Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS INFORMATION SECURITY (IS) INCIDENT HANDLING AND BREACH ANALYSIS/NOTIFICATION PROCEDURE

December 3, 2010

Version 2.3

Summary of changes in Incident Handling Procedure version 2.3

The most significant changes to the document are:

1. This document replaces the *CMS IS Incident Handling and Breach Analysis/Notification Procedure*, v2.2, dated August 18, 2009.
2. Section 2, modified the Computer Incident response procedure to waive the requirement for a incident response form for incidents entered directly into the CMS incident tracking system (RiskVision) by authorized entities.
3. Section 2.2, modified Incident Categories to increase the response time for CAT 1, 2, 3 and CAT PII.
4. Section 3, added additional details and responsibilities for the CISO.
5. General formatting changes.

Summary of changes in Incident Handling Procedure version 2.2

The most significant changes to the document are:

1. This document replaces the *CMS IS Incident Handling and Breach Analysis/Notification Procedure*, v2.1, dated October 28, 2008.
2. Section 1.1, modified section name to Definitions and broke out subsections 1.1.1, 1.1.2, and 1.1.3 for security incident, security event, and reportable event
3. Section 1.2, deleted this section as it is incorporated into section 2.2
4. Section 1.3, changed paragraph to section 1.2 after the deletion of the previous section 1.2.
5. Section 2, replaced entire section with new section 2 titled CMS Computer Security Incident Report Procedure.
6. Sections 2.1 through 2.11, added subsections that describe the procedures for completing the CMS Computer Security Incident Report.
7. Section 3.2.1, added the phone and email contact information for the CMS IT Service Desk.
8. Section 5.1, removed the additional steps for security incidents and security advisory/information.
9. Section 5.2, created new subsection from section 5.1, additional steps for security incidents and security advisory/information.
10. Appendix A, replaced previous Computer Security Incident Report form with new form from DHHS.
11. Appendix B, replaced previous Appendix B with the new Appendix A– Sample CSIR.
12. Appendix B, added Abbreviations and Acronyms.
13. General changes, incorporated and synced changes made in the *CMS IS Incident Handling and Breach Analysis/Notification Template v2.1*, dated August 18, 2009
14. General formatting, added changes throughout the document to bring the document into compliance with Section 508.
15. General formatting, added changes throughout the document to support CMS IS standards.

Summary of changes in Incident Handling Procedure version 2.1

The most significant changes to the document are:

1. The phone and email contact information for the CMS IT Service Desk was added to the document.
2. Section 3.2.1, added the responsibility to determine if an incident is related to PII to the CMS IT Service Desk.
3. Section 3.11.2, added responsibilities for the CMS Senior Privacy Official to determine the impact of an incident/breach pertaining to both personal identifiable information and protected health information.
4. Section 3.12.2, added responsibility for the Chief Information Security Officer to implement training based on the lessons learned from an incident processed.
5. Table 2: Incident Reporting Timeframe Criteria, Added definition of Protected Health Information (PHI) to table.
6. Section 3.4.2, deleted duplicate responsibility bullet item.
7. Section 3.4.2, added responsibility to oversee the development and implementation of the CMS corrective action plan, if applicable.
8. Section 3.5.2, added responsibility to oversee the PHI and PII corrective action plan (if applicable).
9. Section 3.11.2, added responsibility to provide guidance on the impact of both PII and PHI incident/breach.
10. Section 3.11.2, added responsibility to comment on proposed notification letters.
11. Section 3.12.2, added responsibility to coordinate lessons learned type briefings of incidents for Business Owners and System Developers/Maintainers.

Summary of changes in Incident Handling Procedure version 2.0

The most significant changes to the document are:

1. The document name has been changed to include “Breach Analysis/Notification”.
2. This is a complete rewrite of the Incident Handling Procedures due to new guidance from the Department of Health and Human Services (DHHS). This document adopts verbatim many definitions, incident categories, reporting timeframes and reporting templates provided by the DHHS Secure One. The use of common terminology, timeframes and reports will facilitate communication, reporting and incident management.
3. The proponent for this document is now the Office of Information Services, Enterprise Architecture and Strategy Group.
4. Section 1.1, the definition of a security incident has been modified to include the definition from the DHHS incident handling guidance.
5. Section 1.2 Incident Categories and Reporting Time Criteria, has been added per item 1 above.
6. Table 1, Incident Categories, has been added per item 1 above.
7. Table 2, Incident Reporting Timeframe Criteria, has been added per item 1 above.
8. Section 1.3, Event Categories, has been added per item 1 above.
9. Section 1.4, Security Incident Response Phases, has minor word and formatting changes for clarity only.
10. Section 2, Incident Reporting Template and Procedures, has been added

11. Sections 3, 4 and 5 have been completely rewritten per item 1 above.
12. Section 6, Monthly Summary Reports, has been added per item 1 above.
13. Section 7, Security Alerts, has been added per item 1 above.
14. Appendix A, CMS Security Incidents Reporting Template, replaces the previous appendix.
15. Appendix B, Incidents Involving Personally Identifiable Information, replaces the previous appendix.

Executive Summary

The Centers for Medicare & Medicaid Services (CMS) is the Federal agency that administers Medicare, Medicaid and the Children's Health Insurance Program (CHIP). CMS is responsible for protecting health insurance and patient information used in the administration of CMS programs.

CMS' Information Security Program has numerous controls to reduce or eliminate risk to our computer systems and/or sensitive data. Preparation and coordination to handle security incidents, should they occur, improve the overall security posture of the enterprise by providing a systematic process of security incident management. Roles and responsibilities are identified, and escalation procedures are defined to provide an orderly approach to incident response. Incident response involves the following phases: preparation, detection, alert, triage, response (containment and eradication), recovery and follow-up. The goal of a systematic approach to handle security incidents is to resume system and business operations as soon as possible while preserving the incident's forensics information for further analysis and security process enhancements. Escalation procedures are based on incidents that may occur within the CMS business environment.

This procedure also covers CMS' roles and responsibilities in evaluating incidents for determining whether to notify affected individuals and others. Critical to this determination are the roles of the CMS Senior Core Leadership for Breach Notification and the Breach Analysis Team (BAT), which provides staff support to the Senior Core Leadership.

This *Incident Handling and Breach Analysis/Notification Procedure* covers business conducted by CMS employees and contracted personnel. Additionally, the procedure is incorporated by reference into CMS contracts and agreements, and is applicable to those entities as well, e.g., system development and maintenance contracts and the users of CMS data such as the research community.

CMS is an active participant in the Department of Health and Human Services (DHHS) Secure One program. Accordingly, this document adopts verbatim many definitions, incident categories, reporting timeframes and reporting templates provided by the DHHS Secure One. The use of common terminology, timeframes and reports will facilitate communication, reporting and incident management.

Table of Contents

1. INTRODUCTION

1.1. DEFINITIONS

1.1.1 SECURITY INCIDENT

A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Security incidents also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction. Any of these incidents has the potential for jeopardizing the confidentiality, integrity and/or availability of an information system or the data being processed, stored or transmitted by an information system. A security incident is also a violation or an imminent threat of a violation of an explicit or implied security policy, acceptable use policies, or standard security practices. While certain adverse events, (e.g., floods, fires, electrical outages, excessive heat, etc.) can cause system crashes, they are not considered computer-security incidents. A security incident becomes a breach when the incident involves the suspected or actual loss of personally identifiable information including personal health information.

1.1.2 SECURITY EVENT

A security event is an observable occurrence in a network or system, e.g., detected probes, infections prevented, log reviews, etc..

1.1.3 REPORTABLE EVENT

A reportable event is anything that involves: (1) a matter that a reasonable person would consider a violation of criminal, civil or administrative laws applicable to any Medicare contract or Federal health care program; or (2) integrity violations, including any known probable or suspected violation of any Medicare contract term or provision. A reportable event may be the result of an isolated event or a series of occurrences. Reportable events that are subject to reporting under these procedures include events that occur at the contractor site/system or any of its subcontractors, consultants, vendors or agents. If the reportable event results in an overpayment, relating to either Trust Fund payments or administrative costs, the report must describe the overpayment with as much specificity as possible, as of the time of the due date for the submission of the report. Many events are flagged for inappropriate use of resources or reflect situations that do not fall under the definitions above.

1.2. EVENT CATEGORIES

CMS utilizes the following categories to report monthly to DHHS Secure One.

- *Malicious Code Prevented:* Viruses were prevented and did not cause any harm to any system;
- *Probes and Reconnaissance Scans Detected:* Probes and scans were detected and did not pose a serious threat to a critical system;
- *Inappropriate Usage*: Misuse of resources; or
- *Other*: Cannot be categorized under any of the above.

1.3. SECURITY INCIDENT RESPONSE PHASES

1.3.1 PREPARATION PHASE

The preparation phase is the process of establishing policies, processes, procedures and agreements covering the management and response to security incidents. This includes guidelines such as identifying levels and responses, auditing and logging, reporting guidelines, resolution and follow-up communications.

1.3.2 ALERT PHASE

The alert phase is the process of learning about a potential security incident and reporting it to the CMS Help Desk to generate a Remedy incident ticket. This phase also includes the reporting of potential incidents to the CMS IT Service Desk, who will immediately refer this to the CMS Computer Security Incident Response Team (CSIRT). Alerts may arrive from a variety of sources including: monitoring of firewalls and intrusion detection systems, anti-virus software, threats received via e-mail, and media reports about new threats. The CMS CSIRT may also directly generate Remedy tickets while managing potential incidents.

1.3.3 TRIAGE PHASE

The triage phase involves the process of examining the information available about the potential security event to determine whether a security incident has occurred. During this phase, an incident component lead is assigned. If an incident has occurred, the nature of the incident is determined; the initial priority level is assigned; and the documentation of all actions taken is initiated. This phase may also involve creating an Incident Response Team (IRT) to work on activities relating to incident handling. A decision to “pursue” or “protect” is made during his phase according to the sensitivity of the data and criticality of the operational system. If a decision to “pursue” is made, the IRT allows the intrusion or misuse to continue as analyst(s) gather information about the malicious activity before proceeding to “protect” the system and initiate actions to discontinue the unauthorized actions as described in the containment and eradication phases. In either case, protective actions will be performed on the system to safeguard data and system resources on the affected system. For higher priority level incidents, consideration is given to potential legal or public relations impacts arising from each course of action.

1.3.4 RESPONSE (CONTAINMENT AND ERADICATION) PHASE

The response phase is the process of limiting the scope and magnitude of an incident in order to keep the incident from getting worse. Consideration is given to factors such as system backup, risk to continuing operations, and changing passwords or access controls lists (ACLs) on compromised systems and data. This phase also includes determining the cause of the incident, improving system defenses, determining system vulnerabilities and removing the cause of the incident to eliminate possibility of recurrence. It may be necessary to activate Business continuity plans. The Business Owner of the Incident Handling Coordination and Management (IHCM) Team, defined in Section 3.7, would make this determination.

1.3.5 RECOVERY PHASE

The system and business process returns to full and normal operations during this phase. Actions include restoring and validating the system, deciding when to restore operations, and monitoring systems to verify normal operations without further system or data compromise.

1.3.6 FOLLOW-UP PHASE

This phase involves developing an incident report and disseminating it to appropriate entities according to established policies; identifying lessons learned from the incident handling process including the successful and unsuccessful actions taken in response to an incident; and developing recommendations to prevent future incidents and to improve enterprise security implementation.

2. COMPUTER SECURITY INCIDENT REPORT PROCEDURES

The CMS Computer Security Incident Report (CSIR) fully incorporates the HHS Computer Security Incident Response Center CSIR Guide. The CMS CSIR form consists of the following sections:

- Reporting Overview
- Incident Category
- Compromised Device Information
- Section A – Lost/Stolen Asset
- Section B – PII Related Incident
- Section C – Malicious Code
- Section D – Unauthorized Access
- Section E – Improper Usage/Policy Violation
- Section F – Exercise/Network Defense Testing
- Section G – Denial of Service, Scans/Probes/Attempted Access, & Investigations
- Section H – Reportable Events

Some organizations within CMS have been granted authority by the CMS Chief Information Security Officer (CISO) to report incidents directly into the CMS incident tracking system (RiskVision.) Those designated organizations may report incidents directly into the tracking systems thereby bypassing the manual completion of a CSIR form. All others ***must*** report security incidents using the CSIR form.

CMS information and information system security related incidents shall normally be reported using the CSIR form. Incidents that concern PII should be reported using the CSIR form set forth in the *CMS IS Incident Handling Breach Analysis/Notification Template.* The *CMS Incident Handling Template* can be downloaded from the CMS Info Security Library. (http://www.cms.hhs.gov/InformationSecurity/)

All fields marked with an asterisk are required fields. While the CSIR form should be fully completed to the extent possible, CMS is aware that not all requested information may be available at the time of the report. If requested (but not required) information is not available, indicate a reasonable expectation as to when the remaining information will be obtained and provided to the CMS Computer Security Incident Response Team (CSIRT). Appendix A – Sample CMS Computer Security Incident Report Form is provided for information. All CMS information and information system security related incidents will be documented using the CMS CSIR contained within the *CMS IS Incident Handling Breach Analysis/Notification Template* unless prior authorization has been granted to enter directly into the CMS incident tracking system (RiskVision).

2.1. REPORTING OVERVIEW

The fields in this section provide the CMS CSIRT with information necessary to obtain incident status updates. Such information includes the date and time of the report, the tracking number assigned by the reporting entity(ies), and the contact information of the individual reporting the incident as well as that of the impacted user. The reporting overview subsections should be completed as follows:

- **Date/Time**: Enter the date and time of the report.
- **Incident Tracking Number**
    - **HHS**: Enter the incident identification (ID) number provided by HHS CSIRC.
    - **OPDIV**: Enter the incident ID number provided by the Operating Division (OPDIV) reporting the incident.
    - **US CERT**: Enter the incident ID number provided by the United States Computer Emergency Readiness Team (US-CERT).
- **Reporting Individual Contact Information**
    - **Name***: Enter the full name of the individual reporting the incident.
    - **Email***: Enter the email address of the individual reporting the incident.
    - **Office Number***: Enter the office telephone number of the individual reporting the incident.
    - **Cell Number**: Enter the mobile telephone number of the individual reporting the incident.
    - **Dept/OPDIV***: Enter the name of the department or OPDIV of the individual reporting the incident.
    - **UserID**: Enter the User ID of the individual reporting the incident.

- **Name(s) of Dept/OPDIV or individual notified of security incident**: Use a separate row for each notification. All information within each row must relate to the same notified party.
    - **Dept/OPDIV**: Enter the name(s) of the department or OPDIV that was notified of the incident.
    - **Name/Title**: Enter the name(s) and titles of any individuals who were notified of the incident.
    - **Date/Time Notified**: Enter the date and time when the notification was made.

- **Impacted Location**
    - **Address**: Enter the geographical location address where the incident has occurred.
    - **City/State/Zip**: Enter the geographical location city, state, and zip code where the incident has occurred.

- **Impacted User Contact Information**
    - **Name***: Enter the name(s) of any user(s) impacted by the incident.
    - **Email***: Enter the email address(es) of any user(s) impacted by the incident.
    - **Office Number***: Enter the office telephone number(s) of any user(s) impacted by the incident.
    - **Cell Number**: Enter the mobile telephone number(s) of any user(s) impacted by the incident.
    - **Dept/OPDIV***: Enter the name(s) of the department or OPDIV(s) of any user(s) impacted by the incident.
    - **UserID**: Enter the User ID(s) of any user(s) impacted by the incident.

2.2. INCIDENT CATEGORY

This section allows the user to classify the incident appropriately based on categories outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*, as outlined in the table below. Select the appropriate checkbox based on the type of incident being reported. If multiple incident categories are involved (e.g., an unauthorized individual accessing a system containing Personally Identifiable Information (PII)), select all related checkboxes. Based on the category(ies) selected, the CSIR form further directs the user to complete the appropriate section(s) of the form.

Table 1: Incident Categories

Category	Name	Description	HHS Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national and international exercises, and approved activity testing of internal/external network defenses or responses	Not Applicable; this category is for each agency's internal use during exercises
CAT 1	Unauthorized Access	An individual gains logical or physical access, without permission, to a federal agency network, system, application, data, or other technical resource	Within 1 hour of discovery/detection
CAT 2	Denial of Service (DoS)	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources; this activity includes being the victim of or participating in the attack	Within 2 hours of discovery/detection if the successful attack is ongoing and the agency/OPDIV is unable to successfully mitigate activity
CAT 3	Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. (Note: Agencies are NOT required to report within 1 hour for malicious logic that has been successfully quarantined by anti-virus (AV) software)	Within 1 hour of discovery/detection if widespread across agency/OPDIV. The total count of all CAT 3 incidents and events, (including those successfully quarantined), should be rolled up and reported monthly
CAT 4	Improper Usage	An individual violates acceptable use of any network or computer use policy	Weekly
CAT 5	Scans/Probes/ Attempted Access	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit; this activity does not directly result in a compromise or DoS	Monthly (fifth day of the month for the previous month's data) Note: If the system is classified, report within 1 hour of discovery
CAT 6	Investigations	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review	Weekly
CAT PII	PII or Protected Health Information (PHI)	Possible or confirmed compromise of: "Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as a name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual." (Office of Management and Budget (OMB) Memorandum [M] 06-19)	Any incident that involves compromised PII must be reported within 1 hour of detection regardless of the incident category reporting timeframe
CAT RE	Reportable Event	A reportable event is anything that involves: (1) a matter that a reasonable person would consider a violation of criminal, civil or administrative laws applicable to any Medicare contract or Federal health care program; or (2) integrity violations, including any known probable or suspected violation of any Medicare contract term or provision. A reportable event may be the result of an isolated event or a series of occurrences. Reportable events that are subject to reporting under these procedures include reportable events that occur at the contractor or any of its subcontractors, consultants, vendors or agents. If the reportable event results in an overpayment, relating to either Trust Fund payments or administrative costs, the report must describe the overpayment with as much specificity as possible, as of the time of the due date for the submission of the report. Many events are reported for inappropriate use of resources or reflect situations that do not fall under the definitions above.	Weekly

2.3. TYPE OF DEVICE INVOLVED IN INCIDENT

This section provide an overview of the device(s) involved in or affected by the incident, including information about both the attacker and the victim, the anti-virus software installed on the device(s), and the encryption status of the device(s). The Type of Device Involved in Incident* is a required field in the CSIR.

- **Devices ***: Select the type of device and/or operating system involved in the incident. If multiple devices are involved, select all related checkboxes. The CMS standard device types and operating systems are as follows:

Blackberry	E-mail	PDA	Windows
Cell phone	Hard Drive (External)	Server	Linux
Computer (Non-specific)	Hard Drive (Internal)	Tape/DLT/DASD	Unix
Computer Files	Laptop	USB Thumb Drive	Mac
Desktop Computer	Paper Documents	Other_____	
Domain Controller	CD/DVD		

- **Source IP/Network (Attacker)**: Enter the network Internet protocol (IP) address of the attacker, if known.
- **Destination IP/Network (Victim)**: Enter the network IP address of the victim, if known.
- **Source Computer Name (if known)**: Enter the domain name service (DNS) and/or Active Directory (AD) / Windows Internet Naming Service (WINS) name of the attacker, if known.
- **Destination Computer Name (if known)**: Enter the DNS/AD/WINS name of the victim, if known.
- **Anti-virus vendor**: Enter the vendor name for any anti-virus software involved, if known.
- **Anti-virus Signature Version Number**: Enter the version number, date, and time of the anti-virus software signature, if known.
- **Encryption**: Select "Yes" if the device involved was encrypted. If the device involved was not encrypted or the encryption status is unknown, select "No." **Encryption Type/Vendor**: If the device was encrypted, enter the type or vendor of the encryption software; if the device was not encrypted, enter "n/a." If t**he encryption status i**s unknown, provide as much information as possible so that the CMS CSIRT can do the research necessary to determine encryption status.

2.4. SECTION A – LOST/STOLEN ASSET

An asset is any physical computing device or equipment, such as a laptop, Blackberry, disk, or flash drive. This section must be completed if the "Lost/Stolen Asset" checkbox was selected under the Incident Category subsection.

- **PII Involved**: If PII was contained on the lost or stolen asset, select "Yes." If PII was not contained on the lost or stolen asset, select "No." If it is unknown whether PII was contained on the lost or stolen asset, select "Unknown."
    - **Note**: If "Yes" or "Unknown" is selected, the user must also complete Section B.
- **Brief Description**: Enter a description of the lost or stolen asset, including (to the extent of the reporting individual's knowledge) any actions taken, the asset brand/model, the date and time of the loss or theft, the location of the loss or theft, and whether PII was potentially exposed or compromised.

2.5. SECTION B – PII RELATED INCIDENT

Note: Any incident involving PII in electronic or physical form must be reported to the CMS CSIRT within 1 hour of discovery. Suspected and confirmed breaches should be reported identically.[1]

A "breach" is defined in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, as "The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users or authorized purpose have access or potential access to personally identifiable information, whether physical or electronic." Types of breaches include, but are not limited to:

- Loss of federal, contractor, or personal electronic devices storing PII (e.g., laptops, cell phones that can store data, disks, thumb/flash drives, compact discs);
- Sharing paper or electronic documents containing PII with unauthorized individuals;
- Posting PII to a public website either intentionally or unintentionally;
- Mailing hard copy documents containing PII to an incorrect address; and
- Leaving documents containing PII exposed in an area where unauthorized individuals could read, copy, or move for future use.

[1] HHS Incident Notification Process, November 30, 2006 - http://intranet.hhs.gov/infosec/docs/incident_mgmt/Incident_Notification_Process.pdf

This section must be completed if the "PII Related Incident" checkbox was selected under the Incident Category subsection, or if the "Yes" or "Unknown" checkbox was selected in the "PII Involved" field of Section A.

- **Breach Category**: Select the appropriate checkbox based on the type of incident involving PII compromise.
- **Number of Individuals whose PII was Lost or Compromised**: Enter the exact number of individuals whose PII was lost or compromised. If the exact number is not known, select the "Unknown" checkbox and include an estimate in this field, if possible.
- **Brief Description**: Enter a brief description of the PII compromise following the bulleted guidance. Be sure to include the format of the PII (e.g., email, web, database), the population affected, whether the PII was lost or stolen, the summary time stamp, and any actions taken.
- **High-level Executive Summary**: Enter a high-level summary of incident elaborating in bulleted format.
- **Detailed Incident Description**: Enter a detailed description of incident with time stamps.

2.6. SECTION C – MALICIOUS CODE

This section must be completed if the "Malicious Code" checkbox was selected under the Incident Category subsection.

- **Malware Type**: Select the appropriate checkbox based on the type of malware involved in the incident.
- **Operating System**: Select the appropriate checkbox based on the type of operating system affected.
- **Name of Malware (if known)**: Enter the name of the malware, if known.
- **Action Against Malware**: Select the appropriate checkbox based on which action was taken against the malware.
- **Was effected node properly patched prior to event**: Indicate whether the affected node was properly patched prior to the incident.
- **Description of current actions taken (if any)**: Provide a brief description of any actions taken to mitigate the incident.

2.7. SECTION D – UNAUTHORIZED ACCESS

This section must be completed if the "Unauthorized Access" checkbox was selected under the Incident Category subsection.

- **Describe Violation**: Provide a brief summary of the violation, including the date and time when the access occurred.

- **Actions taken (if any)**: Provide a brief description of any actions taken to mitigate the incident.

2.8. SECTION E – IMPROPER USAGE/POLICY VIOLATION

This section must be completed if the "Improper Usage" checkbox was selected under the Incident Category subsection.

- **Type of Violation**: Select the appropriate checkbox based on the type of violation involved in the incident.
- **Describe Violation**: Provide a brief description of the violation, including the name and version of the software, uniform resource locator (URL) address, and any other information if applicable, involved.
- **Describe Incident**: Provide a brief description of the violation, including the date and time that the violation occurred.
- **Actions taken (if any)**: Provide a brief description of any actions taken to mitigate the incident.

2.9. SECTION F – EXERCISE/NETWORK DEFENSE TESTING

This section must be completed if the "Exercise/Network Defense Testing" checkbox was selected under the Incident Category subsection.

- **Testing Approval Provided By**: Enter the name of the individual who approved the testing.
- **Contact Number**: Enter the telephone number of the individual who approved the testing.
- **Testing Time Period**: Enter the time period during which the testing took place.
- **Brief Description**: Provide a brief description of the networks/systems tested and the reason for testing.

2.10. SECTION G – DENIAL OF SERVICE, SCANS/PROBES/ATTEMPTED ACCESS, & INVESTIGATIONS

This section must be completed if the "Denial of Service," "Scans/Probes/Attempted Access," or "Investigations" checkbox was selected under the Incident Category subsection.

- **Describe Violation**: Provide a brief description of the violation, including the date and time that the incident occurred.
- **Actions taken (if any)**: Provide a brief description of any actions taken to mitigate the incident.

2.11. SECTION H – REPORTABLE EVENTS

This section must be completed if the "Reportable Events" checkbox was selected under the Incident Category subsection.

- **Describe Violation**: Provide a brief description of the violation, including the date and time that the reportable event occurred. Provide the quantified overpayment or an estimated amount of the overpayment, the nature of the overpayment, the reasons for the overpayment, and the period of the overpayment.
- **Actions taken (if any)**: Provide a brief description of any actions taken to mitigate the reportable events and overpayment involved.
- **If the Reportable Event Results in an Overpayment**: Provided a description of the following:
    - Amount of the overpayment;
    - If the overpayment has not yet been quantified, the contractor must provide its best estimate of the amount of the overpayment;
    - The nature of the overpayment and the reason for the overpayment;
    - Time period of the overpayment;
    - Any corrective action taken, or intended to be taken, by the contractor;
    - Repayment of the overpayment, which must be done in accordance with CMS policies and procedures.

3. ROLES AND RESPONSIBILITIES

The roles and responsibilities that follow are intended to be advisory and illustrative of possible incident handling and reporting. Owners of CMS systems and business functions, including their contract officers, contract specialists, project owners, government task leads and subordinate managers have a primary responsibility to be aware of and implement these procedures in their areas, particularly with respect to timely and accurate reporting in accordance with section 2.2 of this document. Once reported, entities like the Senior Core Leadership for Breach Notification, the Breach Analysis Team (BAT), the IHCM Team or an IRT may be engaged or activated to direct the management of the incident through the incident response phases.

3.1. SYSTEM USER

3.1.1 DESCRIPTION

CMS employees or contractor staff conducting CMS business functions.

3.1.2 RESPONSIBILITIES

- Reports security incidents to the appropriate point of contact (POC) i.e., CMS IT Service Desk, Business Owner or System Technical Support as directed by the business organization.

- Works with CMS IT Service Desk, Business Owner or System Technical Support in information gathering and incident determination activities.

3.2. CMS IT SERVICE DESK

3.2.1 DESCRIPTION

CMS or contractor staff, which acts as the first POC for reported operational problems and security incidents. The CMS IT Service Desk can be contacted via phone at (410) 786-2580 and by sending an email to CMS_IT_Service@cms.hhs.gov.

3.2.2 RESPONSIBILITIES

- Acts as the first POC for security incidents or anomalies and records information provided by the System User, Business Owner or System Technical Support, depending on alert source.
- Generates a Remedy ticket to document the incident for CMS records.
- Determines if incident is related to PII.
- Immediately refers security incident to the CSIRT.

3.3. CMS COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

3.3.1 DESCRIPTION

CMS contractor staff that acts as the focal point for reporting, monitoring and tracking to closure of reported operational problems and security incidents.

3.3.2 RESPONSIBILITIES

- Generates alert to DHHS Secure One and issues the CSIR form contained in the *CMS IS Incident Handling and Breach Analysis/Notification Template* to the System User, Business Owner or System Technical Support to complete. Copies CMS Chief Information Officer (CIO), Chief Information Security Officer (CISO) and the System Technical Support and/or Business Owner on all alerts sent to Secure One. The CMS Senior Official for Privacy and the Beneficiary Confidentiality Board (BCB) staff are copied only on alerts involving suspected or actual compromise of personally identifiable information.
- Provides ad hoc and periodic reports on security incidents and handling of advisories to the CIO, CISO or the CMS Senior Privacy Official.
- Executes responsibilities of System Technical Support and/or Business Owner for selected incidents as requested by the Director, Enterprise Data Center Group (EDCG).

3.4. SYSTEM TECHNICAL SUPPORT

3.4.1 DESCRIPTION

System Technical Support may be appointed by a Business Owner of a system, or a system developer/maintainer as a lead POC for incident handling and response. Individuals assigned as the System Technical Support may include system administrators, system maintainers, security staff for the General Support System or Major Application(s) affected by the security incident, Component Information System Security Officer (ISSO), or External Business Partner contact. Staff may be a combination of CMS and contractor personnel operating/maintaining the affected system(s). System Technical Support may also be managers and supervisors of CMS systems or business functions, i.e., the Business Owner, who retains this responsibility versus delegating it.

3.4.2 RESPONSIBILITIES

- Report the incident to the CMS IT Service Desk, see section 3.2.1, if not already reported.
- Serves as the system or function focal point for security incidents for triage, response and recovery phases.
- Prepares component-level plans and procedures to address security incidents, in accordance with this document, and information security standard operating procedures.
- Provides technical support and advice for incident handling, impact assessment, and technical system management, including actions to be taken if circumstances are not covered by standard operating procedures.
- Oversees the development and implementation of the CMS Corrective Action Plan(CAP), if applicable.
- Coordinates evaluation and categorization of security advisories/information.
- Refers security advisories/information involving the CMS business function to the IHCM Team, if appropriate.
- Implements changes to information systems to minimize newly discovered vulnerabilities resulting from a security incident.
- Reports incident status/resolution information to DHHS Secure One, the IHCM Team, if activated, the Senior Core Leadership for Breach Notification (if applicable), the Breach Analysis Team POC (if applicable) and the CMS IT Service Desk in accordance with this document.
- Recommends updates and closings of incident and event tickets for all categories.
- Updates and transfers ticket to IHCM Team for incidents and events as appropriate.
- Assists IHCM Team and the IRT in information gathering, forensics and reporting activities.
- Initiates escalation procedures as directed; e.g., for incidents at an Enterprise Data Center, sends electronic notification/page to the pre-determined government/contractor staff, when appropriate, for notification during the investigation, analysis, countermeasures and follow-up phases.
- Upon the decision of the Senior Core Leadership for Breach Notification or the Administrator, implements approved Breach notification process, e.g., mailings to individuals and press releases

3.5. BUSINESS OWNER

3.5.1 DESCRIPTION

A Business Owner is a component or individual who have primary ownership of a major CMS business function or process. Examples are Medicare contractors, Program Safeguard Contractors, Shared Systems, Quality Improvement Organizations, Survey & Certification, Medicare Advantage Contractors, Medicare Call Centers, Enterprise Data Centers, and organizations conducting CMS sponsored research. Business Owners are key to the handling of CMS security incidents. Either in partnership with System Technical Support or in the lead role, Business Owners direct the day-to-day handling of all incidents under guidance from the IHCM (if activated) and the Senior Core Leadership for Breach Notification (if applicable).

3.5.2 RESPONSIBILITIES

- Report the incident to the CMS IT Service Desk, see section 3.2.1, if not already reported.
- Appoint a management and staff POC for incident handling. This may be the component ISSO or his/her manager.
- Other responsibilities parallel those of the System Technical Support, but are directed at business functions generally supported externally to CMS, e.g., functions supported by contracts, agreements or memorandums of understanding.
- Oversees the PHI and PII corrective action plan (if applicable).
- Provides a management representative to the BAT and participates at the executive level in the IHCM (if activated) and the Senior Core Leadership Breach Management (if applicable).
- Upon the decision by the Senior Core Leadership or Administrator, implements approved Breach notification processes, e.g., mailings to individuals, press releases.
- Provides guidance to business partners, if needed, for reporting to the CMS IT Service Desk, e.g., a Business Owner may direct partners to submit via a Central Office or Regional Office contact before the incident is sent to the CMS IT Service Desk.
- Informs the Office of Acquisitions and Grants Management if the incident constitutes a contract violation.

3.6. INCIDENT RESPONSE TEAM (IRT)

3.6.1 DESCRIPTION

The IRT is a logical group assembled by either the Business Owner or System Technical Support POC to handle security incidents. Team membership will vary according to the nature of the security incident, systems and applications affected by the security incident, associated components with business and technical responsibilities concerning the system affected by security incident, and the need to involve contractors providing security services/support and/or other federal agency's staff. The Business Owner or System Technical Support will determine the need for an IRT. Generally, the IRT is activated by the owner of the system or business function compromised. The Director, EDCG, may utilize the CMS CSIRT as his/her System

Technical Support or and IRT to handle incidents involving general support systems for which he/she is the owner.

3.6.2 RESPONSIBILITIES

- Performs a variety of incident handling activities throughout the Security Incident Response phases, depending on the category level and nature of security incident.

3.7. INCIDENT HANDLING COORDINATION AND MANAGEMENT (IHCM) TEAM

3.7.1 DESCRIPTION

The IHCM is a multi-component team that provides support and management direction to more serious security incidents. Members may include but are not limited to the CMS CIO, the CMS CISO, the CMS Senior Official for Privacy, the CMS Chief Financial Officer (CFO), the CMS Press Officer, the Director, External Affairs, the Director, Office of E-Health Standards and Services, as well as the Owner(s) of the Business function or system compromised. The IHCM is activated by the CMS CIO who will also direct membership. Activation may be informal, e.g., by e-mail, directing a level and membership of the IHCM Team. The IHCM would not be responsible for Breach analysis or notification for beneficiaries. These functions are supported by the BAT and Senior Core Leadership for Breach Notification.

3.7.2 RESPONSIBILITIES

- Leads incident handling coordination activities for incidents and assesses security incident's impact and priority.
- Correlates information across multiple components' POC and Business Owner or System Technical Support.
- Coordinates information and evidence gathering, forensics effort, and follow-up activities.
- Updates and closes incident tickets for security incidents involving successful penetrations.
- Prepares and disseminates incident updates and reports to the CIO, and other entities including DHHS Secure One, as appropriate for the security priority level.

3.8. SENIOR CORE LEADERSHIP FOR BREACH NOTIFICATION

3.8.1 DESCRIPTION

This group represents CMS' executive level management, similar to HHS' PII Breach Response Team, and is comprised of: the CIO; the CISO; Senior Agency Official for Privacy; CFO; Office of General Counsel; Director, Office of Beneficiary Information Services; Director, Office of E-Health Standards and Services, Director, Office of External Affairs; and Business Owner Component Executive. The Senior Core Leadership:

3.8.2 RESPONSIBILITIES

- Oversees the risk analysis and breach notification process, including the final determination and/or recommendation of whether to notify (e.g., public notice, notification to individuals, other parties such as providers and/or other federal agencies).
- Provides a management level representative and one senior staff person to support the BAT for each executive management component (above).
- Approves BAT recommendations for individual incidents and/or obtains approval of such recommendations from the Office of the Administrator and/or Chief Operating Officer (COO).
- Approves all public notice(s) and individual notification materials.
- Keeps the Administrator and COO apprised of all significant events/activities and decisions.

3.9. BREACH ANALYSIS TEAM (BAT)

3.9.1 DESCRIPTION

The BAT is comprised of management designees and senior staff appointed by the Senior Core Leadership for Breach Notification with the exception the CIO, the CISO, and the Senior Official for Privacy would represent themselves in the BAT. The CMS Privacy Officer, staff from the BCB, and CMS CIO are also designated members. The manager representing the Business Owner component should be at the Group Director/Deputy level. The CIO is designated as the BAT chair.

3.9.2 RESPONSIBILITIES

- Analyzes the risk of identity theft or health insurance fraud in accordance with OMB requirements and Departmental guidelines. (OMB Memorandum M-07-16 provides detailed guidance including specific factors which an agency should consider in assessing the likely risk of harm caused by the breach.)
- Ensures the breach is reported to any other affected business or system owner, e.g., claims processing or program integrity for payment fraud.
- Conducts assessments of breaches in order to determine next steps, e.g., whether or not to notify, by what means (press releases, letters), and to whom (individuals, providers, other federal agencies), whether to offer credit protection services.
- Develops government cost estimates of notification and/or credit protection services.
- Drafts model breach notification letters and/or other materials in plain language, standardized to the extent possible, with specific tailoring on a case-by-case basis.
- Determines and recommends how the letter and/or public notice gets “rolled-out,” for example, by the agency, a contractor, another agency.
- Assists business owners prepare scripts for Medicare call center operations and/or frequently asked questions to post, if necessary.
- Coordinates recommendations submitted to the Senior Core Leadership for Breach Notification with the HHS PII Breach Notification Team.
- Investigates credit protection services/costs for business components.

3.10. CHIEF INFORMATION OFFICER (CIO)

3.10.1 DESCRIPTION

The CIO is responsible for the overall implementation and administration of the CMS Information Security Program.

3.10.2 RESPONSIBILITIES

- Provides overall incident handling direction for higher priority level security incidents.
- May authorize formation of an IHCM Team and appoint a lead component (usually the Owner of the Business function or system that is compromised).
- Provides guidance for decision-making activities for security incidents escalating beyond CMS boundaries and established policies.
- Participates as a member of the Senior Core Leadership for Breach Notification.
- Chairs the BAT and provides staff support as needed.

3.11. CMS SENIOR OFFICIAL FOR PRIVACY

3.11.1 DESCRIPTION

The Senior Official for Privacy is the individual designated with CMS to protect the information privacy rights of CMS employees and beneficiaries of Agency programs, and to ensure CMS has effective information privacy management processes to accomplish this important function.

3.11.2 RESPONSIBILITIES

- Provides overall direction to the BAT for incidents involving compromise of individually identifiable information.
- Participates as a member of the Senior Core Leadership for Breach Notification and the BAT.
- Provides BCB staff to support on-going BAT roles and responsibilities.
- Provides guidance on the impact of both PII and PHI incident/breach.
- Comments on proposed notification letters.

3.12. CMS CHIEF INFORMATION SECURITY OFFICER (CISO)

3.12.1 DESCRIPTION

The CISO assists the CIO in the implementation and administration of the CMS Information Security Program.

3.12.2 RESPONSIBILITIES

- Assists the CIO in the fulfillment of his/her incident handling responsibilities.
- Maintains coordination and communication with the DHHS CISO and DHHS Security One for incident reporting, tracking and closure.

- Provides overall incident handling direction for lower priority level incidents to System Technical Support or Business Owners, and recommendations to the IHCM for more serious incidents.
- Recommends to the CIO, Senior Privacy Official, and BAT staff to activate the BAT, if not already activated, to provide advice to the Senior Core Leadership for Breach Management on breech notification.
- Participates as a member of the BAT for incidents involving system attacks and/or penetration in which PII might be compromised.
- Serves as an ad hoc consultant of the BAT for other incidents, e.g., lost laptops, stolen hard drives, missing cartridges.
- Monitors recommendations from the BAT to the Senior Core Leadership for Breach Management, as well as updates to the HHS Secure One/PII Breach Response Team.
- Coordinates lessons learned type briefings of incidents for Business Owners and System Developers/Maintainers.

3.13. MANAGED SECURITY SERVICES PROVIDER (MSSP)

3.13.1 DESCRIPTION

Contractor staff composed of system engineers and subject matter experts that specialize in intrusion detection systems monitoring and management, firewall management, network and operating system security, malicious incident analysis and handling, and forensics analysis.

3.13.2 RESPONSIBILITIES

- Monitors 24x7 Intrusion Detection System (IDS) data collected from MSSP-supplied IDS sensors.
- Generates alerts and warnings for possible security incidents, as CMS' IDS managers.
- Provides security advisories to CMS as security incident prevention mechanism.
- Supports information gathering, analysis and forensics activities during the incident handling process.
- Provides technical advice and support in areas of expertise, remotely or on-site.

3.14. OTHER ENTITIES

3.14.1 DESCRIPTION

CMS Executive Leadership, DHHS Secure One, the Office of Inspector General's Computer Crime Unit and the United States Computer Emergency Readiness Team US-CERT).

3.14.2 RESPONSIBILITIES

- Provides DHHS and/or CMS with high-level direction and policies, and assistance for security incident response process.

4. SECURITY INCIDENT INFORMATION GUIDELINES

Actions taken during the incident response phases vary according to the category of incident. This section describes general guidelines for incident response phases for each incident security level category.

4.1. DOCUMENTATION

During the incident response phases, all analysts and administrators must keep a log of all actions taken to aid in incident handling, decision-making and reporting processes. The types of information that should be logged are:

- Dates and times of incident-related phone calls.
- Dates and times when incident-related events were discovered or occurred.
- Amount of time spent working on incident-related tasks.
- The entity or people the component has contacted or who have contacted the component.
- Names of systems, programs, or networks affected by the incident.
- Impact analysis.

The Business Owner or System Technical Support shall maintain a chronology of the significant activities.

All documentation must be provided to the CMS IT Service Desk and the DHHS Secure One upon a recommendation for closure of the incident.

4.2. INFORMATION RELEASE

Release of information during incident handling phases must be on a need-to-know basis. For all categories, when other entities would be notified of the incident, information release must be authorized, in consultation with CMS management. CMS will coordinate with legal and public affairs contacts for the affected entities if appropriate. Such direction may also come from the CIO/CISO or his/her designee, the IHCM or the Senior Core Leadership for Breach Notification.

4.3. BAT RECORDS

The BAT shall maintain a record of their recommendations, as well as summary information on the actions taken on individual incidents.

5. ESCALATION PROCEDURES

During the Alert Phase, a System User, Business Owner, System Technical Support, or MSSP analyst identifies and reports an actual or suspected security incident to the CMS IT Service Desk, Business Owner or System Technical Support, as appropriate for the business organization, so that a security incident ticket is created for tracking of the incident. During the response phases, the Business Owner or System Technical Support may subsequently form an IRT to assist on the incident response effort, as appropriate. Team membership will vary according to the category level and the nature of the security incident.

5.1. ACTION STEPS

- The CMS IT Service Desk records information provided by a System User, Business Owner, System Technical Support or MSSP, and opens a Remedy incident ticket. The CMS IT Service Desk immediately refers the security incident to the CMS CSIRT.
- The CMS CSIRT immediately notifies DHHS Secure One and provides the reporting person or entity with the CSIR form. The CIO, CISO and System Technical Support or Business Owner (as applicable), are copied on all notifications. The CMS Senior Agency Official for Privacy and BAT are copied on PII incidents.
- For security incidents, the Business Owner or System Technical Support verifies the occurrence of the reported or suspected security incident, determines the nature of the risk to CMS information or information systems or business function, and updates the incident ticket, if necessary.
- Business Owner or System Technical Support immediately notifies identified IRT contacts in accordance with the approved notification list.
- Based on the alert provided by the CMS IT Service Desk to DHHS Secure One, the CIO or CISO may activate the IHCM. The BAT is activated for PII incidents.

5.2. ACTION STEPS FOR SECURITY INCIDENTS AND SECURITY ADVISORY/INFORMATION

For security incidents and security advisory/information, the following additional steps may apply:

- IHCM Team gathers information from Business Owner or System Technical Support for incident reporting, and coordinates incident handling efforts if multiple systems/components are affected.
- Business Owner or System Technical Support develops a CAP to protect sensitive information and resolve system vulnerabilities. Business Owner or System Technical Support also tracks CAP and reports to IHCM Team after implementation.
- The CSIRT and/or Business Owner or System Technical Support notifies CIO of incident occurrence and impact, and issues periodic reports to the CIO, as appropriate
- Business Owner or System Technical Support keeps the CMS IT Service Desk/CSIRT and the IHCM Team (if activated) abreast of incident handling actions/progress and updates the incident ticket, as appropriate. Ad hoc progress reports to IHCM Team are issued, as required by the situation.
- Periodic reports are issued and/or prepared for the CIO and CISO, CMS upper management and outside entities, as appropriate; e.g., DHHS Secure One.
- The Business Owner or System Technical Support documents resolution information, including tally of systems affected, and updates and closes the security incident ticket as appropriate.
- The Business Owner or System Technical Support and/or CMS IT Service Desk/CSIRT prepares and disseminates reports to the CIO, CISO, and other entities, as dictated by policies and specific mandates.
- IHCM Team coordinates with Legal and Public Affairs contacts to authorize and prepare public relations statements or legal preparation of evidence, if appropriate.

- System Technical Support and/or the Business Owner implements BAT recommendations that have been approved by the Senior Core Leadership for Breach Notification.
- If a violation of the law is suspected, IHCM Team may notify the Office of Inspector General's Computer Crime Unit and submit a report to the US-CERT with a copy to the DHHS Secure One and CISO, or have the DHHS Secure One and CISO handle these notifications.

6. MONTHLY SUMMARY REPORTS

CMS must generate monthly reports for the DHHS Secure One. The CMS monthly report summarizes the past month's events and incidents, and may include changes to POC information, improvement suggestions, and other incident response issues of concern to CMS. The monthly summary report collects the following information:

- Viruses prevented;
- Probes and reconnaissance scans that were determined not to be causing a threat to critical system; and
- Additional information as required for the DHHS Secure One Department-wide data correlation efforts.

CMS' monthly report is due the fifth calendar day of each month (or the following workday) for events and incidents that occurred during the previous month. Since each incident is reported separately to the DHHS Secure One, incidents need only be included in summary totals in the monthly summary report. CMS should use the DHHS online monthly summary report located at **https://intranet.hisp.hhs.gov/hhs/public/**. Events should be categorized when reporting per the DHHS instructions.

7. SECURITY ALERTS

The following steps constitute the procedures used by the DHHS CISO to notify OPDIVs whenever an information security alert is available.
The DHHS CISO receives an information security alert from the following sources:

- By monitoring the GFIRST portal for notices, alerts, and inquiries from US-CERT.
- An OPDIV finding a potential threat to the department
- Another department within the government finding a potential threat

The DHHS CISO will formulate a communication clearly defining the issue, stating the risk of the threat, and providing instructions on what remedial steps need to be taken. The DHHS CISO will then take this communication and send it to the appropriate individuals via DHHS Secure One Support. The distribution list includes points of contact throughout CMS.

APPENDIX A: SAMPLE CMS COMPUTER SECURITY INCIDENT REPORT (CSIR)

Date/Time: _ April 16, 2009 4:25 p.m._____

Incident Tracking Number		
HHS	OPDIV	US CERT
CSIRC – 20090001		

*** = Required Information**

Reporting Individual Contact Information			
Name*		Email*	
Avery Mann		amann3@cdc.gov	
Office Number*	Cell Number	Dept/OPDIV*	UserID
770-555-6266	n/a	CDC	IEG4
Name(s) of Dept/OPDIV or individual notified of security incident:			
Dept/OPDIV	Name/Title		Date/Time Notified
HHS CSIRC	Mike Rosenwald/Analyst		04/16/2009 4:15 p.m.

Impacted Location*	
Address	City/State/Zip
1963 Street Address	Atlanta, GA 30391

Impacted User Contact Information			
Name*		Email*	
Spencer Hsu		shsu9@hhs.gov	
Office Number*	Cell Number	Dept/OPDIV*	UserID
770-555-7673	n/a	CDC	WJT8

Incident Category*	
☒ Lost/Stolen Asset (*Section A*)(Cat 0)	☐ Exercise/Network Defense Testing (*Section F*)
☒ PII Breach (*Section B mandatory*)	☐ Denial of Service (*Section G*) (Cat 2)
☐ Malicious Code (*Section C*) (Cat 3)	☐ Scans/Probes/Attempted Access (*Section G*) (Cat 5
☐ Unauthorized Access (*Section D*) (Cat 1)	☐ Investigations (*Section G*) (Cat 6)
☐ Improper Usage (*Section E*) (Cat 4)	☐ Reportable Events (*Section H*) (Cat RE)

Type of Device Involved in Incident*	
Devices	Operating System

Type of Device Involved in Incident*			
☐ Blackberry ☐ Cell phone ☐ Computer (Non-specific) ☐ Computer Files ☐ Desktop Computer ☐ Domain Controller	☐ E-mail ☐ Hard Drive (External) ☐ Hard Drive (Internal) ☒ Laptop ☐ Paper Documents ☐ CD/DVD	☐ PDA ☐ Server ☐ Tape/DLT/DASD ☐ USB Thumb Drive ☐ Other_____	☐ Windows ☐ Linux ☐ Unix ☐ Mac

Source IP/Network (Attacker)	Destination IP/Network (Victim)
158.42.068.77	103.64.128.55
Source Computer Name (*if known*)	Destination Computer Name (*if known*)
n/a	n/a
Anti-virus vendor	Anti-virus Signature Version Number
Symantec	Symantec Endpoint Protection V11

Encryption		Encryption Type/Vendor
☒ YES	☐ NO	Check Point

Section A: Lost/Stolen Asset

PII Involved? (if so, complete Section B)	Brief Description Include actions taken, asset brand/model, date and time, location of theft/damage and whether or not PII was exposed
☒ YES ☐ NO	
Theft of laptop was discovered on April 16, 2009 at 4:00 p.m. from Mr. Hsu's car in a Bank of America parking lot. Laptop is an encrypted Lenovo T61 machine containing PII.	

Section B: PII Related Incident

Breach Category		
☐ Document Theft ☒ Hardware/Media Theft ☐ Document Loss ☐ Hardware/Media Loss	☐ Document Lost in Transit ☐ Hardware/Media Lost in Transit ☐ Improper Usage ☐ Unintended Manual Disclosure ☐ Unintended Electronic Disclosure	☐ Unauthorized Access ☐ Hacking or IT Incident ☐ Document sent to Wrong Address

Number of PII Lost or Compromised List Number below
Exact number of PII: _____ Otherwise check: ☒ Unknown
Brief Description: Ensure to include the format of the PII (i.e. email, web, database, etc), population effected, lost/stolen, summary time stamp and the actions taken if any.

Laptop Theft - CDC (April 16, 2009)

- Theft of laptop was discovered on April 16, 2009 at 4:00 p.m. from Mr. Hsu's car in a Bank of America parking lot. Laptop is an encrypted Lenovo T61 machine containing PII.
- Mr. Hsu is a CDC employee.
- PII was owned by individuals involved in a CDC case study.
- Compromised PII involves name, address, date of birth, SSN, and medical history.
- An unknown number of individuals are impacted. CDC will update with number by 5:30 p.m. on April 16, 2009.
- Incident is under investigation.
- Involved individuals include the CDC employee and the CDC case study participants.
- Law enforcement is involved in the investigation; notice will be sent to the participants informing of the compromise; credit monitoring will be offered through Equifax.

High-level Executive Summary
• Laptop stolen containing PII • Laptop has installed security encryption • Compromised/exposed PII under the management of the CDC • CDC to provide extent of exposure on April 16, 2009

Detailed Incident Description
• Laptop discovered stolen at 4:00pm • Incident reported at 4:15pm • CSIRC – 20090001 assigned at 4:25pm • CDC to provide extent of exposure at 5:30pm

Section C: Malicious Code

Malware Type (Check One)		Operating System?
☐ Worm	☐ Denial of Service (DoS)	☐ Windows
☐ Virus	☐ Other _____	☐ Linux
☐ Trojan	_____	☐ Unix
☐ Buffer Overflow	_____	☐ Mac

Name of Malware if known

Action taken regarding Malware?			Prior to Event, was effected node properly patched?	
☐ Quarantined	☐ Cleaned	☐ Left Alone	☐ Yes	☐ No

Description of current actions taken (if any):

Section D: Unauthorized Access

Describe Violation

Actions taken (if any)

Section E: Improper Usage/Policy Violation

Type of Violation					
(P2P) File Sharing	Instant Messenger	Inappropriate Web sites	Remote Access	Unapproved Software	*Other* (Describe)
☐	☐	☐	☐	☐	
Describe Violation: (i.e. software name and version, URL address if applicable)					
Describe Incident					
Actions taken (if any)					

Section F: Exercise/Network Defense Testing

Testing Approval provided by	Contact Number	Testing Time Period
Brief Description: Include reason for testing and the networks and systems tested.		

Section G: Denial of Service, Scans/Probes/Attempted Access, & Investigations

Describe Violation
Actions taken (if any)

Section H: Reportable Events

Describe Violation
Actions taken (if any)
If Reportable Event Results in an Overpayment Provide Description

APPENDIX B – ABBREVIATION AND ACRONYMS

AD	Active Directory
BAT	Breach Analysis Team
BCB	Beneficiary Confidentiality Board
CAP	Corrective Action Plan
CAT	Category
CD	Computer Disk
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
COO	Chief Operations Officer
CSIR	Computer Security Incident Report
CSIRC	Computer Security Incident Response Center
CSIRT	Computer Security Incident Response Team
DASD	Direct Access Storage Device
DEPT	Department
DHHS	Department of Health and Human Services
DLT	Digital Linear Tape
DNS	Domain Name Service
DoS	Denial of Service
DVD	Digital Video Disk
EDCG	Enterprise Data Center Group
FISMA	Federal Information Security Management Act
GFIRST	Government Forum of Incident Response and Security Teams
ID	Incident Identification
IDS	Intrusion Detection System
IP	Internet Protocol
IRT	Incident Response Team
IS	Information Security
ISSO	Information System Security Officer
IT	Information Technology
IHCM	Incident Handling Coordination and Management
NIST	National Institute of Standards and Technology
MSSP	Managed Security Services Provider
OPDIV	Operating Division
OMB	Office of Management and Budget
P2P	People to People
PDA	Personal Digital Assistant
PHI	Protected Health Information
PII	Personally Identifiable Information
POC	Point of Contact
SP	Special Publication
TCP/IP	Transmission Control Protocol/Internet Protocol

WINS	Windows Internet Naming Service
URL	Uniform Resource Locator
USB	Universal Serial Bus
US CERT	United States Computer Emergency Readiness Team