Personally Identifiable Information

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity. Examples include but are not limited to: Name, Social Security number (SSN), date of birth, home address, home phone number, personal email address, financial information, fingerprint or other biometric identifiers, photographs or other images, medical and healthcare information, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, military identity and service record information, criminal history, any other personally identifying characteristics or codes, or any other combination of aforementioned data relating to a consumer, employee, member, client, patient or customer of your organization.

Personally Identifiable Information on Students

Under the Family Educational Rights and Privacy Act, (Authority: 20 U.S.C. 1232g(b)(4)(A)), the term "Personally Identifiable Information" includes, but is not limited to:

(a) The student's name;

(b) The name of the student's parent or other family members;

(c) The address of the student or student's family;

(d) A personal identifier, such as the student's Social Security number, student number, or biometric record;

(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Protected Health Information

The Health Insurance Portability and Accountability Act (HIPAA), 160.103, defines Protected Health Information as meaning individually identifiable health information that is:

- Transmitted by electronic media; or maintained in electronic media
- Transmitted or maintained in any other form or medium

Excluded from this definition are education records covered under the Family Educational Rights and Privacy Act, Sections of the Higher Education Act, and employment records held by a HIPAA-covered entity in its role as an employer.

Privacy-Related Data Breach

A privacy-related data breach is defined as unauthorized acquisition of data that compromises the security, confidentiality or integrity of PII or PHI maintained by your company.

*Data Breach Risk Matrix**

The following Matrix defines the degree of risk from a data breach and illustrates the corresponding steps your organization should take to contain and resolve the breach. Each of these steps is discussed in more detail elsewhere in this document.

> **LOW RISK:** A breach that is created by an unintentional encounter that causes Personally Identifiable Information (PII) to become available to an unintended party.
>
> Examples of such incidents could be a lost file or disk, an unintentional employee upload of information onto an external portal, misappropriation of data, etc. A breach may fall into the medium risk category initially, but when the lost or stolen item is returned and the forensics review ascertains that the data was not viewed and/or the potential for misuse is very low (but cannot be otherwise 100% ruled out), the breach could be re-categorized as low risk.
>
> **MEDIUM RISK:** A breach caused by a malicious act or the intentional theft of property for the primary goal of obtaining PII. There should be a reasonable suspicion that the intention of the thief is to use the information fraudulently.
>
> Examples of such incidents could be an employee that steals system information, a stolen laptop computer or disk containing PII, etc. Exceptions may include a forensics review which ascertains the risk the information was accessed is low, but due to the sensitive or unique nature of the information the population will perceive a much greater threat of misuse than in other incidences.
>
> **HIGH RISK:** Typically a breach in which actual victims of ID theft or fraud are the reason the event is discovered (i.e. the data breach event has resulted in misuse with an egregious intent).
>
> Examples of a high-risk data breach are malicious hacker attacks, malware-infested websites, unauthorized downloads, stolen disks, etc.

** Please note that this methodology will need to be based on your company's culture, security, resources and perceived risk. A stolen laptop may be a more critical threat in one company versus another.*

Data Breach Risk Matrix

Low Risk	Medium Risk	High Risk
Discovery	Discovery	Discovery
Investigation	Investigation	Investigation
Risk Assessment	Risk Assessment	Risk Assessment
Internal Response Plan	Internal Response Plan	Internal Response Plan

Documentation and Debriefing	Resources	Resources
Closure	Internal/External Notification	Internal/External Notification
	Compliance and Legal Requirements	Compliance and Legal Requirements
	Remediation	Legal Ramifications
	Documentation and Debriefing	Remediation
	Closure	Documentation and Debriefing
		Closure

Data Breach Policies

Developing a Policy

In developing a data breach policy for privacy-related data breaches, your organization must consider the following questions:

- What constitutes an actionable breach for your organization?
- What will you always do in case of breach?
- What do you never do in case of breach?
- What are the federal rules for data breach notification?
- What are the state rules for data breach notification?
- What are the deadlines and notification thresholds, if applicable?
- What are the applicable breach risks and classifications (IT system vs. physical loss or intrusion, customer vs. personnel data) and actions by class (i.e., in case employee data is compromised, include IRT member from HR)?

Breach policies should be kept short, with only the information required for corporate governance and compliance, leaving details of the Incident Response Process to the IRP.

Sample Breach Response Policy

In case of a privacy-related data breach, our Company shall execute the following procedures:

- **CONTAINMENT:** The first priority after a data breach is discovered is to contain the breach and notify supervisory personnel as quickly as possible. For any category of breach, the data must be secured, and the reasonable integrity, security and confidentiality of the data or data system must be restored.
- **CLASSIFICATION:** The Incident Response Team shall immediately take steps to determine the exact nature of the breach in terms of its extent and potential risk to persons whose data has been compromised and to our organization.
- **INTERNAL REPORTING OF AN INCIDENT OR BREACH:** As soon as a privacy-related incident has been identified, the employee who discovered it must take immediate steps to report the breach to his or her supervisor. The supervisor must take immediate action to notify the Incident Response Team leader, to determine the extent and cause of the incident, and to take such further action as is necessary to contain a breach or recover the missing data.
- **DOCUMENTATION:** The supervisor reporting an incident must document any breach, noting the categories of information involved, the scope of the breach, steps taken to contain the breach, and the names or categories of persons whose personal information was, or may have been, acquired by an unauthorized person. A copy of that documentation must be sent to Corporate Counsel.

  All members of the IRT must take care to document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation. (Note also that some vendors and business partners, such as Visa, have

specific procedures that must be followed for evidence preservation. These should be identified and documented as part of the plan.)

- **NOTIFICATION OF EXECUTIVE STAFF:** In all cases of where a breach is determined to have occurred, the full executive staff must be notified as soon as practicable.

- **NOTIFICATION TO VICTIMS:** Requirements, timing and forms of notification are all dependent upon constantly changing state and federal laws. The IRT should consult legal experts and the organization's data breach services provider for help in determining relevant statutes and notification requirements.

  - ***Time for Providing Notification.*** *Once the IRT and executive team have determined that notification is required, the Company shall notify affected individuals without unreasonable delay. However, notification may be delayed if law enforcement informs the Company that disclosure of the breach would impede a criminal investigation or jeopardize national or homeland security.*

  - ***Responsibility for Providing Notification.*** *The responsibility for providing notification shall lie with the IRT leader. The leader may delegate this responsibility, but should satisfy him- or herself that the proper notification has, in fact, occurred. A copy of the notification will also be provided to the COO, CMO and Vice President of Sales prior to the time it is posted or sent to affected individuals.*

  - ***Contents of the Notification.*** *Contents of the notification are dependent upon applicable statutes and regulations. At a minimum, notification shall be clear and conspicuous, and it shall describe the incident in general terms along with the type of information involved, the Company's actions, and contact information to receive further assistance.*

  - ***Method of Notification.*** *Notification to affected persons must be provided as determined by the IRT and in compliance with applicable state or federal statutes, unless substitute notification is permitted.*

  - ***Substitute Notification.*** *Acceptable substitute notification will be determined by applicable state or federal statutes.*

- **ADDITIONAL NOTIFICATION REQUIREMENTS:** Many state and federal laws require notification to the state Attorney General's office as well as other agencies.

Tab 3: PII/PHI Inventory and Risk Assessment

If you have an inventory of your privacy-related data assets, a classification using established risk-based models and/or a Privacy and Information Risk Assessment report, include them here. These are invaluable in evaluating the severity of and planning a response to a privacy-related incident. We recommend keeping a copy of these reports in each team member's IRP binder.

Tab 4: Phase 1 — Discovery

Discovery begins when a possible privacy-related incident is reported. The objectives of this phase are to:

- Notify appropriate members of the executive team that there has been a possible incident.
- Investigate and assess to confirm or rule out the existence of a privacy-related data breach, and engage forensics experts as needed. The data breach risk matrix found in Tab 2: Policies and Definitions can help the IRT properly assess the level of risk to affected individuals based upon the nature of the data breach.
- Contain the breach, if needed, and insofar as possible.
- If credit cardholder data is involved, follow bankcard company requirements. (Bankcard companies, specifically Visa and MasterCard, have detailed requirements for reporting security incidents and the suspected or confirmed compromise of cardholder data. Reporting is typically required within 24 hours of compromise.)
- Report findings to the designated privacy/security officer and the executive team for approval to close the incident or move on to the next phase

Discovery and Assessment Process

The Core IRT is responsible for the Discovery phase, working with the business area reporting the incident, and bringing in other experts as needed.

The IRT needs to answer the following questions to complete the Discovery phase. A Discovery Questionnaire template is in *Tab 9: Worksheet Templates*.

Sample Discovery Questionnaire

Discovery Questionnaire	
Incident Number:	
What happened?	Where did the incident take place?
	Who was involved?
	What information was lost (customer data, employee data, consumer data, corporate financials or intellectual property, etc.)?
	How was the information lost or compromised (lost or misplaced, stolen printed documents or digital media, system failure, hacking or malicious attack on IT systems, or other)?
	At exactly what time and where was the incident discovered?
	How was the incident documented?
	Has law enforcement been notified?
	What has been done so far to contain the incident and/or mitigate risks?
Scope of the incident?	How much information was lost (# of records, extent of personal information, etc.)?

	Is the data accessible (i.e., is it encrypted, de-identified, etc.)?
	How many individuals could be affected?
	How could the data be used for malicious purposes?
	Has the incident been leaked and to whom (media, customer base, employees, vendors, etc.)?
What is the potential impact?	What is the potential financial impact to the organization?
	What is the potential financial or personal impact to the persons whose data has been compromised?
	What is the potential media/public relations impact to the organization?
	What is the potential legal impact to the organization?
	What is the potential regulatory impact to the organization?

If the initial discovery efforts indicate that PII/PHI has been compromised or lost, or that there may be significant negative impact to the organization and/or the persons whose data has been compromised, the incident should move to the Investigation stage. It is not necessary to determine at this point what other specific actions are needed. The IRT need only establish that action is warranted and that further investigation and assessment are advisable.

In either case, the IRT should prepare a report with its findings and recommendations, then archive or retain any incident-related reports and other documentation in accordance with company policy. The role of the IT department is especially critical in discovering and containing the source of the breach. An IT checklist for breach discovery, containment and documentation can be found in Tab 8: Reference Materials. The IRT leader, in consultation with the designated privacy/security officer and appropriate members of the executive team, can then make a final determination whether to move ahead with the Investigation phase or to consider the incident closed.

Sample Privacy Incident Report

See *Tab 9: Worksheet Templates* for a Privacy Incident Report to copy and fill out.

Privacy Incident Report	
Incident Number:	
Incident Description	Time reported:
	Time discovered:
	Time of incident:
	Place of incident:
	Personnel involved:
	Type and amount of personal information involved:
	Accessibility/vulnerability of information (encryption, etc.):
	Cause of incident:
	Potential privacy breach (Yes/No):
	Awareness of incident (who knows about it now):
Initial Risk Assessment	Number of individuals potentially affected:
	Risk to individuals (types and extents):
	Financial risk to organization:
	Legal/contractual risk to organization:
	Regulatory risk to organization:
	Public relations risk to organization:
Steps Taken	Data loss containment:
	Incident documentation:
	Law enforcement contacted:
	Data breach services provider contacted:
	Agencies notified:
Recommendations	Close or move to Investigation phase and why
	Immediate notification requirements
	Priorities and considerations for further investigation

Tab 5: Phase 2 — Investigation

During the Investigation phase, the IRT will conduct an in-depth investigation and assessment to determine what further actions need to be taken.

At the end of the Investigation phase, the IRT should prepare a report with its findings and recommendations. The IRT leader, in consultation with the designated privacy/security officer and appropriate members of the executive team, can then decide what responses the organization will implement in the next phase.

Forensics/Containment

During this phase, the IRT needs to conduct in-depth investigation to confirm that any breach has been fully contained and to determine the steps necessary to help prevent similar incidents in the future. This investigation will be conducted by a subset of the IRT and other contacts. The makeup of this team will be determined by the cause and nature of the incident, but it will typically consist of some combination of:

- The IRT leader, representing the designated privacy/security officer
- The IT representative
- The HR representative
- A representative from the business area where the incident occurred
- Outside forensics consultant, if needed

This team will investigate to determine:

- The exact circumstances and causes of the data breach or loss
- Whether the data breach or loss has been stopped to the full extent possible
- What system, process or personnel changes are necessary or advisable to help prevent similar incidents in the future

Depending on the nature of the incident, the forensics and prevention team may:

- Coordinate with the Legal representative on evidence-gathering
- Conduct forensic analysis on computer systems, databases, IT maintenance logs, backups, system audits, etc., looking for inconsistencies, improper security settings and evidence of unauthorized access
- Review facilities records to determine who had physical access to the data
- Review business, personnel and security processes and records to identify weaknesses that might have contributed to the incident
- Implement any system changes needed to fully contain a breach
- Outline and make recommendations on system, personnel, business and security process changes needed to help prevent similar incidents in the future

Legal

The Legal representative on the IRT is responsible for investigating the legal ramifications and risks of a privacy-related incident and formulating a plan to mitigate those risks. The Legal representative will likely work closely with:

- The Quality Assurance and Compliance representative
- The Finance representative
- Law enforcement contacts
- The IT representative

The Legal investigation and assessment needs to determine:

- Are the possible legal liabilities from this incident such that further evidence gathering or other action is advisable?
- Are there regulatory or contractual obligations to notify any customers, vendors or business partners of this incident?
- Are there any known contractual obligations to provide remediation in this case?
- Are there other actions required by existing contractual obligations?

If the Legal representative and other team members determine that there are legal risks from the incident, they will:

- Work with business areas to locate and evaluate all evidence pertinent to the incident
- Document and securely store evidence gathered during the investigation, working with IT and business areas to ensure that clear chain-of-custody is established and preserved for physical and electronic evidence
- Create an itemized inventory of evidence
- Be present in all meetings with law enforcement
- Coordinate with law enforcement and other business areas on evidence gathering, notification, etc.
- Outline and make recommendations on notifications and remediation required to meet contractual obligations
- Outline and make recommendations on notifications and remediation required by law
- Outline and make recommendations, including cost/benefit analysis, on notifications and remediation required to mitigate business risks
- Make legal recommendations on public and private communications about the incident
- Work with the data breach services provider to plan for complete records of notification and remediation for individuals affected by a data breach

Besides legal ramifications, assessment of the incident should include other factors, such as a company's reputation and customer retention. The risk of losing existing (and potential) customers or of being perceived as negligent may require a response plan that goes beyond meeting legal requirements.

Sample Investigative Report and Recommendations

See *Tab 9: Worksheet Templates* for an Investigative Report to copy and fill out.

Privacy Incident Investigative Report and Recommendations	
Incident Number:	
Incident Summary	What, when, where, who was involved:
Forensic Findings	Cause(s), contributing factors, etc.:
Risk Summary	Risks to organization (types and extents):
	Risk to individuals (types and extents):
Recommendations (Including Cost/Benefit Analyses)	Notification:
	Remediation:
	Legal action:
	Publicity:
	Personnel action:
	Prevention (system and process changes):

Tab 6: Phase 3 — Response

During the Response phase, the IRT will execute those recommendations selected by the executive staff upon review of the Investigation phase report. The IRT will, in some cases, be directly responsible for execution, and in other cases they will oversee and track actions taken by other staff and/or outside vendors. For example, an organization typically contracts with an outside data breach services provider to manage the notification process because of large call volumes, risk of error, constantly changing laws, data security and retention issues and other special requirements.

The objectives of this phase are to:

- Execute approved recommendations from the investigation report, including notification and remediation, public relations efforts, legal and law enforcement efforts, personnel actions, and system and process changes to help prevent similar incidents in future
- Resolve any issues that arise during implementation
- Track implementation and report status to the executive staff
- Document responses and securely archive documentation
- Upon completion, report to the designated privacy/security officer and executive team and request approval to close the incident

Response Project Plan

The Incident Response implementation should be managed like any other multi-department business project, using whatever project planning methods and tools are available and familiar to staff.

Notification

Investigation and assessment of notification needs are the responsibility of a subset of the IRT, consisting of:

- The QA and Compliance representative
- The Legal representative
- The Finance representative
- The Marketing representative
- The Customer Service/Sales representative

This team will work in consultation with the data breach services provider, the public relations vendor and any regulatory agency contacts.

Notification may be required under contractual commitments, applicable laws or regulations, or to avoid harm to the organization and/or the individuals whose data was compromised. The notification assessment needs to fully investigate the extent and risks of the data loss to determine:

- Is there potential risk to individuals affected by the breach that can be mitigated through notification?
- Is there a possible regulatory requirement to notify the individuals whose data was lost or compromised?

- Is there a possible regulatory requirement to notify government or other agencies of a data breach?
- Are the estimated business or public relations impacts such that notification may be advisable to prevent damage to our business or brand?
- Would notification help to mitigate our legal liability for the data breach?

If the team determines that notification is required or advisable, they will make recommendations outlining:

- Groups of individuals who should be notified
- Agencies to notify, agency contacts, required information and deadlines for notification
- State Attorneys General to be notified
- Timing of notification, to protect individuals and meet legal and regulatory requirements while not interfering with any law enforcement investigation
- Recommended form(s) of notification (email, phone, letter, website, etc.)
- Any special notification needs (persons with disabilities, minors, military personnel on active duty, etc.)
- Recommended resources for assistance after notification (call center assistance, etc.)

The forms of notification required will vary by situation, but standard best practices include the following components:

- Website to enroll victims in credit monitoring or other remediation services, educate consumers about identity theft and provide contact information
- Call center to enroll victims in credit monitoring or other remediation services, and to address questions or concerns consumers may have regarding the incident or protection of their personal information
- Letter to notify breach victims about the incident, inform them about preventative and remediation services and direct them to public resources for monitoring their credit. In some circumstances an email may be an acceptable alternative to a written letter. The following sample letter is for information only. No single letter can comply with every state and federal regulation; check the laws that pertain to your particular situation when creating your letter. Your data breach services provider stays up-to-date with each state's requirements and can assist you.

[Name]
[Address]
[City, State Zip]

To enroll, please call:
1-800-555-555 or visit:
www.example.com

Your access code:
[insert access code]

Dear [Name],

We recently learned that [describe incident here].

[Client] has discovered that [incident details/loss details] (Example: a group of files containing names and Social Security numbers was inadvertently disclosed on a web server.) We regret to inform you that you have been identified as one of the individuals whose personal data was included in those files.

Preliminary investigation indicates that some of your personal information, including your name, address and Social Security number may have been compromised. [Make revisions here as necessary.]

The information was removed immediately upon discovery, and at this time, there is no evidence to suggest that there has been any attempt to misuse any of your personal information; yet there is always some risk.

[Client] has contracted with ID Experts® to provide you with a comprehensive membership to help protect your identity. With this protection, ID Experts will help you resolve issues if your identity is compromised. **We strongly encourage you to register for this free identity theft protection service by calling [TFN] or going to [URL].**

Please note the deadline to enroll is: [Enrollment deadline]

Your one-year membership will include the following:

- **Fraud Resolution Representatives:** ID Experts will provide assistance if you suspect that your personal information is being misused. A recovery advocate will be assigned to your case, and they will work with you to assess, stop and reverse any fraudulent activity. If you suspect or discover suspicious activity, you should contact them immediately for assistance.
- **Credit Monitoring:** ID Experts will provide 12 months of credit monitoring that gives you unlimited access to your TransUnion credit report and score and will notify you by email of key changes in your TransUnion credit report. Credit monitoring is included as part of your ID Experts membership, but you must activate it for it to be effective. Detailed instructions for activating your credit monitoring are provided on the ID Experts member website which you may log into once you enroll.
- **Exclusive Educational Materials:** The ID Experts website includes a wealth of useful information, including instructive articles, a Protection Test that you can take, their very helpful ID Self-Defense Academy™ and a place where you can review and update your account. Their experts will keep you up-to-date on new identity theft scams, tips for protection, legislative updates and other topics associated with maintaining the health of your identity.
- **Insurance Reimbursement:** ID Experts will arrange $30,000 of identity theft reimbursements for certain expenses that can be incurred when resolving an identity theft situation.

To learn more about these services and to ensure the safety of your personal information, we strongly encourage you to call ID Experts at [TFN]. Alternatively, you can learn more about the incident and enroll in the services at [URL].

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. Representatives from ID Experts are available to assist with enrollment in the program Monday through Friday from 6 am-6 pm (PST) by calling [TFN]. They can also address any questions or concerns you may have regarding protection of your personal information.

You will find additional instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the following access code when calling or enrolling on the website, so please do not discard this letter.

Your Access Code: [Insert access code]

We sincerely regret any inconvenience or concern that this matter may have caused you. Thank you for your patience and understanding while we work together to protect your good name.

Yours truly,

[Name]
[Company]

Remediation

Investigation and assessment of remediation needs such as credit or identity monitoring and restoration for breach victims are the responsibility of a subset of the IRT, consisting of:

- The Legal representative
- The QA and Compliance representative
- The Finance representative
- The Marketing representative
- The Customer Service/Sales representative

This team will work in close consultation with the executive team, data breach services provider and the public relations vendor.

Remediation may be required under contractual commitments or to avoid harm to the organization and/or the individuals whose data was compromised. The notification assessment needs to fully investigate the extent and risks of the data loss to determine:

- Is it possible that persons or organizations whose information was compromised will be damaged by this data breach or loss?
- Are the estimated possible damages to those individuals or organizations or to our organization such that remediation measures may be advisable?
- Are there remediation measures available to protect or restore the identities of people whose personal information was lost or compromised?
- Are there any known contractual obligations or legal or regulatory requirements to provide remediation in this case?

The data breach risk matrix found in *Tab 2: Policies and Definitions* can help the IRT determine the appropriate level of remediation services, such as credit or identity monitoring or fully managed recovery of stolen identity, to provide to the breach population.

Sample Incident Closure Report

See *Tab 9: Worksheet Templates* for an Incident Closure Report to copy and fill out.

Incident Closure Report	
Incident Number:	
Incident Summary	Summary of incident, actions taken and completed:
Legal Mitigation	Partners and agencies notified:
	Contractual obligations fulfilled:
	Regulatory obligations fulfilled:
	Documentation archived:
	Other actions:
Notification	Groups notified (types of notification, % contacted and other stats):
	Public/media notification:
	Summary of response:
Remediation	Program(s) offered, % enrollment, etc.:
	Remediation provided (number and type of incidents, actions taken, resolution to date):
Prevention	System changes:
	Process changes:
Follow-up	Actions remaining:
	Plan for monitoring and assessment (of process changes, etc.):
Recommendation to Close	Criteria to consider the incident resolved:
Reviewed By:	___ IT Department ___ Designated privacy/security officer ___ Other

Tab 7: Incident Response Scenarios

The scenarios below depict typical privacy-related incidents and how the Incident Response Process might be used in each case.

Scenario 1: Misplaced Laptop, Low Risk

Summary	An employee reports that their laptop computer has been misplaced at their place of residence. The laptop is found within 24 hours.
Discovery	• Employee alerts their manager immediately, who escalates to the department head, notifies IT and follows procedural steps. • The employee, employee's manager and IRT meet to review, discuss implications and discuss project plan. • The IRT meets with IT to discuss the impact of what may have been compromised. IT explains that if the laptop is fully powered off when lost or stolen, all information on the drive (account information, documents, etc.) are fully encrypted, so it is reasonably certain that a thief could not view the data. • The IRT meets to discuss findings, implications and a plan to move forward. They decide that if the laptop is not found within 24 hours, it will be considered lost, and the IRT will meet to pull in additional resources and discuss next steps. • Laptop is found.
Investigation	n/a
Response	HR and IT review laptop security procedures with the employee.
Closure	The IRT has a final meeting to document resolution and close the incident.

Scenario 2: Attempted Unauthorized System Access, Medium/High Risk

Summary	Employee A, without authorized access, attempts to crack into the accounting system to review company payroll and salary information. Employee A confides in Employee B regarding the attempt. Employee B goes to management with the information.
Discovery	• Employee B alerts their manager immediately, who escalates to the department head, notifies IT and follows procedural steps. • Employee A's manager and the IRT meet to review and discuss implications and malicious intent.
Investigation	• IRT meets with IT to discuss the impact of what could or may have been compromised: – *Was the system accessed, reviewed, deleted?* – *How many attempts were made, successful vs. unsuccessful?* – *Impact on departments and employees* – *Impact on the company* • Employee's manager and HR manager meet with the employee to discuss incident

	and disciplinary action: – *Review incident and specifics* – *Malicious intent* – *Disciplinary action* • IT removes the employee's accounts and access privileges to contain a possible breach. • The IRT meets to review findings, actions taken and status: – *Incident and implications* – *What was viewed or potentially viewed* – *Determine risk* – *IRT meets with data breach services provider to develop response plan:* – *Who needs to be notified: employees, managers, legal or law enforcement* – *Fully document all procedures, deadlines and owner of each* • The IRT meets with executive management to review incident report.
Response	• IRT takes precautionary and necessary steps, under executive management's guidance, to carry out plan of action as indicated above. • Data breach services provider conducts notification and follow-up. • IRT debriefs with executive management and recommends closure.
Closure	The IRT has a final meeting to document resolution and close the incident.

Scenario 3: Misplaced Physical Record, Medium/High Risk

Summary	Janitorial service finds a printed resume and job application on an internal company printer. The applicant's name, date of birth and Social Security number are documented on the forms. The resume and job application are returned the following day, but it is not possible to determine if the material was copied.
Discovery	• The employee who forgot the materials on the printer alerts their manager as soon as they realize the exposure. • Employee, employee's manager and IRT meet immediately to review specifics of incident.
Investigation	• IRT holds a meeting with the janitorial service to investigate what they did with the material, if it was photocopied and/or written down. • IRT meets to discuss the individual incident, risks to this individual and company, implications and create project plan to move forward: – *Review specifics* – *Was this malicious?* – *Did employee follow protocol and policies?* – *Whom to notify*

	– *Collaborate plan and operational steps (whether to manage the breach internally or seek outside partners)* – *Determine potential budget* – *Alert legal counsel* – *Contact law enforcement in case of potential lawsuit* • IRT reviews findings and recommendations with the executive team.
Response	• HR contacts the victim applicant to advise of the situation, confirm their information has not been misused, and provide a 2-5 year identity protection full-service offering. • IRT notifies the janitorial services of what has taken place. • HR manager and business manager meet with the janitorial employee to discuss security procedures and take corrective action, if necessary. • IRT leader, the designated privacy/security officer, HR and Legal departments meet to re-review company policy and procedure around PII and evaluate for needed changes. • Legal representative securely archives documentation around the incident, investigation and actions. • IRT debriefs with executive management and recommends closure.
Closure	The IRT has a final meeting to document resolution and close the incident.

Scenario 4: Laptop Stolen During Off-site Meeting, High Risk

Summary	Laptop is stolen during an off-site meeting. Employee notices the theft immediately.
Discovery	• The employee alerts their manager of the theft immediately. • Manager escalates to the department head, who notifies IT and follows procedural steps. • Employee, employee's manager and IRT meet immediately to review specifics of incident.
Investigation	• IRT meets immediately to review specifics and discuss plan. • To mitigate risk: – *IT has employee change their domain password.* – *IT has employee change their VPN account password.* – *IT will monitor user's account to report any suspicious activity.* • IRT meets immediately with IT to discuss the impact of what may have been compromised and the population that could have been affected: – *If the laptop is powered on or in stand by then there is a greater risk for stolen information and account compromise.* – *IT begins investigation to identify any data records, logs and electronic files that could have been compromised.* – *IT will work to wipe the drive remotely if the system or Internet access is*

	compromised. • IRT meets to discuss the individual incident, risks to this individual and company, implications and plans to move forward: – *Review specifics* – *Was this malicious?* – *Did employee follow protocol and policies?* – *Whom to notify* – *Is public disclosure advisable?* – *Alert legal counsel* – *IRT meets with data breach services provider to develop response plan:* – *Determine which state Attorneys General need to be notified. (The IRT will have current information surrounding laws and timeframes. Consider deadlines and ramifications for late notifications.)* – *Who else needs to be notified: employees, managers, legal or law enforcement?* – *Determine potential budget.* – *Fully document all procedures, deadlines and owner of each.* • IRT meets with the executive team to discuss breach, risks, implications and project plan to move forward.

Response	• IRT meet to pull in resources, discuss specifics and needs. • IRT and forensic resources finalize any and all PII audit of who was affected and needs to be notified and possibly provided with remediation. • IRT oversees notification and remediation efforts. • IRT leader, the designated privacy/security officer, HR and Legal departments meet to re-review company policy and procedure around PII and evaluate for needed changes. • Legal representative securely archives documentation around the incident, investigation and actions. • IRT debriefs with executive management and recommends closure.
Closure	The IRT has a final meeting to document resolution and close the incident.

Scenario 5: Unauthorized, Malicious Access to HR Records, High Risk

Summary	Human Resources (HR) file drawer was broken into during non-business hours. The suspect used a key entrance to gain entrance into the office building, and the HR office was unlocked. Only the building manager and janitorial service have keys to enter the building; any additional access is via key card. Both key and card entrances and exits are tracked and logged.
Discovery	• HR employee who discovers break-in alerts their manager, IRT and executive management immediately, as this is a clear security breach. • Core IRT contacts law enforcement immediately as this is an immediate security concern (obtain a copy of police report for records). The specifics below will also need to be addressed with law enforcement. • IRT confirms with the building manager who entered the office between the specific hours in question. Security reports that only the janitorial service was in the company office during the hours when the incident occurred. • With forensics and law enforcement, IRT cross-references the suspects' access and timeframes. • IRT reports initial findings to executive team and proceeds immediately to full investigation.

Investigation	• IRT meets immediately to review specifics and discuss plan. IRT proceeds only under advisement from law enforcement as this is a company security breach and prosecutable by law. • Under advisement from law enforcement, IRT proceeds to: – *Contact janitorial service to report incident and file immediate complaint. (Law enforcement may also contact the janitorial service.)* – *Obtain name of all janitors with clearance* – *Obtain history and background of suspected janitor(s)* – *Obtain janitor(s) address and phone number* – *Remove security clearance for janitorial service* – *Contact legal counsel with specifics* – *Law enforcement may also contact the janitorial service* • IRT provides all relayed and documented information to law enforcement. • HR representative and IRT meet immediately, probably with law enforcement input, to review specifics: – *What was broken into?* – *Was this a successful attempt?* – *First attempt or are previous concerns warranted?* – *Was the file drawer locked, security in place?* – *What was compromised?* – *What was not compromised?* – *Background of janitorial service* – *Background of the suspected janitor(s)* – *Discuss proposed and immediate ramifications of janitorial service* – *How to protect security of employees and the company* • IRT meets immediately with the executive team to review specifics, risks, implications and project plan to move forward: – *Review specifics* – *Whom to notify?* – *Collaborate on plan and operational steps (whether to manage the breach internally or seek outside partners)* – *Determine potential budget* – *Is public disclosure advisable?* – *Further legal and law enforcement actions*

Response	• IRT immediately moves forward with operational steps and plan, pulling in additional resources as needed. • IRT and forensic resources finalize any and all PII audit of who was affected and needs to be notified and possibly provided with remediation. • IRT oversees notification and remediation efforts. • IRT and data breach services provider, if any, determine which state Attorneys General and/or federal agencies need to be notified. • The IRT will have current information surrounding laws and timeframes. • Consider deadlines and ramifications for late notifications. • IRT leader, the designated privacy/security officer, HR and Legal departments meet to re-review company policy, security measures and procedures around PII and evaluate for needed changes. • Legal representative securely archives documentation around the incident, investigation and actions. • IRT debriefs with executive management and recommends closure.
Closure	The IRT has a final meeting to document resolution and close the incident.

Tab 8: Reference Materials

Regulatory References

A company's privacy and data breach responses may be guided by the policies and procedures in this IRP, and by the requirements imposed by the following business and industry regulations, as well as state laws. Note that the laws governing privacy-related breaches are constantly changing and may conflict with one another. The IRT should consult legal and compliance experts, including its data breach services provider, in deciding how to respond to any privacy-related incident.

Gramm-Leach-Bliley Act (GLBA)

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," including banks, securities firms and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities.

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, which receive such information.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information, including prevention, detection and response to attacks, intrusions or other system failures. Specific requirements include maintaining up-to-date and appropriate programs and controls by following a written contingency plan to address any breaches of nonpublic personal information and notify customers if their personal information is subject to loss, damage or unauthorized access.

Fair and Accurate Credit Transactions Act (FACTA) and the Red Flag Rules

Under the terms of the Red Flag Rule of FACTA, virtually every U.S. business larger than a sole proprietorship is required to have a program in place to prevent and mitigate the effects of identity theft.

According to the Federal Trade Commission:

"The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The rule goes into effect on November 1, 2009, and requires businesses to provide for the identification, detection, and response to patterns, practices, or specific activities—known as 'red flags'—that could indicate identity theft.

"Under the Red Flags Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs —or 'red flags'—of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to

update the program. The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers."[1]

Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HITECH Act

The primary focus of HIPAA was to improve the health insurance accessibility for people changing employers or leaving the workforce. The HIPAA Security Standards require a covered entity to implement policies and procedures to ensure:

- The confidentiality, integrity and availability of all electronic Protected Health Information (see definition in *Tab 2: Policies and Definitions*)
- Protection against any reasonably anticipated threats or hazards to the security of such information
- Protection against any reasonably anticipated uses or disclosures that are not permitted

Within this context, HIPAA requires a covered entity (CE) to implement policies and procedures to address security incidents. A security incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Response and reporting implementation requirements include identifying and responding to suspected or known security incidents; mitigating, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and documenting security incidents and their outcomes.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act (ARRA), signed in February 2009, seeks to streamline healthcare and reduce costs through the use of health information technology. The Act clarifies and extends the HIPAA privacy requirements. Under the HITECH Act, obligation to notify after a data breach is much broader than under HIPAA and applies to all breaches that are discovered on or after September 23, 2009.

- HIPAA-covered entities must provide notification within 60 days when PHI in any form or medium is breached, not just electronic records.
- The HITECH rules clarify that a breach is officially discovered on "the first day it is known to the HIPAA-covered entity or business associate or should reasonably have been known."
- Notification requirements are specific in terms of content, timing and obligations to ensure contact with affected individuals, and there is an imposed burden of proof on the HIPPA-covered entity that suffered the breach to demonstrate that all required notifications were made, and that telephone notifications were made in urgent situations.
- If a business associate experiences a breach, it has the same notification requirements and burden of proof as a CE, plus it must notify the covered identity whose information was breached.
- Should a breach impact more than 500 individuals, the CE is required to provide "immediate" notice to the Secretary of the Department of Health and Human Services (HHS), making the breach notice public.
- Additionally, if 500 or more individuals are affected in a single state or jurisdiction, notice must be provided to prominent media outlets.

1. Source: FTC Business Alert:" New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft." http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

- In cases of less than 500 individual records, the entity must maintain a log of such breaches and submit the log annually to the Secretary of the Department of HHS, which will publish the information on a public website.

- Public disclosure obligation can be required even at a much lower threshold than previously. For example, if 10 or more individuals affected by the breach have out-of-date contact information, the CE must post a notice on its website and in major print or broadcast media in geographic areas where the individuals are likely to reside.

- Under HIPAA, CEs were required to be in compliance with current federal and state laws regarding data security, but they were not actively audited, and there was no defined penalty structure for companies that had neglectful privacy practices. Under the HITECH Act, the Secretary of the Department of Health and Human Services (HHS) is directed to conduct periodic audits to ensure compliance within the first 12 months after enactment of the new rules. There is an increased, tiered penalty structure, with maximum fines ranging from $25,000 to $1.5M, and penalties are mandatory for cases of "willful neglect."

- HITECH provides explicit authority for state Attorneys General to enforce HIPAA rules and to pursue HIPAA criminal cases against CEs, employees of CEs or their business associates.

State Civil Codes

<Include text of relevant statutes in states and jurisdictions where your company conducts business.>

There are at least 110 state laws covering privacy-related data breaches. Each law is different, and the complexity of complying with multiple statutes requires expertise and careful attention to your organization's risk profile and business goals. Your data breach services provider is current on state laws and can help you comply with them.

Checklists for Discovery and Breach Containment

The following steps will help IT contain the breach, while gathering and preserving data for the Investigation phase.

IT Checklist

- Determine where and how the breach occurred. Note:
  - ***Do not*** *access or alter the compromised system.*
  - ***Do not*** *turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).*
- Determine if an intruder has exported or deleted any personal information data.
- Review the network to identify all compromised or affected systems. Consider e-commerce third- party connections, the internal corporate network, test and production environments, virtual private networks and modem connections. Look at appropriate system and audit logs for each type of system affected.
- Document all Internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.
- Take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third-party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.

  - *Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.*
  - *Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the corporate wireless network.*

- Monitor systems and the network for signs of continued intruder access.
- Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed.

Documentation Checklist

- Keep the initial incident report and all computer logs, email, and other data relating to the incident.
- Archive the final report, an annotated evidence list and all other incident-related data in secure storage.
- Give copies of all documentation to the Legal department.

Credit Card Processors Procedures

<Include your own copy of relevant procedures here.>

Additional References

- American Institute of Certified Public Accountants, Inc. Privacy Incident Response Plan. (2004).
- Johns Hopkins HIPAA Office. Personal Information Theft Events, Procedures for Providers and Health Plans. 1-6. (2007)
- Family Educational Rights and Privacy Act (FERPA) regulations and guidelines http://www.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf and http://www.ed.gov/policy/gen/guid/fpco/pdf/ht12-17-08-att.pdf
- Payment Card Industry (PCI) Data Security Standards (DSS) https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- PrivaWorks (2006) Version 4.0

Tab 9: Worksheet Templates

Incident Response Team and Other Contacts Worksheets

Core IRT Roles and Responsibilities Worksheet

Core IRT Contacts	Office Phone	Mobile Phone	Email
IRT Leader:			
Alternate:			
Legal Representative:			
Alternate:			
IT Representative:			
Alternate:			
QA and Compliance Representative:			
Alternate:			

Extended IRT Roles and Responsibilities Worksheet

Extended IRT Contacts	Office Phone	Mobile Phone	Email
Financial Representative:			
Alternate:			
Marketing Representative:			
Alternate:			
Customer Service/ Sales Representative:			
Alternate:			
HR Representative:			
Alternate:			

External IRT Contacts Worksheet

External IRT Contacts	Name	Phone/Fax	Email
Data Breach Services Provider Contacts	ID Experts		
Public Relations Vendor Contacts			
IT Security Consultant Contacts			
Outside Legal Contacts			
Regulatory Agency Contacts			
Law Enforcement Contacts (if any)			

Third-party PII/PHI Contacts Worksheet

Third-party PII/PHI Contacts	Name	Phone/Fax	Email

Phase 1 — Discovery Worksheets

Discovery Questionnaire	
Incident Number:	
What happened?	Where did the incident take place?
	Who was involved?
	What information was lost (customer data, employee data, consumer data, corporate financials or intellectual property, etc.)?
	How was the information lost or compromised (lost or misplaced, stolen printed documents or digital media, system failure, hacking or malicious attack on IT systems, or other)?
	At exactly what time and where was the incident discovered?
	How was the incident documented?
	Has law enforcement been notified?
	What has been done so far to contain the incident and/or mitigate risks?
Scope of the incident?	How much information was lost (# of records, extent of personal information, etc.)?
	Is the data accessible (i.e., is it encrypted, de-identified, etc.)?
	How many individuals could be affected?
	How could the data be used for malicious purposes?
	Has the incident been leaked and to whom (media, customer base, employees, vendors, etc.)?
What is the potential impact?	What is the potential financial impact to the organization?
	What is the potential financial or personal impact to the persons whose data has been compromised?
	What is the potential media/public relations impact to the organization?
	What is the potential legal impact to the organization?
	What is the potential regulatory impact to the organization?

Privacy Incident Report	
Incident Number:	
Incident Description	Time reported:
	Time discovered:
	Time of incident:
	Place of incident:
	Personnel involved:
	Type and amount of personal information involved:
	Accessibility/vulnerability of information (encryption, etc.):
	Cause of incident:
	Potential privacy breach (Yes/No):
	Awareness of incident (who knows about it now):
Initial Risk Assessment	Number of individuals potentially affected:
	Risk to individuals (types and extents):
	Financial risk to organization:
	Legal/contractual risk to organization:
	Regulatory risk to organization:
	Public relations risk to organization:
Steps Taken	Data loss containment:
	Incident documentation:
	Law enforcement contacted:
	Notification/remediation vendor contacted:
	Agencies notified:
Recommendations	Close or move to Investigation phase and why
	Immediate notification requirements
	Priorities and considerations for further investigation

Phase 2 — Investigation Worksheet

Privacy Incident Investigative Report and Recommendations	
Incident Number:	
Incident Summary	What, when, where, who was involved:
Forensic Findings	Cause(s), contributing factors, etc.:
Risk Summary	Risks to organization (types and extents):
	Risk to individuals (types and extents):
Recommendations (Including Cost/Benefit Analyses)	Notification:
	Remediation:
	Legal action:
	Publicity:
	Personnel action:
	Prevention (system and process changes):

Phase 3 — Response Worksheet

Incident Closure Report	
Incident Number:	
Incident Summary	Summary of incident, actions taken and completed:
Legal Mitigation	Partners and agencies notified:
	Contractual obligations fulfilled:
	Regulatory obligations fulfilled:
	Documentation archived:
	Other actions:
Notification	Groups notified (types of notification, % contacted and other stats):
	Public/media notification:
	Summary of response:
Remediation	Program(s) offered, % enrollment, etc.:
	Remediation provided (number and type of incidents, actions taken, resolution to date):
Prevention	System changes:
	Process changes:
Follow-up	Actions remaining:
	Plan for monitoring and assessment (of process changes, etc.):
Recommendation to Close	Criteria to consider the incident resolved:
Reviewed By:	___ IT Department ___ Designated privacy/security officer ___ Other

About ID Experts®

ID Experts provides data breach solutions, risk assessment, forensic investigation and fully managed victim identity restoration to corporations, financial institutions, healthcare organizations and government agencies. As a leader in data breach prevention and remediation, the company has managed hundreds of data breach events, protects millions of individuals from identity theft and authored the Identity Crime Victim's Bill of Rights. ID Experts is actively involved with industry organizations including ANSI/Identity Theft Prevention and Identity Management Standards Panel, International Association of Privacy Professionals, Internet Security Alliance, and the Santa Fe Group. For more information, visit www.idexpertscorp.com.

Contact Us

ID Experts®
10300 SW Greenburg Road, Suite 570
Portland, Oregon 97223

Jeremy Henley
Insurance Solutions Executive
p: 760-304-4761
f: 800-298-8457
www2.idexpertscorp.com
Cyberinsurance@idexpertscorp.com