Information Security Form

<table>
<thead>
<tr>
<th>Title</th>
<th>Incident Report Form</th>
<th>Reference No</th>
<th>02.01.02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version No</td>
<td>0.1</td>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Creation Date</td>
<td>01/02/2008</td>
<td>Revision Date</td>
<td>10/14/2011</td>
</tr>
<tr>
<td>Approval Date</td>
<td>9/30/2010</td>
<td>Approved by</td>
<td></td>
</tr>
<tr>
<td>Applicability</td>
<td>Protected, Confidential and Public</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Departments are requested to use this form when reporting an incident that involves the availability, confidentiality, and integrity of sensitive university information. For urgent assistance or help in completing this form contact the Information Security Office at Infosec@wusm.wustl.edu or call 747-2955.

Please complete and return the form within 3 business days, the Information Security Office will follow-up on any outstanding forms.

Sections 1 – 2 should be completed the Data custodian and/or owner.
Sections 3 – 9 should be completed by the IT Department.

1. Contact Information for this Incident (To be completed by the Data Custodian and/or Owner)

   Name: ____________________  Organization/Department: ____________________

   Title: ____________________  Address: ____________________

   Office Phone: _____________  Cell Phone/Pager: ____________________

   Fax Number: _______________

2. Information Assessment (To be completed by the Data Custodian and/or Owner)

   IMPORTANT NOTE: Please describe in detail anything you know about the computer system, the data on the system, its use, who had access to the system, how the system was used, protection mechanisms used on the system to protect the data, etc. The intent is to access the likelihood of the information being compromised by a party or parties with the intent of using it to harm the University or its affiliates.

   Did this incident result in a compromise of sensitive university information to include EPHI, Employee, Financial, Research Data, etc?

   Yes  No

   If yes, please elaborate;
   Please describe the type of data on the system:
   Was PHI on the system?

   Were any of the following 18 identifiers on the system:

   1. Name
   2. DOB
Information Security Form

3. SSN
4. Address
5. Telephone Number
6. Email Address
7. Fax Number
8. Medical Record Number
9. Health Plan ID
10. Internet IP address
11. Certificate Number
12. Device Identifiers
13. Photograph
14. Biometric Identifiers
15. Web Address (URL)
16. Vehicle Identifier
17. Account Numbers
18. Any other unique identifying number, characteristic or code

Was sensitive information other than PHI on the system?

Was the system password protected?

Was the data encrypted?

Damage or observations resulting from incident:

3. Physical Location of Incident (To be completed by the IT department)

(Include building number, room number, if available): ________________________________

4. Date and Time Incident Occurred (To be completed by the IT department)

Date (mm/dd/yy): ________________________________________________________________

Time (hh:mm:ss am/pm/Time Zone): ______________________________________________

5. Type of Incident (Mark all that Apply) (To be completed by the IT department)

- Intrusion
- Virus / Malicious Code
- Social Engineering
- Root/Administrator Compromise
- User Account Compromise
- Policy Breach
- Network Scanning / Probing

- Denial of Service
- System Misuse
- Technical Vulnerability
- Web Site Defacement
- Hoax
- Theft

Other (Specify):
Information Security Form

6. Information on Affected System (To be completed by the IT department)

IP Address: ______________________________________________________________

Computer/Host Name: ______________________________________________________

Operating System (please include release number and patch level if known): ______

Application(s) associated with the Incident: __________________________________

7. How Many Host(s) are affected (To be completed by the IT department)

[ ] 1 to 10  [ ] 10 to 100  [ ] More than 100

8. Information Sharing (To be completed by the IT department)

Has the Information Security Officer been notified?

[ ] Yes  [ ] No

If yes, provide name and date of notification:

Consider with whom this information may be shared outside of the Washington University (do not leave blank and check all that apply):

[ ] BJC  [ ] General Counsel  [ ] Other Physicians

[ ] Other Washington University Departments  [ ] Local Police  [ ] Local News Services

[ ] FBI

Other (Specify): ____________________________________________________________

9. Additional Information (To be completed by the IT department)

(If this incident is related to a previously reported incident, include any previously assigned incident number for reference. Also please provide a brief explanation of what the system/computer was used for, applications it contained to perform what it was normally used for and a description of the physical security of the machine if this was a theft).