SECURITY INCIDENT INVESTIGATION REPORT
<Practice Name>

Directions: Upon receipt of a Security Incident Report, an investigation into the incident shall be initiated. The Security Incident Investigation Report should be completed as thoroughly as possible by the Incident Handler and Investigators. Since investigations vary, some sections may not be applicable to every investigation. In the electronic version, clicking on any blue link in the form will move you to the applicable instructions. Please print clearly or type.

Section 1: Incident Handler			
Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

Section 2: Incident Update	
Current Status of Incident Response:	
Summary of Incident:	

Section 3: Investigators				
Name	**Title**	**Organization**	**Phone**	**Email**

Section 4: Log of Actions Taken			
Date	**Incident Handler/ Investigator**	**Action**	**Results**

Section 5: Evidence Found		
Date	**Incident Handler/ Investigator**	**Evidence**

Section 6: Parties Involved in Incident				
Name	**Title**	**Organization**	**Phone**	**Email**

Section 7: Incident Handler and Investigator Comments		
Date	**Incident Handler/ Investigator**	**Comments**

Section 8: Findings		
Type of Incident:	☐ Unauthorized Access	☐ Inappropriate Usage
☐ Malicious Code	☐ Denial of Service	☐ Multiple Component
Cause of Incident:		
Cost of Incident:		
Business Impact of Incident:		
PHI Compromised? ☐ Yes ☐ No		
If yes, Estimated Number of Compromised PHI Accounts: _____ - or -		
(If known) Actual Number of Compromised PHI Accounts: _____.		
PHI Breach Impact: ☐ High (≥ 500 PHI Accounts) ☐ Medium (< 500 PHI Accounts) ☐ Unknown		
Data Encrypted? ☐ Yes ☐ No If yes, description of encryption:		

CONFIDENTIAL DOCUMENATION – Intended for internal use only!

Section 8: Findings
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 breach evaluation initiation: _____.

Section 9: Recommended Corrective Actions		
Recommended By	**Date**	**Recommended Corrective Action**

Section 10: Actions Taken		
Performed By	**Date**	**Action Taken**

Section 11: Notifications Made			
Organization	**Point of Contact**	**Date of Notification**	**Summary of Information Provided**

I attest that the information contained in this Investigation Report is true and accurate to the best of my knowledge and the knowledge of all contributors. I further attest 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 Investigation 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

SECURITY INCIDENT INVESTIGATION REPORT INSTRUCTIONS

- **Date Report Received** is the date that the Security Officer or Risk Manager first viewed the Incident Report.
- **Date Report Processing Began** is the date that the assigned Incident Handler began reviewing and investigating the Incident Report.
- **Report Number** should be assigned by the Security Officer. This Report Number should be noted on both the Security Incident Investigation Report and the Security Incident Report. If more than one Security Incident Report was filed for the same security incident/event, all of the applicable Report Numbers should be listed on the Security Incident Investigation Report.
- **Current Status of Incident** may be an ongoing attack, one time occurrence, resolved issue, etc.
- **Summary of Incident** is the summary of all information known about the security incident/event at the beginning of the investigation process.
- **Parties Involved in Incident** should include all persons who were interviewed and all persons who were found to be involved in the incident/event.
- **Cause of Incident** may include misconfigured application, unpatched host, compromised user account, inappropriate user permissions, etc.
- **Cost of Incident** should include both the cost of the investigation including the time spent investigating and the cost of any actions necessary to mitigate the security breach including initial and ongoing costs.
- **Business Impact of Incident** could either be a description of the incident's effect (i.e. the accounting department was unable to perform tasks for two days) or an impact category based on the cost (i.e. a "major" incident has a cost of over $100,000) as defined in the practice's Security Incident Policy.
- **PHI Breach Impact** is based on either the estimated number of compromised PHI records or, if known, the actual number of compromised PHI records.
- **Description of Encryption** should include the encryption type (i.e. DES, 3DES, AES, etc.); the encryption level (i.e. 128-bit, 192-bit, 256-bit); compliance with the FIPS 140-2 standard; whether data was encrypted at rest, in transit, or both; and any other pertinent information.
- **Recommended Corrective Actions** includes ALL recommended corrective actions even if they were not acted upon. This will create a clear record of all corrective actions considered.
- **Actions Taken** should include, of course, only the recommended corrective actions that were acted upon.
- **Notifications Made** may include the CEO, the Board of Directors/Trustees, legal counsel, law enforcement, and employees. However, any breach notification as required in HIPAA regulations, including the American Recovery and Reinvestment Act's (ARRA) Health Information Technology for Economic and Clinical Health (HITECH) Act, should be documented within the breach evaluation and notification procedure.

This Report is based on the guidelines found in Appendix 3 of NIST SP 800-61 Rev. 1: *Computer Security Incident Handling Guide*. A list of all NIST 800 publications can be found at http://csrc.nist.gov/publications/PubsSPs.html.