# SECURITY INCIDENT REPORT

**<Practice Name>**

**Directions:** The reporting employee or witness needs to complete Section 1 and Section 2. If needed, the employee or witness can consult with the IT Department to complete Section 2. **Please Note:** All persons who contribute information to the report should be recorded in the "Report Augmented By" field. In the electronic version, clicking on any blue link in the form will move you to the applicable instructions. When completed, the form should be **submitted to the Security Officer or Risk Manager** with a copy to be retained by the reporting employee or witness and, if applicable, to be provided to the employee's Supervisor. The completed form should be submitted **within 24 hours of discovery of the incident or event**. Please print clearly or type.

| | |
|---|---|
| **Section 1: Incident Reporter** | |
| Name: | |
| Title: | |
| Report Number: | |
| Department: | |
| Email Address: | |
| Phone Number and, If Applicable, Extension: | |
| (If Available) Alternate Phone Number: | |
| Report Submitted To – **Indicate name and title**: | |

| | |
|---|---|
| **Section 2: Incident Details** | |
| Date and Time of Discovery of Incident: | |
| Estimated Date and Time Incident Started: | |
| Description of Incident – **Be Specific**: | |
| PHI Compromise Suspected? | □ Yes □ No |
| Location of Incident: | |
| Current Status of Incident: | |
| Source or Cause of Incident: | |
| Employees, Contractors or Others with Incident Knowledge – **List all known potential witnesses**: | |
| Operating System, version, and patch level: | |
| Antivirus Software Installed, Enabled and Updated? | □ Yes □ No Comments: |
| Description of Affected Resources: | |

| **Section 2: Incident Details** | |
|---|---|
| Mitigating Factors: | |
| Estimated Technical Impact of Incident: | |
| Response Actions Performed: | |
| Other Organizations Contacted: | |
| Report Augmented By: | |
| Additional Comments: | |

I understand that by submitting this Incident Report in good faith, I cannot be subject to retaliation. I attest that the information contained in this Incident Report is true and accurate to the best of my knowledge on the date indicated below. If I obtain any additional information regarding this incident, I agree to provide said supplementary information to the person specified above in "Report Submitted To" and/or the designated Incident Handler. I agree to cooperate fully with all investigators of this incident until the incident is closed.

_______________________________________________ ___________________________

Incident Reporter's Signature Date

## SECURITY INCIDENT REPORT INSTRUCTIONS

- **Report Number** should be left blank; this will be completed by the Incident Handler.
- **Time** should be recorded in the 24 hour format and include the time zone of the primary location of the incident. Unless otherwise noted, the time zone will default to your primary office location.
- **Description of the Incident** may include how it was detected, what occurred, who detected it, etc.
- **PHI Compromise Suspected** should be "Yes" if there is any concern by any person contributing to this report that personal health information (PHI) was compromised. "No" should only be indicated if all persons contributing to the report are certain that PHI was not compromised.
- **Location of Incident** may be a campus, building, department, or room. Please be as specific as possible.
- **Current Status of the Incident** may be an ongoing attack, one time occurrence, resolved issue, etc.
- **Source or Cause of Incident** (if known) may include the computer's location, host name, and/or IP address; user account; etc.
- **Contact Information** should include name, title, organization, phone number and email (as known).
- **Operating System** may include Windows XP, Vista, or 7; Windows Server 2003 or 2008; Mac; Linux; Unix; etc.
- **Affected Resources** may include a network device, a workstation, an application, or specific data and may be described as hardware location, IP address, and host name; a system name, location, and function; a user account; etc.
- **Technical Impact** may include data deleted or compromised, system crashed, application unavailable, nonfunctional workstation, etc.
- **Response Action Performed** may include shutting off the computer, disconnecting the computer from the network, beginning malicious software removal, disabling an affected user account, etc.; documentation should include the action taken and identify who took the action.
- **Organizations Contacted** may include software vendor(s), hardware vendor(s), contracted IT support and others; recorded information should include organization, contact's name, date and time of initial contact, and contact method (phone, email, etc.). Any response from the contacted organizations should be noted in the Additional Comments field.
- **Report Augmented By** should list the contact information of everyone except the initial reporter who provided data for the report.

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.