

# Security Incident Investigation Report

**Directions:** After the report regarding a security incident is received, an investigation into the incident shall be initiated. The report must be completed by the incident responders.

## Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

## Section 2: Details of the Incident Handler

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

## Section 3: Incident Update

Current Status of Incident Response:	
Severity of the Incident:	<input type="checkbox"/> <b>Low</b> <input type="checkbox"/> <b>Moderate</b> <input type="checkbox"/> <b>High</b> <input type="checkbox"/> <b>Critical</b>
Incident Type:	
Summary of Incident:	

#### Section 4: Details of the Investigators

Name	Title	Organization	Phone	Email

#### Section 5: Log of Actions Taken

Date	Incident Handler/ Investigator	Actions	Results

#### Section 6: Identified Evidence Details

Date	Incident Handler/ Investigator	Evidence

### Section 7: Parties Involved in the Incident

Name	Title	Organization	Phone	Email

### Section 8: Incident Handler and Investigator Comments

Date	Incident Handler/ Investigator	Comments

## Section 9: Findings

Type of Incident:	<input type="checkbox"/> Unauthorized Access	<input type="checkbox"/> Inappropriate Usage
	<input type="checkbox"/> Malicious Code	<input type="checkbox"/> Denial of Service
	<input type="checkbox"/> Multiple Component	<input type="checkbox"/> Network Attack
	<input type="checkbox"/> Policy Violation	<input type="checkbox"/> Unknown/Other (Please describe below)
Incident Description Notes:		
Cause of Incident:		
Cost of Incident:		
Sensitivity of Data:	<input type="checkbox"/> Public	<input type="checkbox"/> Restricted/Confidential (Privacy Violation)
	<input type="checkbox"/> Internal Use Only	<input type="checkbox"/> Unknown/Other (Please describe below)
Brief Description of Compromised Data:		
Business Impact of Incident:	<input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Critical	
PHI Compromised?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
If yes, Estimated Number of Compromised PHI Accounts:		
(If known) Actual Number of Compromised PHI Accounts:		
PHI Breach Impact:	<input type="checkbox"/> High ( $\geq 500$ PHI) <input type="checkbox"/> Medium ( $< 500$ PHI) <input type="checkbox"/> Unknown	
Data Encrypted?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Encryption Description:		

**Important Note:** If PHI accounts may have been compromised and data was not encrypted, please follow breach evaluation procedures and, if necessary, breach notification procedures.

**Was the Breach Evaluation Processes Initiated?** ☐ Yes ☐ No

If Yes, Date of Initiation: \_\_\_\_\_

#### Section 10: Recommended Corrective Actions

Recommended By	Date	Recommended Corrective Action

#### Section 11: Actions Taken

Performed By	Date	Action Taken

### Section 12: Notifications Made

Organization	Point of Contact	Date	Summary of Information Provided

I hereby declare that the details provided in this report are true and accurate to the best of my knowledge and all contributors. I further declare that all parties who participated in the investigation, all findings of the investigation, and all recommended corrective actions as well as all actions taken by any parties to this investigation are clearly documented. This report has been provided to the HIPAA Committee for review in both its final form and, as appropriate, throughout the term of the investigation. Effective on the date indicated below, this incident investigation is considered closed.

\_\_\_\_\_  
Incident Handler's Signature

\_\_\_\_\_  
Date