**[LOGO]**

**Security Incident Response Plan**

**[Date], Revision [Number]**

**For Internal Use Only - CONFIDENTIAL**

***[Note: All highlighted text should be replaced and/or removed from the final document. Highlights are context specific.]***

**Table of Contents**

[1 Purpose 3](#_Toc412640386)

[2 Audience 3](#_Toc412640387)

[3 Terminology 3](#_Toc412640388)

[4 References/Related Documents 4](#_Toc412640389)

[5 Information Security Incident Response Preparation 4](#_Toc412640390)

[6 Information Security Incident Response Process 4](#_Toc412640391)

**Table of Revisions [*Note: Add as necessary.]***

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Date** | **Revision Detail** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Purpose

The [Covered Entity] Information Security Incident Response Plan (“ISIRP”) provides a consistent framework for [Covered Entity] to respond to a security incident. The ISIRP will serve as a system-wide guide to facilitate a response in a systematic manner to security incidents and is designed to (a) prevent or minimize disruption of critical information systems; (b) minimize loss or theft of sensitive or critical information; and (c) quickly and efficiently remediate and recover from security incidents.

The use of the ISIRP is mandatory for all employees, partners, and information processing components of [Covered Entity], all computer networks and systems owned or operated by [Covered Entity], and all systems or networks connected to the [Covered Entity] information technology infrastructure under the control of business associates or strategic partners.

# Audience

The following is the audience for the [Covered Entity] ISIRP (Appendix A contains a list and contact information for current members):

* Information Security
* Privacy/Compliance
* Health Information Management (HIM)
* Incident Response Team (IRT)
* Human Resources
* Legal Department
* Corporate Communications / Media Relations

# Terminology

| **Term** | **Definition** |
| --- | --- |
| Incident | An “Incident” is any observable or reported occurrence that a preliminary investigation indicates has a sufficient potential for adverse impact on the confidentiality, availability, or integrity of [Covered Entity]’s information technology or data, whether it is in paper, verbal or electronic form. Incidents include those that occur in departments other than IT or HIM, including HR, Accounting, Marketing, etc. |
| Incident Response Team (IRT) | The IRT or “Incident Response Team” is responsible for responding to Incidents, ensuring successful resolution, tracking Incidents, and advising Information Security on proactive measures to prevent future incidents. |
| Security Incident | See “Incident.” |
| HIPAA | Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, and/or regulations promulgated under such laws. |
| Privacy Laws and Regulations | Means all corporate, international, State and Federal laws, standards, guidelines, policies, regulations, and procedures applicable to [Covered Entity] pertaining to security, confidentiality or privacy, as amended, including without limitation the Health Insurance Portability and Accountability Act, Health Information Technology for Economic and Clinical Health Act, all state data breach notification laws, and all state information security laws and regulations. |
| Data | Means any data or information (whether in electronic or non-electronic form) in the care, custody or control of [Covered Entity] including without limitation, PHI and [Covered Entity]’s confidential information, intellectual property and trade secrets. |
| Protected Health Information (“PHI”) | Shall have the meaning given to such term at 45 C.F.R. § 160.103. |
| Breach | Means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA which compromises the security or privacy of the protected health information. |

Any capitalized terms herein not otherwise defined will have the same definitions as given to them under HIPAA and regulations promulgated under Privacy Laws and Regulations.

# References/Related Documents

| Title | Location |
| --- | --- |
| Incident Report Form 1.0 | [Covered Entity] Shared Drive |
| Business Associate Agreement | [Covered Entity] Shared Drive |

# Information Security Incident Response Preparation

[Covered Entity] should develop incident response capabilities, including the following:

1). Identifying service providers that may support [Covered Entity]’s efforts to detect and respond to an Incident (e.g. external legal counsel, forensic investigation providers, crisis communication firms, call center and mailing vendor) (*see* Appendix B for a list of service providers approved by [Covered Entity]’s cyber insurance carrier to consider);

2). Evaluating opportunities to procure incident response resources (e.g. hardware, software, storage media) that may be useful in responding to an Incident; and

3). Evaluating a schedule for conducting tabletop or mock-breach scenario exercises.

# Initial Reporting of Potential Incidents

* Identify member(s) of the IRT who will be designated as the initial person to contact when someone becomes aware of a potential Incident; and
* Publish and make employees aware of who the initial IRT reporting contacts are.

# Incident Response Process

Upon classification of a scenario as an Incident, IRT shall initiate the following process to verify, investigate, contain, and remediate the Incident. Because Incidents will vary, usage of the process may vary and certain steps in the process may not apply to all Incidents.

Identification & Assessment

* When IRT members learn an Incident may have occurred, the initial IRT members shall:
* Conduct initial analysis and validation to determine if the report represents an actual Incident; and
* Based on initial analysis of the scope, nature, and potential impact of a verified Incident, prepare initial prioritized approach for organizing and assembling an appropriate Incident Response Team. Response priority should consider current and future impact on technology and resources.
* The following threat classifications should be used to assist in the initial classification and validation of a potential security incident:
* **Level 1.** A “Level 1” Incident exists when the initial information shows a low severity and low likelihood of potential impact on core business functions, systems, or Data. Examples may include attempted systematic web site or network perimeter probes, commodity malware infections, or unexplained system malfunctions of user workstations or other non-core production devices.
* **Level 2.** A “Level 2” Escalated Incident exists when the initial information indicates a potential impact to key business functions, systems, or Data. Examples may include a lost unencrypted laptop believed to contain PHI, potential unauthorized access to elevated network administrator credentials, or unexplained malfunctions of security appliances.
* **Level 3.** A “Level 3” Critical Incident exists when the initial information shows a high likelihood of or confirmed unauthorized access to critical systems or access or acquisition of sensitive information. Examples include reports from third parties of confirmed theft of Social Security numbers or PHI, cyber-extortion demands, or unexplained outbound data flow.
* Forming the Incident Response Team:
* The team will likely include representatives from Information Security, Privacy/Compliance, Health Information Management, and Legal;
* As appropriate, the team may also include: HR, Internal Infrastructure, Executive Management Team, external counsel, other external service providers, and others as needed and depending on the nature of the incident.
* HIPAA Privacy Officer shall lead the response to the Incident. The HIPAA Privacy Officer will have the following responsibilities: (1) coordinating the activities of the Incident Response Team; (2) reporting on status of Incident response to executive management as appropriate; (3) identifying when additional resources are needed for the Incident Response Team; and (4) ensuring that the Incident Response Team strategy is carried out.
* Incident Response Team members are expected to devote appropriate time to the response. Internal departments will be expected to supply the necessary resources.
* Legal will maintain a list of the members of the Incident Response Team. All members of the Incident Response Team must receive the Incident Response Team Member instructions form from Legal upon joining the team, which should, among other things as appropriate, advise members to preserve information related to the Incident and not to share details with anyone outside of the team unless doing so is explicitly approved by Information Security and Legal. After obtaining approval to share information, the amount of information shared should be limited to the information necessary to accomplish the task.
* The HIPAA Privacy should assign a name to the Incident (e.g. “Project Orange”) and initiate the Incident tracking process. All subsequent written communications concerning the Incident shall include “Attorney-Client Privileged Communication – Project \_\_\_\_\_” in the Subject line and be limited to fact-based information necessary for the Incident response. Depending on the nature of the Incident, consideration should be given to using out-of-band communication to avoid interception by any unauthorized person who may have system access.
* Prepare a preliminary containment plan based on appropriate considerations, including: (1) The potential scope of the Incident; and (2) the potential impact/risk of the Incident on [Covered Entity]’s systems or data. Additional considerations and guidelines are contained in Appendix C.
* Consider preparing a brief, fact-based summary of what is believed to have occurred to the attention of the Incident Response Team Legal representative with copies to appropriate Incident Response Team members.
* Develop a process to preserve evidence, including: (1) impacted devices, servers, etc.; (2) relevant logs; and (3) timeline of the Incident and response actions taken.

Containment, Eradication, & Recovery

* Upon formation of the Incident Response Team, the team should develop a plan to contain the Incident based on the following considerations where appropriate:
* potential damage to or loss of resources or data;
* the need for forensic analysis of the root cause;
* the need for preservation of evidence;
* time and resources necessary to enact the containment plan; and
* the projected effectiveness of the plan.
* When an Incident has been contained, the Incident Response Team should develop a recovery plan to eliminate effects of the Incident and return assets and business processes to an operational state based on the following considerations, where appropriate:
* eradication work that was completed during the containment phase;
* a determination of the overall impact of the recovery plan and the “next steps” necessary to enact the plan;
* necessary internal resources and communications to form and accomplish the plan;
* necessary external resources to accomplish the plan; and
* the impact of the plan on the ability to investigate the Incident.

Communication & Notification

* Development of the communication plan should consider the following:
* State, federal, and international regulatory obligations, such as HIPAA, state breach notification laws and SEC disclosure requirements; and
* contractual notice obligations, such as business associates.
* HIPAA Breach Notification - Following a breach of unsecured protected health information, [Covered Entity] must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media.
  + Individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the [Covered Entity] is doing to investigate the breach, mitigate the harm, and prevent further similar breaches, as well as contact information for [Covered Entity].
  + If [Covered Entity] experience a breach affecting more than 500 residents of a State or jurisdiction, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. This media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.
  + In addition to notifying affected individuals and the media (where appropriate), [Covered Entity] must notify the Secretary of breaches of unsecured protected health information. If a breach affects 500 or more individuals, [Covered Entity] must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, [Covered Entity] may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.
* Legal is responsible for the development of, and must approve all communications to parties outside of the [Covered Entity] organization. Legal may involve Corporate Communication in developing appropriate communications. A notification checklist is contained in Appendix D.

Special Considerations

* If personal information of individuals (e.g. a person’s name associated with a SSN, driver’s license number, passport, national identification number, bank account, credit card or username/password), may be involved in the Incident, Legal should be notified immediately so they may:
* Begin to assess whether there are any US or international law notification obligations; and
* The timing of any required or recommended notification.
* If an internal user (authorized or unauthorized associate, contractor, consultant, etc.) is suspected to have been involved in the Incident, notify Human Resources.
* Risk Management will coordinate with the insurance broker and carrier to address insurance coverage under [Covered Entity]’s cyber insurance policy or other policies.
* Performing a Breach Risk Assessment for Incidents Involving Protected Health Information
  + Once a potential security incident has been discovered, [Covered Entity] must determine whether the incident was in fact a violation of the HIPAA Privacy Rule. This determination is made by collecting the facts of the incident and analyzing the findings against the requirements of the HIPAA Privacy Rule. If the PHI was acquired, accessed, used or disclosed in a manner not permitted by HIPAA, a violation has occurred. A violation is presumed to be a breach unless [Covered Entity] can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
    - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    - The unauthorized person who used the protected health information or to whom the disclosure was made;
    - Whether the protected health information was actually acquired or viewed; and
    - The extent to which the risk to the protected health information has been mitigated.

|  |  |  |
| --- | --- | --- |
| Breach Risk Assessment Factors | | |
| Factor | Description | Questions to Consider |
| Nature and Extent | The first factor to consider is the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. The probability of compromise increases when the information is of a sensitive nature or the type of identifiers exposed increase the risk of identity theft, financial fraud, or improper use of the information. If the amount and type of PHI used or disclosed is minimal then the probability may decrease.  The goal of evaluating this factor is to determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipients' own interests. | Which patient identifiers were used or disclosed? Does the combination of identifiers used or disclosed increase risk? Are there particular identifiers such as a Social Security Number (SSN) that raise concerns?  Does the PHI used or disclosed contain a sensitive diagnosis? (i.e., substance abuse, mental health, sexually transmitted disease (STD), HIV, cancer)  Does the amount of PHI used or disclosed increase the risk?  Does the use or disclosure reveal the PHI of a well-known individual?  Does the PHI used or disclosed include sufficient indirect patient identifiers that could make re-identification of the individuals possible? |
| Unauthorized Person | The unauthorized person who impermissibly used or to whom the PHI was disclosed is relevant to the risk assessment to assist in determining the probability for compromise. For example, if the recipient is another entity regulated by the HIPAA Privacy and Security Rules or other privacy laws, there may be a lower probability that the PHI has been compromised since the recipient is obligated to protect the information. On the other hand, if the unauthorized person is not a Covered Entity, the probability for compromise may be increased, especially if the recipient's actions are untrustworthy or unpredictable.  The goal of evaluating this factor is to determine the probability as to whether the recipient might further use or disclose the PHI in a manner adverse to the individual or for the recipient's own interests. | Does the unauthorized recipient have obligations to protect the privacy and security of the disclosed information such as a Business Associate or another Covered Entity?  Is the recipient a member of your internal workforce or a BA such that you can assure that the PHI will not be further used or disclosed?  Does the recipient have a relationship with the individual where they are likely to act in the individual's best interest?  Is there additional risk if the recipient likely knows the subject of the PHI?  If the recipient impermissibly used the PHI, what was their purpose or motive for doing so? (i.e., unintentional or inadvertent error, intentional self-serving, malicious, or harmful intent)  What was the attitude and demeanor of the unauthorized recipient? Were they cooperative and willing to work with you to secure the PHI? Were they also concerned about protecting the PHI? Did they initiate contact with you right away or did they appear reluctant to cooperate as leverage for something else they wanted for their own best interests?  Was the recipient an unintended recipient or did they seek out the information?  If only indirect identifiers were disclosed, does the recipient have the ability to re-identify the PHI?  Is it believed that the PHI was taken with intent to use or sell? |
| Acquisition / Viewing of PHI | [Covered Entity] must consider whether or not the PHI was actually acquired or viewed or whether there was an opportunity for the PHI to be acquired or viewed. The probability of compromise is lowered only if the opportunity existed for the PHI to be acquired or viewed but the PHI was not actually acquired or viewed. For example, a billing statement sent to the wrong address that is returned unopened would be considered PHI that was not actually viewed. In contrast, if the billing statement was opened and the recipient called to notify the covered entity, it would be considered acquired and viewed. | Was the PHI actually acquired or viewed by an unauthorized person?  Is it possible to demonstrate that the disclosed PHI was never accessed, viewed, or acquired?  If an electronic device was involved, does forensic analysis show that the PHI was accessed, acquired, viewed, transferred, or compromised?  If electronic PHI (ePHI) is involved, what does the audit trail indicate? What actions (i.e., print, view) were taken? What parts of the record were accessed? |
| Extent Risk Has Been Mitigated | Quickly mitigating any risk to PHI that was impermissibly used or disclosed, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed or will be destroyed, may lower the probability that the PHI has been compromised.  The goal in evaluating this factor is to determine how thoroughly and quickly the PHI involved has been secured following the impermissible use or disclosure. | If the recipient was a Covered Entity or other reliable business bound by privacy obligations (i.e., business associate, banks, or attorneys), was verbal confirmation given and documented that PHI was destroyed?  If the recipient was not a Covered Entity or business associate otherwise bound by privacy obligations, was written confirmation of destruction obtained?  If the recipient was an employee who impermissibly used PHI, was a statement of assurance obtained attesting that PHI will not be further used or disclosed?  Has satisfactory assurance been obtained from the unauthorized recipient that the disclosed PHI will not be further used or disclosed or will be destroyed? Has an effective mitigation strategy been implemented such that further unauthorized disclosures are extremely unlikely?  Was the PHI returned in a timely fashion and intact? |
| Once all factors have been reviewed, [Covered Entity] must then evaluate the overall probability that the PHI has been compromised by considering all the factors in combination. Other factors may also be considered where necessary. | | |

Final Steps

* Following an Incident, [Covered Entity] should consider doing the following:
* Analyzing the root causes of the incident.
* Perform Risk Assessment to determine whether additional physical, administrative or technical safeguards are warranted.
* Remedial measures taken.
* Lessons learned.
* Whether revisions to this policy should be made.
* Whether policies and processes should be modified to meet new or different risks.
* If the Incident involved business associate or third party service providers, review third party service provider’s compliance with relevant privacy or data security requirements and whether any potential issues need to be addressed.

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

**APPENDIX A**

**INCIDENT RESPONSE TEAM MEMBERS & CONTACT INFORMATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Title | Name | Office Phone | Alternate Phone | E-mail |
| **HIPAA Privacy Officer** |  |  |  |  |
| **HIPAA Security Officer** |  |  |  |  |
| **Chief Technology Office** |  |  |  |  |
| **Corporate Communications** |  |  |  |  |
| **General Counsel** |  |  |  |  |
| **[Others]** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**APPENDIX B**

**INCIDENT RESPONSE SERVICE PROVIDERS**

**Forensic Investigation**

Forensic Investigation Inc.  
[Address 1]

[Address 2]

Contact Name: [Contact Name]

Phone No.: (555) 555-5555

**Crisis Communications**

Crisis Communications Inc.

[Address 1]

[Address 2]

Contact Name: [Contact Name]

Phone No.: (555) 555-5555

**Mailing/Call Center/Credit Monitoring**

Mailing, Inc.

[Address 1]

[Address 2]

Contact Name: [Contact Name]

Phone No.: (555) 555-5555

Call Center Inc.

[Address 1]

[Address 2]

Contact Name: [Contact Name]

Phone No.: (555) 555-5555

Credit Monitoring Inc.

[Address 1]

[Address 2]

Contact Name: [Contact Name]

Phone No.: (555) 555-5555

**Legal**

Law Firm

[Address 1]

[Address 2]

Contact Name: [Contact Name]

Phone No.: (555) 555-5555

**APPENDIX C**

**ADDITIONAL GUIDELINES/CONSIDERATIONS**

1. Don't panic. Be as calm and methodical as you can, and think about your course of action. Involve a second person to assist and observe all actions you take.

2. Do a quick assessment. Do not immediately shut down the machine, as you may lose important information that resides only in system memory. Consider disconnecting it from the network but leaving the power on.

3. Report the problem. Call the [IR Team] at [Contact Phone Number]. Alternatively, you can send a message (using a different PC) to [IR Email Address].

4. Gather and preserve all relevant information. This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and database activity logs. Copy them to a safe location (that will not be deleted or over-written), so that you can study them later.

5. Take notes. Record key **factual** events, including things you observed, actions you took, dates and times, and the like. It is best to log your activities as they occur. Over time, your actions and the order in which they were executed may not be easily remembered.

**APPENDIX D**

**Notification Checklist**

* Consider internal and/or external forensics analysis. Engage forensic firm through legal counsel.
* Determine the universe of affected individuals and the data elements for those affected individuals. Identify minors, deceased, U.S. residents, Canadian residents, persons residing outside of the U.S. or Canada.
* Analyze data elements to determine if notification is required under federal and state laws.
* Determine if law enforcement should be notified.
* Determine which regulators, if any, need to be notified.
* Determine if a crisis management firm needs to be engaged (consider sensitivity of data, number of people involved, etc.).
* Prepare and continue to update a media hold statement or press release in conjunction with client’s PR team (and possibly a crisis management firm—engage crisis management firm through legal counsel).
* Determine if notification vendor (for mailing and operating a call center) is to be used.
* Assess if credit monitoring should be offered and to whom (minors and adults)
* If mailing will occur, prepare a spreadsheet of affected individual with name, address, and possibly nature of data elements. Identify minors, deceased, U.S. residents, Canadian residents, persons residing outside of the U.S. or Canada.
* Prepare notification letter(s) based on type of person affected (customer, employee, etc.) and data elements (name, SSN, DOB, payment card, etc.).
* For mailing, send logo (.jpeg), signature (.jpeg), address list of affected persons to vendor.
* If mailing and offering credit monitoring, purchase codes from credit monitoring provider.
* Prepare FAQs for call center.
* Prepare any regulatory letters (AG notices, state offices, CRAs, if there are other states involved).
* Receive and approve proofs of letters from notification vendor.
* Prepare internal communications to board, leaders, and employees.
* Prepare website posting and in-store notices if necessary.
* Determine if substitute notice is necessary (e.g, email, website posting, and media notice).
* Establish call center escalation process.
* Print and mail letters.
* Ongoing media relations, as needed.