CENTERS for MEDICARE & MEDICAID SERVICES
Enterprise Information Security Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Risk Management Handbook
Volume III
Standard 7.1

Incident Handling and Breach Notification

FINAL
Version 1.0
December 6, 2012

Document Number: CMS-CISO-2012-vII-std7.1

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *INCIDENT HANDLING AND BREACH NOTIFICATION* VERSION 1.0

1. Baseline Version. This document, along with its corresponding *Risk Management Handbook (RMH)*, Volume II Procedure, replaces *CMS Information Security (IS) Incident Handling and Breach Analysis/ Notification Procedure*, dated December 3, 2010.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURE

(This Page Intentionally Blank)

1 INTRODUCTION

CMS must be able to respond to computer security-related and/or privacy-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

This *Risk Management Handbook* Volume III, Standard 7.1, *Incident Handling and Breach Notification* standard, along with the companion procedures of the RMH Volume II, Procedure 7.2, *Incident Handling,* supersedes the *CMS Information Security (IS) Incident Handling and Breach Analysis/Notification Procedure* dated December 3, 2010.

1.1 BACKGROUND

1.1.1 SECURITY EVENT

A *Security Event*[1] is an observable occurrence in a network or system (e.g., known or suspected penetrations of information Technology (IT) resources, probes, infections, log reviews), or any occurrence that potentially could threaten CMS data confidentiality, integrity, or availability.

1.1.2 REPORTABLE EVENT

A *Reportable Event* is any activity or occurrence that involves:

- 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[2].
- Integrity violations, including any known, probable, or suspected violation of any Medicare contract term or provision.
- A matter considered to have an "adverse" impact on the IT system/infrastructure or CMS data confidentiality, integrity, or availability. Examples of specific events that should be reported include (but are not limited to):
  - Unauthorized access to or use of sensitive data for illegal purposes.
  - Unauthorized altering of data, programs, or hardware.
  - Loss of mission-essential data (i.e., patient, financial, benefits, legal, etc.).
  - Environmental damage/disaster (greater than $10,000) causing loss of IT services or data, or which may be less than $10,000 in damage yet affect CMS' ability to continue *any* day-to-day functions and operations.
  - Infection of sensitive systems, firmware, or software by malicious code (i.e., Viruses, Worms and Trojan Horses, etc.).

[1] *Event* is defined in HHS-IRM-2000-0006, *Policy for Establishing an Incident Response Capability.*
[2] For purposes of this document, the term *federal health care program* means any plan or program that provides health benefits, whether directly, through insurance, or otherwise, which is funded directly, in whole or in part, by the United States Government (other than the health insurance program under chapter 89 of U.S. Code Title 5).

- Perpetrated theft, fraud, vandalism, and other criminal computer activity that did, or may, affect the organization's capabilities to continue day-to-day functions and operations.
- Telecommunications/network security violations, i.e., networks (including local area networks [LANs], metropolitan area networks [MANs], and wide area networks [WANs]) that experience service interruptions that cause an impact to an indefinite number of end users.
- Unauthorized access to data when in transmission over communications media.
- Loss of system availability affecting the ability of users to perform the functions required to carry out day-to-day responsibilities.
- Root-level attacks on networking infrastructure, critical systems, or large, multi-purpose, or dedicated servers.
- Compromise (or disclosure of account access information) of privileged accounts on computer systems.
- Compromise (or disclosure of account access information) of individual user accounts or desktop (single-user) systems.
- Denial-of-service attacks on networking infrastructure and systems.
- Attacks launched on others from within organizational boundaries or systems.
- Scans of internal organizational systems originating from the Internet or from within the organizational boundaries.
- Any criminal act that may have been committed using organizational systems or resources.
- Disclosure of protected data, including paper disclosure, email release, or inadvertent posting of data on a web site.
- Suspected information-technology policy violation.

A *Reportable Event* may be the result of an isolated event or a series of occurrences. *Reportable Events* under these procedures include events that occur at CMS federal sites, contractor/ subcontractor sites/systems, 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.

Security events that may consist of an observable occurrence in a network or system (e.g., detected probes, infections prevented, log reviews, etc.), that do not threaten system integrity, are ***not*** considered *Reportable Events* unless they may be reasonably associated with other incidents, Reportable Events, or breaches. CMS categorizes these events in a monthly report to the Department of Health and Human Services (HHS) (hereafter referred to as the "Department" or "HHS") *Cybersecurity Program*[3] as follows:

- *Malicious Code Prevented*: Viruses were prevented and did not cause any harm to any system.

[3] Additional information on the *HHS Information Security and Privacy Program* and applicable contact information can be found at http://www.hhs.gov/ocio/securityprivacy/index.html.

- *Probes and Reconnaissance Scans Detected*: Probes and scans were detected but did not pose a serious threat to a CMS system.
- *Inappropriate Usage*: Misuse of computing resources by an otherwise authorized individual.
- *Other*: Cannot be categorized under any of the above and do not threaten system integrity.

There are many events that may be flagged as inappropriate use of resources, but reflect situations that do not fall under the definitions associated with incidents, Reportable Events, or breaches. In such cases, reporting should be made through applicable contractual resources, or through appropriate *Federal Fraud, Waste, and Abuse* reporting channels[4].

1.1.3 PRIVACY INFORMATION

Privacy is the right of an individual to control their *own* personal information, and not have it disclosed or used by others without permission. At CMS, we are charged with protecting *other people's* private information—that of every citizen (or legal resident) beneficiary utilizing benefits the vast Medicare/Medicaid program, as well as many subsidiary programs.

Confidentiality is the obligation of another party to respect privacy by protecting personal information they receive, and preventing it from being used or disclosed without the subject's knowledge and permission. Again, at CMS we are charged with protecting the confidentiality of *other people's* citizen-beneficiary information. A *breach* of that confidentiality is not simply a failure of a "technical control", it is a basic failure of CMS to meet its obligation to protect the individual citizen. Moreover, unlike the banking industry where *financial* compensation is a readily-available remedy to a breach, private medical information cannot be simply replaced with something of "similar value", or by simply *closing* an account, and *opening* a new (better protected) one. Once a *privacy* breach occurs, the ramifications can be far-reaching and long lasting—with no readily available "patch" to undo the damage (we cannot simply *replace* one *violated* health record with a *brand new* one.)

Security is the means used to protect the confidentiality of personal information through physical, technical, and administrative safeguards.

***Privacy* is the "business objective" of *security*.** The core of the relationship between *information security* and *information privacy* lies in the fact that *security*, or lack of it, is *the* determinant of the level of *privacy* that a system or infrastructure can assure. If there is a breach of computer security, it has a corresponding negative effect on the *confidentiality*, *integrity*, and *availability* of the information therein. Inadequate *security* leads directly to loss of *privacy*. Therefore, if privacy is the "business objective", then security is the "functional requirements" necessary for an IT system to meet those "business objectives".

1.1.3.1 PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a

[4] Medicare fraud may be reported at http://oig.hhs.gov/fraud/report-fraud/index.asp.

specific individual, such as date and place of birth, mother's maiden name, etc.[5]. PII also includes *individually identifiable health information* as defined by the *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, Privacy Rule (45 CFR Section 164.501[6]). PII is also often referred to as *personally identifiable data* or *individually identifiable information*.

1.1.3.2 PROTECTED HEALTH INFORMATION (PHI)

Protected Health Information[7] (PHI) is *individually identifiable health information* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

Individually Identifiable Health Information is a subset of health information, including demographic data collected concerning an individual that:

- Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse.
- Relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual, and meets either of the following:
  - Identifies the individual.
  - There is a reasonable basis to believe the information can be used to identify the individual.

The HIPAA Privacy Rule excludes from the definition of PHI individually identifiable health information that is maintained in education records covered by the *Family Educational Right and Privacy Act* (as amended, 20 U.S.C. 1232g) and records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records containing individually identifiable health information that are held by a covered entity in its role as an employer[8].

The HIPAA *Privacy Rule* covers PHI in any medium (including paper) while the HIPAA *Security Rule* covers PHI in electronic form (ePHI) only.

1.1.3.3 DE-IDENTIFIED HEALTH INFORMATION

With those definitions in place, what information (or data) *elements* comprise PHI such that, if they were removed, the above definition of individually identifiable health information would

[5] PII is defined in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*
[6] Text of the HIPAA legislation is available at http://www.gpo.gov/fdsys/pkg/CRPT-104hrpt736/pdf/CRPT-104hrpt736.pdf.
[7] PHI is defined in 45 C.F.R. §160.103, available at http://edocket.access.gpo.gov/cfr_2004/octqtr/pdf/45cfr160.103.pdf.

not apply? The answer is in the HIPAA de-identification use standard[9] and its two implementation specifications[10] of the HIPAA *Privacy Rule*.

There are no restrictions on the use or disclosure of *de-identified health information*. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two specifications for de-identifying *individually identifiable health information*; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and *is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual*.

The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the *safe harbor* method of de-identification:

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census:
    a. The geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people.
    b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers

[9] *Uses and disclosures of de-identified protected health information* is discussed in 45 C.F.R. §164.502(d)(2), and is available at http://edocket.access.gpo.gov/cfr_2010/octqtr/pdf/45cfr164.502.pdf.
[10] The *standards for de-identifying PHI* is discussed in 45 C.F.R. § 164.514, and is available at http://edocket.access.gpo.gov/cfr_2002/octqtr/pdf/45cfr164.514.pdf.

13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voiceprints
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met

In *addition to the removal of the above-stated identifiers*, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information.

1.1.3.4 FEDERAL TAX INFORMATION

Internal Revenue Code (IRC), Section 6103(p)(4)(D) requires that agencies receiving *Federal Tax Information (FTI)* provide appropriate safeguard measures to ensure the confidentiality of the FTI. The IRC provides the following definitions regarding FTI:

1. **Federal Tax Information (FTI)**: The term "Federal Tax Information" or FTI, includes the combined definitions of the terms *return, return information,* and *taxpayer return information.*

   Generally, Federal Tax Returns and return information are confidential, as required by IRC Section 6103. The information is used by the Internal Revenue Service (IRS) to ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality.

2. **Return**: Any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of the IRC which is filed by the Secretary of the Treasury by, on behalf of, or with respect to any person, and any amendment or supplemental to, or part of the return filed.

3. **Return Information**:

   a. A taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over-assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary of Treasury with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense, and

   b. Any part of any written determination or any background file document relating to such written determination [as such terms are defined in section 6110 (b)] which is not open to public inspection under section 6110, but such term does not include data in a form which

cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. Nothing in the preceding sentence, or in any other provision of law, shall be construed to require the disclosure of standards used or to be used for the selection of returns for examination, or data used or to be used for determining such standards, if the Secretary of Treasury determines that such disclosure will seriously impair assessment, collection, or enforcement under the internal revenue laws.

4. **Taxpayer Return Information**: The term "taxpayer return information" means return information as defined in paragraph 3 above which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates.

5. **Taxpayer identity**: The term "taxpayer identity" means the name of a person with respect to whom a return is filed, his mailing address, his taxpayer identifying number (as described in section 6109), or a combination thereof.

6. **Inspection**: The terms "inspected" and "inspection" mean any examination of a return or return information.

7. **Disclosure**: The term "disclosure" means the making known to any person in any manner whatever a return or return information.

Internal Revenue Code section 7213 specifies that willful unauthorized *disclosure* of returns or return information by an employee—whether federal or state—former employee, or contractor employee, is a ***felony***. The penalty can be a *fine of up to $5,000* and/or *up to five years in jail*, plus the costs of prosecution.

Under IRC section 7213A, willful unauthorized *access or inspection* of taxpayer records is a misdemeanor. This applies to both paper documents and computerized information. Violators can be subject to a *fine of up to $1,000* and/or up to *one year in prison*.

In addition to criminal penalties, civil remedies may also be pursued by any taxpayer whose return or return information has been knowingly or negligently inspected or disclosed in violation of section 6103. Section 7431 allows a taxpayer to institute action in district court for civil damages. If the court finds there has been an unauthorized inspection or disclosure of FTI, *the taxpayer may receive damages of $1,000 for **each act** of unauthorized access or disclosure* and/or the actual damages sustained, if greater, *plus punitive damages* and costs of the action.

CMS takes its obligations to protect FTI very seriously, and mandates the highest level of due-diligence in protecting that data.

1.1.4 INCIDENT

1.1.4.1 SECURITY INCIDENT

A *Security Incident* is a *Reportable Event* that meets one or more of the following criteria:

- The successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system processing information on behalf of CMS. It 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 CMS data at risk of unauthorized access, use, disclosure, modification, or destruction.

- An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.
- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices[11].

1.1.4.2 PRIVACY INCIDENT

A *Privacy Incident*[12] is a *Security Incident* that involves *Personally Identifiable Information (PII)* or *Protected Health Information (PHI)* where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII/PHI in usable form, whether physical or electronic.

Privacy incident scenarios include, but are not limited to:

- Loss of federal, contractor, or personal electronic devices that store PII/PHI affiliated with CMS activities (i.e., laptops, cell phones that can store data, disks, thumb-drives, flash drives, compact disks, etc.).
- Loss of hard copy documents containing PII/PHI.
- Sharing paper or electronic documents containing PII/PHI with individuals who are not authorized to access it.
- Accessing paper or electronic documents containing PII/PHI without authorization or for reasons not related to job performance.
- Emailing or faxing documents containing PII/PHI to inappropriate recipients, whether intentionally or unintentionally.
- Posting PII/PHI, whether intentionally or unintentionally, to a public website.
- Mailing hard copy documents containing PII/PHI to the incorrect address.
- Leaving documents containing PII/PHI exposed in an area where individuals without approved access could read, copy, or move for future use.

[11] As defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*.

[12] OMB uses the term "breach" in OMB M-07-16 to refer to situations in which PII is suspected or confirmed to be lost or compromised. The Department of Health and Human Services (HHS) uses the term *privacy incident* to refer to situations where PII is *suspected* or *confirmed* to be lost or compromised. Based on its usage within the media, the term *Breach* is commonly perceived as a situation in there is a *likelihood of harm* and individuals have received notification in order to take protection measures. *Breach* (for PHI) is defined in §164.402 of 45 CFR Parts 160 and 164, *Breach Notification for Unsecured Protected Health information, Interim Final Rule*, date August 24, 2009. The term *privacy incident* is used because it more accurately reflects the types of scenarios that occur at HHS and CMS, including incidents that are lower risk and incidents that do not result in *notification* (see Section 0.0.0.0 for the definition of *Breach*.)

The Department has established the *Privacy Incident Response Team (PIRT)*[13] (formerly known as the *PII Breach Response Team [BRT]*) to support the HHS *Risk Management and Financial Oversight Board (RMFOB)* in managing response efforts for privacy incidents, identifying trends, and making recommendations to reduce the risks to PII/PHI on behalf of the Department and its OPDIVs. Table 1 shows the HHS-defined roles for privacy incidents.

Table 1 Privacy Incident Roles

Role	Responsibilities
HHS	
HHS *Risk Management Financial Oversight Board (RMFOB)*	Oversees risk management for the Department. The RMFOB charters the HHS PIRT to help manage risks associated with the loss of PII .
HHS *Privacy Incident Response Team (PIRT)*	Oversees privacy incident response efforts and activities to manage risks associated with the suspected or confirmed loss or compromise of PII. The HHS PIRT is chartered by the RMFOB.
HHS PIRT Chair	Leads HHS PIRT in completing activities to manage privacy incidents response and identifying risks associated with the loss or potential loss of PII.
HHS PIRT Coordinator	Supports privacy response activities, particularly as it relates to coordinating HHS PIRT and OPDIV interactions and ensuring procedures are followed. The HHS PIRT coordinator may delegate certain responsibilities to other parties.
Office of the Assistant Secretary for Public Affairs (ASPA)	Provides guidance and recommendations to the HHS PIRT regarding communications on all incidents and with a particular emphasis on high risk or high-profile incidents that may require a media strategy or public outreach component.
HHS *Computer Security Incident Response Center (HHS CSIRC)*	Collects, analyzes, and disseminates incident-related information and reports this information to internal and external stakeholders (United States Computer Security Emergency Readiness Team (US-CERT) and HHS PIRT). Manages information repository of incident information in the Enterprise Risk Management Tool (Risk Vision). Collaborates with HHS PIRT and OPDIVs to ensure incident information is accurate and appropriate response procedures are executed prior to incident closure.
CMS	
CMS *Chief Information Security Officer (CISO)*	Participates or leads incident response processes as a security subject matter expert. Ensures CMS identification, investigative, and incident reporting processes are effective.
CMS *Senior Official for Privacy (SOP)*	Participates or leads incident response processes as a privacy subject matter expert. Assists in identifying privacy implications of an incident and provides privacy expertise to response efforts.
CMS *Computer Security Incident Response Team (CSIRT)*	Identifies, reports, and manages incidents at the CMS level. The CMS CSIRT should work with the CMS CISO, CMS SOP, CMS Business Owners experiencing the incident, and maintain situational awareness with the HHS PIRT.
CMS Public Affairs Officials	Participates in responses that involve media strategy or a public outreach component. Collaborate with Department ASPA staff on design and execution of outreach efforts.

[13] The *Charter* for the HHS PIRT can be found at http://www.hhs.gov/ocio/policy/hhs-ocio-2010-0001.001c.html.

Role	Responsibilities
CMS Business Owners	Business owners carry out the mission of HHS and often require PII in the course of performing their duties. Business Owners have responsibility for both protecting PII appropriately and identifying when this protection breaks down. Business Owners should report any incident immediately and work closely and diligently with CMS staff to quickly respond and resolve incidents.
CMS *Breach Analysis Team (BAT)*	Team comprised of security, privacy, business owners, and staff authorized to review incidents and make response recommendations (e.g., notification).
CMS Employees/ Contractors	Reports any suspected or confirmed incident involving PII immediately.

1.1.5 BREACH

A *Breach*[14] is a *privacy incident* that poses a *reasonable risk of harm*[15] to the applicable individuals. For the purposes of Office of Management and Budget (OMB) (for PII incidents) and *Health Information Technology for Economic and Clinical Health (HITECH) Act* (for PHI incidents) reporting requirements, a *privacy incident* does not rise to the level of a *Breach* until it has been determined that the use or disclosure of the protected information *compromises the security or privacy of the protected individual(s)* and poses a *reasonable risk of harm* to the applicable individuals. For any CMS *privacy incident*, the determination of whether it may rise to the level of a *Breach* is made (exclusively) by the CMS Breach Analysis Team (BAT), which determines whether the privacy incident *poses a significant risk of financial, reputational, or other harm to the individual(s).*

1.2 APPLICABILITY

CMS operates under federal privacy and information security requirements as both a federal agency and as a health care component of the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Act of 1974 is the primary authority under which CMS, as a federal agency, may collect, use, and disclose PII necessary to accomplish program purposes and operations. The Office of Management and Budget (OMB) is responsible for developing guidance and providing assistance to and oversight of the agencies' Privacy Act implementation. Additionally, CMS is subject to the *Federal Information Security Act of 2002 (FISMA),* which places responsibility and accountability for information security on CMS as well as entities which operate, use, or have access to federal information systems on the agency's behalf.

CMS is also subject to the HIPAA Privacy Rule in administering the Original Medicare Plan (fee-for-service program). The agency has been designated as an HHS health care component

[14] *Breach* (for PII) is defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information. Breach* (for PHI) is defined in §164.402 of 45 CFR Parts 160 and 164, *Breach Notification for Unsecured Protected Health information, Interim Final Rule*, date August 24, 2009. The CMS definition of *Breach* integrates applicable attributes of both of these definitions.

[15] *Reasonable Risk of Harm* is the likelihood that an individual may experience a substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

under HIPAA to the extent that its activities relate to the administration of the Medicare fee-for-service (FFS) health plan. This means CMS is responsible for the Original Medicare program's compliance with HIPAA standards. Other health plans, such as the State Medicaid programs and Medicare Parts C and D plans are covered-entities subject to HIPAA in their own right and responsible for their own compliance. The Office for Civil Rights (OCR) of HHS enforces the HIPAA privacy and security standards for all these health plans and other covered entities.

This standard for incident response, and its associated procedures in Volume II of the RMH, applies to all CMS federal and federally-contracted organizations.

CMS contracts with entities subject to FISMA to assist in the agency's day-to-day business operations. These include Medicare Administrative Contractors (MACs), Fiscal Intermediaries (FI), and carriers for claims payment in operating the Medicare FFS Program, analytical contractors, Program Integrity (PI) contractors, and Quality Improvement Organizations (QIO). As CMS business associates, these entities report PII/PHI incidents in accordance with the provisions in their CMS contracts/agreements.

1.2.1 MEDICARE FEE-FOR-SERVICE (FFS) PROGRAM

This Program includes CMS contracts with Medicare Administrative Contractors (MACs), Fiscal Intermediaries (FI), and carriers for claims payment in operating the Medicare FFS Program. As CMS contractors, these entities are subject to all federal requirements, including OMB and FISMA.

The Medicare FFS contractors are HIPAA business associates doing work on behalf of the Original Medicare health plan. The HIPAA Business Associate provision in all CMS contracts references safeguarding PHI, mitigating any harmful effect(s) of the use or disclosure of PHI, and reporting any use or disclosure not provided for under the contract.

1.2.2 ANALYTICAL CONTRACTORS

Analytical contractors work on behalf of CMS in conducting its administrative responsibilities. Their CMS contract requires safeguarding PII/PHI in accordance with FISMA and other federal requirements, including reporting incidents to the contractors' Project Officers.

1.2.3 PROGRAM INTEGRITY (PI) CONTRACTORS

The PI contractors collect and use PII on behalf of Medicare to perform such activities as medical review and PI activities to prevent fraud and abuse. These PI contractors–program safeguard contractors (PSC) and zone PI contractors (ZPIC)–are required to report incidents in accordance with instructions in the Medicare Program Integrity Manual, 100-08[16].

[16] See Chapter 4, Section 4.2.2.6.C. at http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/pim83c04.pdf.

1.2.4 QUALITY IMPROVEMENT ORGANIZATIONS (QIO)

The Quality Improvement Organizations (QIOs) conduct activities to improve the quality of care delivered to Medicare beneficiaries. The QualityNet Security Program[17] provides guidance on incidence response by QualityNet users, contractors, and others who process, store, transmit, or have access to PII/PHI.

1.2.5 EXTERNAL RESEARCH ENTITIES

CMS discloses PII/PHI to external entities to conduct research studies that will improve CMS programs or services provided to its beneficiaries. These entities are often federally funded grantees of another HHS Operating Division or other federal agency.

These external entities are not subject to FISMA. However, their research protocols include a description of the database management safeguards to ensure the privacy and confidentiality of CMS data. The entities are also required to sign the CMS Data Use Agreement (DUA) Form[18], which requires reporting incidents involving PII to the CMS IT Service Desk.

1.2.6 RESEARCH ENTITIES

External entities are instructed to immediately notify their CMS Project Officer of a breach involving data provided by the agency for research purposes. Additionally, the entities follow the DUA's provision to immediately report a PII breach to the CMS IT Service Desk.

1.2.7 NON-FISMA ENTITIES

Private Medicare plans and State Medicaid Programs are HIPAA covered entities in their own right. As such, these health plans are subject to HITECH breach notification requirements and are responsible to report breaches directly to HHS OCR, as required. CMS does not report incidents from these entities to HHS CSIRC (the agency reports incidents involving FISMA entities only).

The CMS components with program administration and oversight responsibilities for these health plans have established the process and procedures to report PII breaches.

1.2.8 PRIVATE MEDICARE PLANS

CMS contracts with private health plans for health coverage choice and prescription drug coverage to beneficiaries. These Medicare Part C and D plans are HIPAA covered entities in their own right and are responsible for reporting breaches directly to the HHS OCR in accordance with HITECH requirements. CMS requires these organizations to submit concurrent notification to their Regional Office account managers of breach notifications submitted to OCR.

[17] For the QualityNet Incident Response Procedures, go to http://www.qualitynet.org/.
[18] For the DUA Form, CMS-R-0235, go to http://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/Downloads/CMS-R-0235.pdf.

Additionally, these organizations are required to comply with all federal requirements under their CMS contract, including HIPAA. CMS has authority to take compliance or enforcement actions where the agency believes organizations have not taken appropriate measures to safeguard the privacy of its Medicare members.

1.3 INCIDENT RESPONSE PHASES

There are five basic steps in incident handling: *Preparation, Identification, Response, Recovery,* and *Follow-up*.

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 such as guidelines identifying levels and responses, auditing and logging, reporting guidelines, resolution and follow-up.

By establishing policies, procedures, and agreements in advance, organizations minimize the chance of making catastrophic mistakes. Within the CMS federal environment, this *Standard,* and the associated *RMH Procedures* lays the foundation for the policy and procedural-level preparations.

As in most areas of life, *prevention* is better than *cure*—and security is no exception. Wherever possible, organizations need to prevent security incidents from happening in the first place. However, it is impossible to prevent *all* security incidents. When a security incident does happen, organizations need to ensure that the impact is minimized. To minimize the number and impact of security incidents, organizations should:

- Clearly establish and enforce all policies and procedures. Many security incidents are accidentally created by IT personnel who have not followed or not understood change management procedures or have improperly configured security devices, such as firewalls and authentication systems. Organizational (both CMS and contractor) policies and procedures should be thoroughly tested to ensure that they are practical and clear and provide the appropriate security.
- Gain management support for security policies and incident handling.
- Routinely assess vulnerabilities in their environment (continuous monitoring—a key component to a health security program.)
- Routinely check all computer systems and network devices to ensure that they have all of the latest patches, and are securely configured to (at *least*) minimum standards.
- Establish security-training programs for both IT staff and end users. The largest vulnerability in any system is the inexperienced user.
- Routinely monitor and analyze network traffic and system performance.
- Routinely check all logs and logging mechanisms, including operating system event logs, application-specific logs, and intrusion-detection system logs.

- Verify organizational back-up and restore procedures. Organizations should be aware of where backups are maintained, who can access them, and the procedures for data (and system) restoration and recovery. Organizations should regularly verify backups and media by selectively restoring data.
- Create an *Incident Response* capability (local incident response authority) within the organization to deal with security incidents specific to the organizational level. At contractor-hosted sites, the applicable organizations should establish an on-site response capability, supported by applicable Incident Response Policy and Procedures. The following steps should be taken in the preparation phase:
  - Establish an applicable local security policy, develop management support for an incident handling capability, monitor and analyze the network traffic, assess vulnerabilities, configure systems wisely, install updates regularly, and establish training programs.
  - Establish an organizational approach for handling incidents.
    - Pre-select incident handling team members and organize the team.
    - Establish a primary point of contact as the on-site *Incident Response (IR) Authority* and, if applicable, an incident command and communications center.
    - Conduct necessary training for team members.
    - Involve system administrators and network managers early.
  - Establish a policy for notifying the CMS CSIRT and other outside organizations that may be connected to operating unit systems.
  - Update the organization's business continuity plan to include computer security incident handling.
  - Develop a listing of law enforcement agencies and applicable response assets to notify when an incident occurs.

All members of the IT environment should be aware of what to do in the event of an incident. The *on-site IR authority* and the CMS CSIRT will perform most of the *direct* actions in response to an incident, but *all* levels of CMS and contractor staff should be aware of how to report and respond to incidents internally. End users should report suspicious activity to the on-site IR authority directly or through the CMS IT service desk (as applicable) rather than directly to the CMS CSIRT (or HHS CSIRC.)

A successful incident response plan should include the following elements:

- Make an initial assessment.
- Communicate the incident.
- Contain the damage and minimize the risk.
- Identify the type and severity of the compromise.
- Protect evidence.
- Notify external organizations if appropriate.
- Recover systems.
- Compile and organize incident documentation.
- Assess incident damage and cost.

- Review the response and update policies, if necessary.

These steps are not purely sequential. Rather, they happen throughout the incident. For example, documentation starts at the very beginning and continues throughout the entire life cycle of the incident; communication also happens throughout the entire incident.

Other aspects of the process will work alongside each other. For example, as part of an organization's initial assessment, they will gain an idea of the general nature of the attack. It is important to use this information to contain the damage and minimize risk as soon as possible. If organizations act quickly, they may help to save time and money, protect citizen data, as well as CMS' and individual contractor's reputations.

By acting quickly to reduce the actual and potential effects of an attack, organizations can make the difference between a minor *event* and a major *incident*. The exact response will depend on the organization's mission and the nature of any specific attack. However, the following priorities are suggested as a starting point in designing an effective on-site IR plan:

- **Protect human life and people's safety.** This must always be the first and highest priority.
- **Protect sensitive and privacy related data.** As part of planning for incident response, organizations should clearly define which data is *business sensitive* and which is *PII* or *PHI* data. This will enable organizations to prioritize their responses in protecting the data. This is doubly important due to specific reporting time-lines and notification requirements for incidents involving PII and/or PHI.
- **Protect other data, including proprietary, scientific, and managerial data.** Other data in the CMS environment may still be of great value. All CMS organizations should act to protect the most valuable data first before moving on to other, less useful, data. This may include isolation of affected systems, and even *intentionally* disrupting CMS services in favor of securing sensitive data.
- **Protect hardware and software against attack.** This includes protecting against loss or alteration of system files and physical damage to hardware. Damage to CMS systems can result in disruptive (and highly visible) downtime of Medicare services.
- **Minimize disruption of computing resources (including processes).** Although uptime is very important in most CMS environments, keeping systems up during an attack might result in greater problems (and more lengthy disruptions) later on. For this reason, minimizing disruption of CMS computing resources should generally be a relatively *low* priority.

1.3.2 IDENTIFICATION PHASE

The ***Identification Phase*** is the process of detecting a potential security incident and reporting it. This phase also involves the reporting of security incidents to the *CMS IT Service Desk*, who will immediately refer security incidents to the *CMS Computer Security Incident Response Team (CSIRT)*. The CSIRT receives **all** incidents reported to the *CMS IT Service Desk*.

Alerts to a potential incident may arrive from a variety of sources including: monitoring of firewalls and intrusion detection systems, anti-virus software, threats received via email, and media reports about new threats. The CSIRT assesses, tracks, and reports all incidents to HHS'

security program and privacy incidents are immediately reported to the *CMS Breach Analysis Team (BAT)* for assessment.

Incident detection occurs internally in all areas and at all levels of CMS, as well as externally, through reports from business partners and non-organizational users. All incidents should immediately be reported once detected. The earlier an incident is reported, the faster the necessary resources can be made available to combat the threat.

Administrators and users must be familiar with their systems to determine if an event constitutes an incident. Effective incident detection occurs when:

- The administrator or user is familiar with normal operations.
- Systems are equipped with effective auditing and logging tools.
- Administrators review systems and logs to identify deviations from normal operations.
- Users and administrators have been trained to recognize and report suspicious activities.

Appropriate security and information technology contacts must analyze all available information in order to understand the scope of an incident and effectively contain and remediate the incident.

As part of the *Identification Phase*, reported incidents are immediately "triaged". This is where the *CSIRT* coordinates the examining (investigating) of available information to determine whether a security incident has actually occurred, and conducts necessary preliminary risk assessments for privacy incidents. This process includes the following steps:

1.3.2.1 ASSESSMENT

In this step, the CSIRT will determine the nature of the incident. The following steps are immediately taken:

- The CSIRT, with support from the applicable Business Owner, will establish communications and coordination with an on-site IR authority to be responsible, locally, for the incident response.
- Determine whether an event is actually an incident.
- Verify that the system/business process involved is actually a CMS or CMS contractor operation.
- For IT system events, check for simple mistakes such as errors in system configuration or an application program, hardware failures, and most commonly, user or system administrator errors.
- Identify and assess the evidence in detail and maintain a chain of custody. Control access to the evidence.
- Notify appropriate officials such as immediate supervisors or managers, the organization's Security Officer, Business Owners, and the HHS CSIRC.

1.3.2.2 INCIDENT CATEGORIZATION

The next step is the *Categorization* of the incident. This process is directly related to the information type and the type of event. These two factors are used to categorize an incident using the HHS/CMS incident categories in Table 2.

1.3.2.3 COORDINATION

Coordination of resources is extremely important—especially in the highly-diverse business environment of CMS. Notification of other involved parties, on a need-to-know basis, is critical for rapid response and limiting the damage of an active attack.

- The CMS CSIRT identifies applicable Business Owners to participate on the response team.
- The CMS CSIRT, in coordination with the applicable Business Owner(s), facilitates contact with other sites and organizations that may be involved.
- The CMS CSIRT manages contact with the on-site response authority and the HHS CSIRC.
- The CSIRT determines the nature of the incident, assigns the initial categorization, and documents (along with applicable on-site IR authorities) actions taken.

A decision to *pursue* or *protect* occurs during this phase, according to the sensitivity of the data and criticality of the operational system. Upon making a decision to *pursue*, it assumes the intrusion or misuse may continue as analysts gather information about the malicious activity before proceeding to *protect* the system and initiate actions to discontinue the unauthorized actions as in the *Response Phase*. In each scenario, the CMS CSIRT and the on-site IR authority will perform protective actions on the system to safeguard data and system resources on the affected system. The CMS CSIRT considers potential legal or public relations impacts arising from each course of action.

For privacy incidents, the CMS CSIRT, as part of its role on the *Pre-Breach Analysis Team*[19] (Pre-BAT), applies *Assessment Guidelines*. This process will quickly identify events with little or no risk of financial, reputational, or other harm to affected individuals. The *Assessment Guidelines* relate to specific situations involving Medicare documents containing PII/PHI that are received by other HIPAA covered entities or beneficiaries other than to whom they were intended.

The *Pre-BAT* triage is managed by the CSIRT, with the assistance of the Business Owner and CMS Senior Official for Privacy (SOP) staff for privacy-related incidents. The Pre-BAT reviews and triages incidents, as appropriate, for a formal risk assessment and/or for coordination with the HHS Privacy Incident Response Team (PIRT).

1.3.3 RESPONSE PHASE

The ***Response Phase*** (also known as the *Containment and Eradication Phase*) is the process of limiting the scope and magnitude of an incident in order to keep the incident from getting worse. It may be necessary to activate Business Continuity Plans in this phase.

[19] See Section 2.6 for a description of the Pre-BAT *Roles and Responsibilities*.

The CMS CSIRT establishes strategies and procedures for containing incidents. However, it should be noted that no two incidents are alike, and each will require specific and unique responses. It is important to contain incidents quickly and effectively to limit their business impact. On-site IR authorities should define acceptable risks in containing incidents (within their own infrastructure) and develop strategies and procedures accordingly. Containment strategies should vary based on the type of incident.

The CSIRT and the associated on-site IR authorities should follow established procedures for evidence gathering and handling. The teams should clearly document how all evidence has been preserved. Evidence should be accounted for at all times. The team should meet with legal staff and law enforcement agencies to discuss and plan for evidence handling, and develop processes and procedures based on those discussions.

Capture volatile data from systems as evidence. This effort includes lists of network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. Running carefully chosen commands from trusted media can collect the necessary information without damaging the system's evidence.

Incident response teams should create a containment strategy that includes several solutions in sequence. The decision-making process for containing DoS incidents is easier if recommended solutions are predetermined. Because the effectiveness of each possible solution will vary among incidents, organizations should select several solutions and determine the sequence in which the solutions should be attempted.

Incident response teams should contain malicious code incidents as quickly as possible. Because malicious code works surreptitiously and can propagate to other systems rapidly, early containment of a malicious code incident is needed to stop it from spreading and causing further damage. Infected systems should be disconnected from the network immediately. Organizations may need to block malicious code at the email server level, or temporarily suspend email services to gain control over serious email-borne malicious code incidents.

System administrators should be prepared to provide change management information to the incident response team. Indications such as system shutdowns, audit configuration changes, and executable modifications are probably caused by routine system administration, rather than attacks. When such indications are detected, the team should be able to use change management information to verify that the indications are caused by authorized activity.

Incident response teams should select containment strategies that balance mitigating risks and maintaining services. Incident handlers should consider moderate containment solutions that focus on mitigating the risks as much as is practical while maintaining unaffected services. However, the primary focus is to regain full control over affected systems.

Be prepared to restore or reinstall systems that appear to have suffered a root compromise. The effects of root compromises are often difficult to identify completely. The system should be restored from a known good backup, or the operating system and applications should be reinstalled from scratch. The system should then be secured properly so the incident cannot recur.

For any incident, do not overlook the possibility that the effects are more pervasive than symptoms may indicate. However, first contain the initial incident, and then search for signs of

other incident components. It can take some time to search an enterprise for other affected components. Do NOT allow a single affected component to continue to operate (unmitigated) while you determine the full extent of the scope. It is generally better to contain the initial incident as soon as possible before diverting resources to conduct a scope analysis.

Organization's should create separate containment strategies for each major type of incident, and should factor in:

- Potential damage to and theft of resources.
- Need for evidence preservation.
- Service availability.
- Time and resources needed to implement the strategy.
- Effectiveness of the strategy (partial or full containment).
- Duration of the solution (i.e., work around or permanent fix).

Some incidents may involve extensive evidence-gathering activities. Incident response teams should plan for the need for resolving the incident and potential legal requirements, and should be aligned with appropriate regulatory and compliance requirements. Chain of custody should be maintained when evidence is transferred between parties, and detailed logs of the evidence should be maintained. These logs should retain:

- Name, title, and contact information of the person who gathered the evidence.
- Date, time, and place of evidence receipt or collection.
- Description of data obtained, including identifying information, and media-specific information.
- Description of evidence collection procedures.
- Name, title, and contact information for each person who collected or handled the evidence.
- Time and date of each occurrence of evidence handling.
- Locations where the evidence was stored.

The CMS CSIRT (under the guidance of the HHS CSIRC and the HHS OIG) will serve as the lead organization for evidence handling and collection. On-site incident response authorities shall defer to the CMS CSIRT for guidance.

There are several key factors that incident response teams need to fully understand prior to conducting forensic analysis on IT equipment subsequent to an incident:

- Any action performed on the host will alter the state of the machine to some extent.
- Issue only the minimum commands needed for acquiring dynamic evidence without altering other evidence.
- Obtaining a full disk image is superior to a standard file system backup for computer forensic purposes because it records more data.
- It's more forensically sound to analyze an image rather than to perform analysis on the original resource. (preservation of evidence).

- Computer forensic software is available to not only acquire disk images, but also to automate much of the analysis process.

Again, the CMS CSIRT (under the guidance of the HHS CSIRC and the HHS OIG) will serve as the lead organization for forensic investigations. On-site incident response authorities shall defer to the CMS CSIRT for guidance before conducting ANY forensic analysis or attempting to access resources that might later be used as evidence.

1.3.4 RECOVERY PHASE

In the ***Recovery Phase***, the system and business process returns to full and normal operations. 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.

This phase ensures that the system is returned to a fully operational status. The following steps should be taken in the *Recovery Phase*:

- Restore the system.
- Validate the system. Once the system has been restored, verify that the operation was successful and the system is back to its normal condition.
- Decide when to restore operations. Management may decide to leave the system offline while operating system upgrades and patches are installed.
- Monitor the systems. Once the system is back on line, continue to monitor for malicious back doors that may have escaped detection.

1.3.5 FOLLOW-UP PHASE

The ***Follow-up Phase*** involves fully documenting in the final incident report and disseminating the report 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.

Incident response teams should hold lessons learned meetings after major incidents. Lessons learned meetings are extremely helpful in improving security measures and the incident handling process itself. These meetings should *not* be limited to only the CSIRT or the on-site IR authority personnel. Most valuable lessons are applied by system administrators and/or users.

1.4 SECURITY INCIDENT CATEGORIZATION

CMS classifies incidents, as shown in Table 2, based on categories outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*, and the HHS CSIRC.

If multiple incident categories are involved (e.g., an unauthorized individual accessing a system containing PHI and/or PII, then multiple categories may apply. Any incident that involves

compromised PII/PHI must be reported within one (1) hour of detection, regardless of the incident category reporting timeframe.

Table 2 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 one (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 two (2) hours of discovery/ detection if the successful attack is ongoing and the 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. Agencies are NOT required to report malicious logic that has been successfully quarantined by anti-virus software.	Within one (1) hour of discovery/ detection if widespread across the 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).
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Weekly

1.5 PRIVACY BREACH HANDLING

Privacy Incidents occur when there is an unauthorized release of PII. However, PII can be broken down into more granular subsets. These subsets include PHI as defined by HIPAA and HITECH, and Federal Tax Information as defined by the *Tax Information Security Guidelines for Federal, State and Local Agencies* (available at http://www.irs.gov/pub/irs-pdf/p1075.pdf.)

1.5.1 BREACH OF PERSONALLY IDENTIFIABLE INFORMATION

This section addresses ***only*** the requirements for individual Breach Notification for information that falls under the definition provided under the *Privacy Act of 1974* (Privacy Act). PII that is also classified as *PHI* or *Federal Tax Information (FTI)*[20] will have additional notification requirements, in addition to those noted in this section.

The Privacy Act requires each agency to develop an effective response that requires disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach. OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*[21], provides extensive guidance on the requirements for individual notification (to those individuals affected by the breach) of a breach.

Agencies must report all incidents involving personally identifiable information to US-CERT. This reporting requirement does not distinguish between *potential* and *confirmed* breaches—all must be reported within 1-hour of discovery/detection.

1.5.1.1 WHEN BREACH NOTIFICATION IS REQUIRED

To determine whether notification of a breach is required, the agency should first assess the ***likely risk of harm*** caused by the breach, and then assess the level of risk. CMS must consider a wide range of harms, such as harm to reputation (for the individual) and the potential for harassment or prejudice (to the individual), particularly when health or financial benefits information is involved in the breach.[22] CMS management must bear in mind that notification, when there is little or no risk of harm, might create unnecessary concern and confusion.[23] Additionally, under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

Five factors should be considered to assess the likely *risk of harm*:

1. **Nature of the Data Elements Breached.** The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to

[20] *Federal Tax Information* – Generally, Federal Tax Returns and return information are confidential, as required by Internal Revenue Code (IRC) Section 6103. The information is used by the IRS to ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality.
[21] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, is available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
[22] For reference, the express language of the *Privacy Act* requires CMS to consider a wide range of harms: agencies shall *"establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."* 5 U.S.C. § 552a (e)(10).
[23] Another consideration is a surfeit of notices, resulting from notification criteria that are too strict, could render *all* such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant.

affected individuals.[24] It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual—therefore, this risk is NOT directly related to the system security category of the applicable FISMA system, nor is it related to the data type assigned to the information. A *name* in one context may be less sensitive than in another context.[25] In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

2. **Number of Individuals Affected.** The *magnitude* of the number of affected individuals *may* dictate the method(s) you choose for providing notification, ***but should not be the determining factor*** for whether CMS should provide notification.

3. **Likelihood the Information is Accessible and Usable.** Upon learning of a breach, agencies should assess the likelihood personally identifiable information will be, or has been, used by unauthorized individuals. An *increased* risk that the information will be used by unauthorized individuals *should* influence the agency's decision to provide notification.

   The fact the information has been lost or stolen does not necessarily mean it has been, or can be, accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed by the agency. If the information is properly protected[26] by encryption, for example, the risk of compromise may be low to non-existent.

   CMS will first need to assess whether the personally identifiable information is at a *low*, *moderate*, or *high* risk of being compromised. The assessment should be guided by NIST security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

4. **Likelihood the Breach May Lead to Harm**

   a. **Broad Reach of Potential Harm.** The *Privacy Act* requires agencies to protect against any anticipated threats or hazards to the security or integrity of records that could result in *"substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."*[27] Additionally, CMS should consider a number of possible harms associated with the loss or compromise of information. Such harms may

[24] For example, theft of a database containing individuals' names in conjunction with Social Security numbers, and/ or dates of birth may pose a *high* level of risk of harm, while a theft of a database containing only the names of individuals may pose a *lower* risk, depending on its context.

[25] For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a *higher* risk of harm, whereas a database of names of subscribers to agency media alerts may pose a *lower* risk of harm. In fact, a list of names that is included in a demographic data file, even though the data demographic is not actually identified in the *individual records*, may still be highly relevant when determining the risk of harm. For instance; a breached data file labeled as *"HIV carriers"* with a name and address of each individual would likely carry a *high* risk of harm to the individuals therein.

[26] In this context, proper protection means encryption has been validated by NIST. See http://csrc.nist.gov/groups/STM/cmvp/validation.html for NIST validated modules.

[27] See the *Privacy Act or 1074*, 5 U.S.C. § 552a(e)(10) (as amended), available at http://www.justice.gov/opcl/privstat.htm.

include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

b. **Likelihood Harm Will Occur.** The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease.

   In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the *Identity Theft Task Force*.[28]

5. **Ability of the Agency to Mitigate the Risk of Harm**. Within a CMS information system, the *risk of harm* will depend on how CMS is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken.[29] Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

1.5.1.2 NOTIFICATION TIMELINESS

CMS organizations should provide notification without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement any measures necessary for CMS to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised.

Decisions to delay notification should be made by the CMS Administrator or a senior-level individual designated by the Administrator in writing. In some circumstances, law enforcement considerations may require a delay if it would seriously impede the investigation of the breach or the affected individual. However, any delay should not exacerbate risk or harm to any affected individual(s).

1.5.1.3 SOURCE OF NOTIFICATION

In general, notification to individuals affected by the breach should be issued by the CMS Administrator. This demonstrates that the breach has the attention of the highest levels of CMS.

[28] See *Recommendations for Identity Theft Related Data Breach Notification*, available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/task_force_theft_memo.pdf.
[29] For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.

Notification involving only a limited number of individuals (e.g., under 50) may also be issued jointly under the auspices of the *Chief Information Officer* and the *Chief Privacy Officer* or *Senior Official for Privacy*. This approach signals the agency recognizes both the security and privacy concerns raised by the breach.

When the breach involves a CMS contractor or a public-private partnership operating a *system of records* on behalf of CMS, CMS is responsible for ensuring any notification and corrective actions are taken. The roles, responsibilities, and relationships with contractors or partners should be reflected in the CMS breach notification policy and plan, the CMS FISMA system *Authorization to Operate* documentation, and contracts and other relevant documents.

1.5.1.4 NOTIFICATION CONTENTS

Notification should be provided *in writing* and should be *concise*, *conspicuous*, and in *plain language*. The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery.
- To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.)
- A statement as to whether the information was encrypted or protected by other means, when determined that such information would be beneficial and would not compromise the security of the system.
- What steps individuals should take to protect themselves from potential harm, if any.
- What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches.
- Who affected individuals should contact at the agency for more information, including a toll-free telephone number, e-mail address, and postal address.

Given the amount of information required above, relevant CMS notification organizations should consider layering the information as suggested in Section 1.5.1.5 below, providing the most important information up front, with the additional details in a *Frequently Asked Questions (FAQ)* format or on an applicable web site. If CMS has knowledge the affected individuals are not English-speaking, then notice should also be provided in the appropriate language(s). Organizations may seek additional guidance on how to draft the notice from the *Federal Trade Commission*, a leader in providing clear and understandable notices to consumers, as well as from communication experts who may assist in designing model notices.[30] A standard notice should be part of applicable breach plans.

[30] Additional guidance on how to draft a notice is available in the FTC publication titled *Dealing with a Data Breach* (available at www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html). Although the brochure is designed for private sector entities that have experienced a breach, it contains sample notice letters that could also serve as a model for federal agencies.

1.5.1.5 MEANS OF PROVIDING NOTIFICATION

The best means for providing notification will depend on the number of individuals affected and what contact information is available about the affected individuals. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following examples are types of notice that may be considered:

1. **Telephone.** Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be at the same time as, or in parallel with, written notification by first-class mail.

2. **First-Class Mail.** First-class mail notification to the last known mailing address of the individual in CMS records should be the primary means notification is provided. Where CMS has reason to believe the address is no longer current, organizations should take reasonable steps to update the address by consulting with other agencies such as the Social Security Administration. The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If CMS uses another agency to facilitate mailing (for example, if the agency that suffered the loss consults the IRS for current mailing addresses of affected individuals), care should be taken to ensure that CMS is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its contents, e.g., *"Data Breach Information Enclosed"* and should be marked identifying CMS as the sender to reduce the likelihood the recipient thinks it is advertising mail.

3. **E-Mail.** E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. Notification by postal mail is preferable. However, where an individual has provided an e-mail address and has expressly given consent to e-mail as the primary means of communication with CMS, ***and*** no known mailing address is available, notification by e-mail *may* be appropriate. E-mail notification may also be employed *in conjunction* with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the agency and http://www.usa.gov/[31] web sites, where the notice may be "layered" so the most important summary facts are up front with additional information provided under link headings.

4. **Existing Government Wide Services.** CMS should leverage Government-wide services already in place to provide support services needed, including toll free number of *1-800-FedInfo* and http://www.usa.gov/.

5. **Newspapers or other Public Media Outlets.** Additionally, CMS may supplement individual notification with placing notifications in newspapers or other public media outlets. Organizations should also set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

[31] The current domain name for the *Federal Internet Portal* required by section 204 of the *E-Government Act of 2002* (available at http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm) is www.usa.gov.

6. **Substitute Notice.** Substitute notice in those instances where CMS does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice on the home page of CMS' web site and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media should include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

7. **Accommodations.** Special consideration to providing notice to individuals who are visually or hearing impaired consistent with *Section 508 of the Rehabilitation Act of 1973* should be given. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on an applicable CMS web site.

1.5.1.6 WHO RECEIVES NOTIFICATION

Public outreach in response to a breach may include:

1. **Notification of Individuals.** The final consideration in the notification process when providing notice is to whom you should provide notification: the affected individuals, the public media, and/or other third parties affected by the breach or the notification. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals should receive prompt notification.

2. **Notification of Third Parties including the Media.** If communicating with third parties regarding a breach, agencies should consider the following:

    a. **Careful Planning.** CMS' decision to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public. When appropriate, public media should be notified as soon as possible after the discovery of a breach and the response plan, including the notification, has been developed. Notification should focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies as described above in Section 1.5.1.2. To the extent possible, when necessary, *prompt* public media disclosure is generally preferable because delayed notification may erode public trust.

    b. **Web Posting.** CMS should post information about the breach and notification in a clearly identifiable location on the CMS web site as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. The posting should include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach and the notification process. The information should also appear on the http://www.usa.gov/ web site. CMS may also consult with GSA's *USA Services* regarding using their call center.

    c. **Notification of other Public and Private Sector Agencies.** Other public and private sector agencies may need to be notified on a need to know basis, particularly those that

may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach.[32]

d. **Congressional Inquiries.** Agencies should be prepared to respond to inquiries from other governmental agencies such as the *Government Accountability Office (GAO)* and Congress.

3. **Reassess the Level of Impact Assigned to the Information.** After evaluating each of these factors, you should review and reassess the level of impact (security category) already assigned to the information using the impact levels defined by the NIST.[33] The impact levels – *low*, *moderate*, and *high*, describe the (worst case) potential impact on an organization or individual if a breach of security occurs.[34]

- ***Low:*** the loss of *confidentiality*, *integrity*, or *availability* is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- ***Moderate:*** the loss of *confidentiality*, *integrity*, or *availability* is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- ***High:*** the loss of *confidentiality*, *integrity*, or *availability* is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The impact levels will help determine when and how notification should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood the information is accessible and usable and whether the breach may lead to harm. If agencies appropriately apply the five risk factors discussed in Section 1.5.1.1 within the fact-specific context, it is likely notification will only be given in those instances where there is a reasonable risk of harm *and* will not lead to the overuse of notification.

1.5.2 BREACH OF FEDERAL TAX INFORMATION

Disclosure or *inspection* of *FTI* is generally prohibited unless ***specifically*** authorized by statute. Agencies having access to FTI are ***not allowed to make further disclosures*** of that information, to their agents or to a contractor, unless *specifically* authorized by statute. CMS contracting agents are encouraged to use specific language in contractual agreements to avoid ambivalence or ambiguity. Note: Absent specific language in the *Internal Revenue Code (IRC)* or where the IRC is silent in authorizing an agency to make further disclosures, IRS' position is that further disclosures are ***NOT*** authorized. Any unauthorized disclosure of FTI would constitute a breach of FTI, and should be treated accordingly.

[32] For example, a breach involving medical information may warrant notification of the breach to health care providers and insurers through the public or specialized health media, and a breach of financial information may warrant notification to financial institutions through the federal banking agencies.
[33] See FIPS 199 available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. Reassessment is suggested as the context of any breach may alter the original designation.
[34] The determination of the potential *impact* of loss of information is made during an information system's *Authorization to Operate (ATO)* process.

All CMS organizations intending to disclose FTI to contractors (including consolidated data centers, off-site storage facilities, shred companies, information technology support, and for tax modeling or revenue forecasting purposes) ***must notify the IRS prior to executing any agreement to disclose*** to such a person (contractor), but in no event less than ***45 days prior*** to the disclosure of FTI. In addition, if an existing contractor employs the services of a subcontractor, a notification is required 45-days prior to the disclosure of FTI (See IRS Publication 1075 for specific data required in the 45-day notification.) Agencies receiving FTI under authority of IRC 6103(l)(7) may not disclose FTI to contractors for any purpose.

Reporting requirements for PII breaches that include Federal Tax Information should be coordinated with the *U.S. Department of the Treasury* and the *Internal Revenue Service*. Upon discovering a possible improper *inspection* or *disclosure* of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the CMS CISO, in coordination with the applicable Business/Data Owner, should contact and coordinate with the office of the appropriate *Special Agent-in-Charge, Treasury Inspector General for Tax Administration* and the IRS (see the IRS Publication 1075, Section 10.2).

1.5.3 BREACH OF PROTECTED HEALTH INFORMATION

The *American Recovery and Reinvestment Act of 2009 (ARRA)* was enacted on February 17, 2009. ARRA contains extensive provisions seeking to improve the current U.S. health care information technology infrastructure, promote electronic data exchange, and encourage greater use of electronic health records (EHRs). Collectively referred to as the *"Health Information Technology for Economic and Clinical Health Act"* or the *"HITECH Act"*, these provisions also include important changes to the *Health Insurance Portability and Accountability Act (HIPAA) Privacy* and *Security* Rules.

The *HITECH Act* obligates CMS business associates to comply with specific HIPAA requirements (previously HIPAA business associates were solely obligated under their contracts with covered entities). In addition, the *HITECH Act* clarifies that organizations providing data transmission of protected health information (PHI) and vendors that provide personal health records with respect to covered entities are to be treated as business associates.

As part of their requirements under the *HITECH Act*, HHS issued regulations requiring health care providers, health plans, and other HIPAA-covered entities to notify individuals when their health information is breached. These *breach notification* regulations implement several provisions of the *HITECH Act*.

The regulations, developed by HHS Office of Civil Rights (OCR), require health care providers and other HIPAA-covered entities to **promptly notify affected individuals of a breach**, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals must be reported to the HHS Secretary on an annual basis. The regulations also require business associates of HIPAA-covered entities to notify the covered entity of breaches at or by the business associate.

The regulations were developed in consultation with the Federal Trade Commission (FTC), which has issued companion breach notification regulations that apply to vendors of personal health records and certain others not covered by HIPAA. *The Interim Final Rule for Breach*

Notification for Unsecured Protected Health Information ("interim rule"), issued in August 2009, implement section 13402 of the *HITECH Act* by requiring HIPAA-covered entities and their business associates to provide notification following a breach of *unsecured* protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the *HITECH Act*.

To determine when information is *"unsecured"* and notification is required by the HHS and FTC rules, HHS is also issued, in the same document as the regulations, an update to its guidance[35] specifying encryption and destruction as the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information.

HHS reviewed the public comment on the *interim rule* and developed a *final rule*, which was submitted to the Office of Management and Budget (OMB) for Executive Order 12866 regulatory review on May 14, 2010. However, HHS has *withdrawn* the breach notification *final rule* from OMB review to allow for further consideration, given the Department's experience to date in administering the regulations. HHS intends to publish a *final rule* in the Federal Register soon. Until such time as a new *final rule* is issued, the *interim rule* that became effective on September 23, 2009, remains in effect. Limited changes may occur when the Interim Final Rule is made final. At that time, further information and direction will be provided.

1.5.3.1 PHI BREACH NOTIFICATION

If an event occurs that *may* involve improper use or disclosure of PHI, CMS entities should *immediately* report it as a security/privacy incident to the *CMS IT Service Desk*. The CMS CISO will follow existing CMS breach response procedures, which include reporting the breach to the *CMS Breach Analysis Team (BAT)*. The BAT will determine whether the HHS *Interim Final Rule for Breach Notification for Unsecured Protected Health Information* applies; and if it does, the BAT will make recommendations to the *HHS Privacy Incident Response Team (PIRT)* and advise the CMS component on complying with individual notification requirements.

1.5.4 BREACH NOTIFICATION ACTIONS

Actual or possible breaches of PII that occur within a CMS organization must be immediately reported to the *CMS IT Service Desk* as soon as they are discovered. It is important that this initial report be made *immediately* in order that subsequent notification and reporting may be completed in a timely manner. The CMS BAT will determine if the incident qualifies as a breach under the HITECH provisions. If so, the BAT will advise the applicable CMS organization on notifying affected individuals in accordance with HITECH requirements. In addition, the CMS CSIRT will report the incident directly to the Department of Health and

[35] The current *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

Human Services (HHS) via the HHS *RiskVision* incident reporting and tracking system. The BAT will make recommendations to the HHS PIRT for disclosure notifications in accordance with the *HITECH Act*.

The *HITECH Act* requires that HIPAA-covered entities notify individuals *"without unreasonable delay"* after a breach of unsecured PHI has been discovered. A breach is treated as *"discovered"* on the first day the breach is ***known*** or ***should have been known*** to any person who is a workforce member or agent of the HIPAA-covered entity (other than the person committing the breach). When there is insufficient contact information for individual written notice, special rules for substitute notice apply. In all cases, individual notification or substitute notice must be issued no later than sixty (60) calendar days from the time a breach is discovered. The 60-day period is an outer limit; in most cases, the "without unreasonable delay" standard will require notifying affected individuals shortly after the breach is discovered. Typically, CMS should endeavor to meet this requirement within approximately ten (10) days.

Notice to the media is required when a breach affects more than 500 residents of a state or jurisdiction. The CMS BAT will work with the applicable CMS organization to provide the required notices in compliance with both CMS guidance and the HHS *interim rule* (if it applies). If a law enforcement official requests delay of notification, the BAT should be informed immediately.

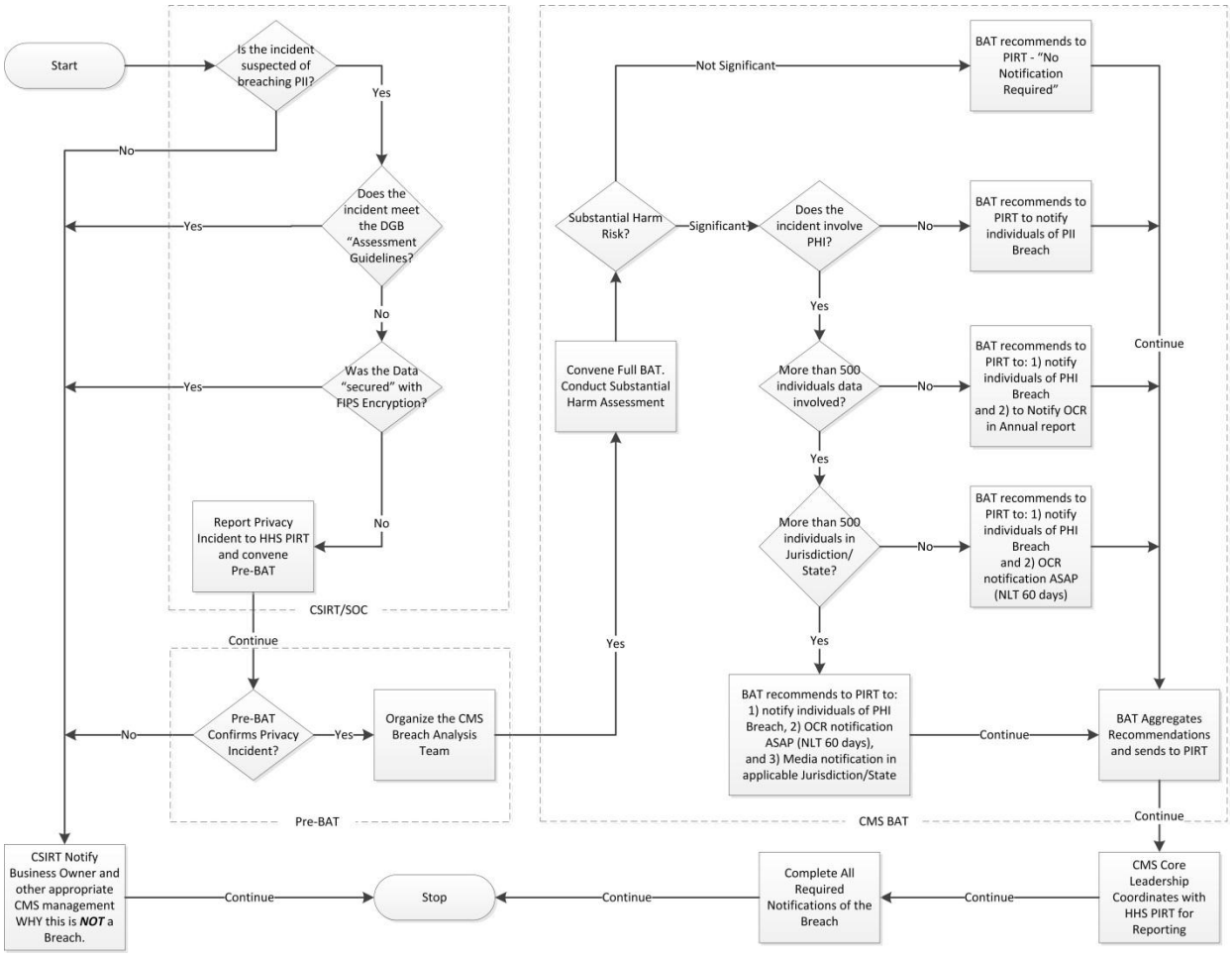
The HHS *interim rule* applies not only to HIPAA-covered entities but also to their contractors/ business associates. Under the HHS *interim rule,* a business associate must notify the covered entity with which it has a contractual relationship if any employee or agent becomes aware of a breach. Business associates shall continue to follow existing contract reporting requirements and shall ensure that CMS is promptly informed of the occurrence of a breach.

1.5.5 BREACH RESPONSE

Though all incidents must be reported to the appropriate government entities, the Office of Management and Budget (OMB) states that "agencies should bear in mind that notification of a breach when there is *little or no risk of harm* might create unnecessary concern and confusion." The HHS PIRT decision to notify, based on the CMS BAT recommendations, should be made once the level of risk involved has been assessed. As stated by OMB, *"In general, the risk of harm to the individual is higher the greater the sensitivity of the data involved. For example, a name associated with a Social Security number poses a higher risk and potential harm to the individual than a name associated with a subscription list."*

Any decision to *delay* notification should be made by the CMS Administrator or a designated individual in a senior-level position. According to the OMB, a delay may be required *"if it would seriously impede the investigation of the breach or the affected individuals."* However, any delay should not exacerbate risk or harm to any affected individual(s).

Figure 1 PII and PHI Privacy Breach Reporting Requirements



2 ROLES AND RESPONSIBILITIES

2.1 HHS ROLES AND RESPONSIBILITIES

Responding to security incidents requires coordination, collaboration, and communication between the HHS CSIRC, the HHS PIRT (for *privacy* incidents), and CMS. The level of coordination varies on the level of risk presented by an incident. Additional information about roles that support the incident response processes can be found in HHS-OCIO-2008-0001.003 *HHS Policy for Responding to Breaches of PII* (as amended) and HHS-OCIO-2010-0004 *HHS Policy for IT Security and Privacy Incident Reporting and Response* (as amended).

The following sections define roles and responsibilities for security incident response.

2.1.1 HHS CHIEF INFORMATION OFFICER (CIO)

The responsibilities of the HHS CIO include but are not limited to the following:

- Establish, implement, and enforce an HHS-wide framework to facilitate an incident response program that ensures proper and timely reporting to the United States Computer Emergency Readiness Team (US-CERT).

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.1.

2.1.2 HHS CHIEF INFORMATION SECURITY OFFICER (CISO)

The responsibilities of the HHS CISO include but are not limited to the following:

- Ensure the Department-wide implementation of federal policies and procedures related to information security and privacy incident response.
- Manage the resources that support HHS CSIRC operations.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.2.

2.1.3 HHS COMPUTER INCIDENT RESPONSE CENTER (CSIRC)

The responsibilities of the HHS CSIRC include but are not limited to the following:

- Serve as the primary entity in the Department responsible for maintaining Department-wide operational information security situational awareness and determining the overall information security risk posture of HHS.
- Serve as the lead organization for coordinating Department-wide cybersecurity information sharing, analysis, and response activities.
- Report HHS information security and privacy incidents to US-CERT.
- Serve as the Department's primary point of contact with US-CERT.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.3.

2.1.4 HHS OIG COMPUTER CRIMES UNIT (CCU)

The responsibilities of the HHS OIG CCU include but are not limited to the following:

- Investigate confirmed or suspected violations of the law pertaining to information systems.
- Coordinate with the HHS CSIRC to respond to information security incidents that involve a violation of the law.
- Provide assistance to the Department in resolving questions of suspected criminal activity and other investigative policy questions.

- Serve as the Department's central point of contact to law enforcement agencies and to the Department of Justice (DoJ).

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.4.

2.1.5 HHS OFFICE FOR CIVIL RIGHTS (OCR)

The responsibilities of the HHS OCR include but are not limited to the following:

- Enforcement of the regulatory standards and requirements in the HIPAA Privacy and Security Rule, and Notification of Breaches of Unsecured Protected Health Information under the HITECH Act, including receiving complaints or reports of alleged violations, investigation of such reports, obtaining corrective action and imposing civil money penalties as appropriate and necessary.
- Receive reports of breaches of unsecured PHI on behalf of the Secretary of HHS and refer for investigation as appropriate.
- Post on the HHS OCR website entities reporting breaches of unsecured PHI affecting 500 or more individuals.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.5.

2.1.6 HHS OFFICE OF SECURITY AND STRATEGIC INFORMATION (OSSI)

The responsibilities of the HHS OSSI include but are not limited to the following:

- Provide overall leadership for the development, coordination, application, and evaluation of all policies and activities within the Department that relate to physical and personnel security, the security of classified information, and the exchange and coordination of national security-related strategic information with other federal agencies and the national security community, including national security-related relationships with law enforcement organizations (LEOs) and public safety agencies.
- Provide current and timely information to the HHS CSIRC and OPDIV CSIRCs and other key personnel as deemed necessary.
- Ensure communications security, including secure telecommunications equipment and classified information systems, for the discussion and handling of classified information in support of the detection, defense, and response to security and privacy vulnerabilities, threats, and incidents.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.6.

2.1.7 HHS PRIVACY INCIDENT RESPONSE TEAM (PIRT)

The responsibilities of the HHS PIRT[36] are defined in the HHS *Policy for Responding to Breaches of Personally Identifiable Information (PII)* (as amended). They include but are not limited to the following:

- Evaluate breaches or suspected breaches of PII and deciding which actions should be taken.
- Provide input to and approve breach response activities for breaches involving PII.
- Assess the responsible organization's proposed course of action, risk assessments, response plan, and proposed notification activities; provide feedback; and make recommendations for improvement or course corrections in a timely manner.
- Ensure proper reporting, notification, and follow-up actions to stakeholders across relevant HHS organizational components when a breach involving PII occurs.
- Work closely with the HHS Information Security and Privacy Program to coordinate Department response activities and data collection.
- Refer HIPAA compliance breaches to HHS Office of Civil Rights (OCR) as appropriate.
- Notify appropriate internal HHS stakeholders, including the following: CMS CISO; HHS Records Officer; CMS building physical security; the HHS Assistant Secretary for Preparedness and Response (ASPR); the Office of the Inspector General (OIG); HHS Office of Civil Rights (OCR); as well as, through the HHS CSIRC and the HHS CCU, appropriate external entities such as the US-CERT and law enforcement.
- Provide notification and assessments of information breaches to the HHS Risk Management and Financial Oversight Board (RMFOB).

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.7; *HHS Policy for Responding to Breaches of Personally Identifiable Information (PII),* dated November 17, 2008; and M-08-10, *Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA).*

2.2 CMS CHIEF INFORMATION OFFICER (CIO)

The CMS CIO is responsible for the overall implementation and administration of the CMS Information Security Program. The responsibilities of the CMS CIO include but are not limited to the following:

- Establish, implement, and enforce a CMS-wide framework to facilitate an incident response program (including PII and PHI breaches) that ensures proper and timely reporting to HHS.
- Ensure the establishment of a CMS CSIRT to participate in the investigation and resolution of incidents in CMS.
- Assign the CMS CISO as the lead for the CMS CSIRT.

[36] The PIRT is formerly known as the HHS Breach Response Team (BRT). The name was changed in the July 7, 2011 issuance of the HHS-OCIO-2011-0003, *HHS-OCIO Policy for Information Systems Security and Privacy*.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.8; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.11.

2.3 CMS CHIEF INFORMATION SECURITY OFFICER (CISO)

The responsibilities of the CMS CISO include but are not limited to the following:

- Ensure CMS-wide implementation of Department and CMS policies and procedures that relate to information security and privacy incident response[37].
- Advise the CMS CIO about security breaches in accordance with the security breach reporting procedures developed and implemented by the Department and/or CMS.
- Collaborate with the HHS PIRT Coordinator when the PIRT Coordinator is engaging CMS for information collection and clarification, and sit on the HHS PIRT while CMS privacy incident and breaches are under investigation[38].
- Coordinate with the CMS SOP to ensure privacy implications are addressed when PII incident response activities occur within CMS.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.9; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.12.

2.4 CMS COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

The CMS CSIRT is the main focal point for all security and privacy incident response and reporting; and is managed under the authority of the CMS CIO and coordinated under the leadership of the CMS CISO. The responsibilities of the CMS CSIRT include but are not limited to the following:

- Serve as the primary entity in CMS responsible for maintaining CMS-wide operational information security situational awareness and determine the overall information security risk posture of CMS.

[37] NIST refers to this as an *Incident Response Plan*, which is documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's information systems(s). (Defined in NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Information Technology Systems.*) CMS develops the *Procedures* portion of this plan requirement in Vol II of the RMH.
[38] The HHS PIRT has named the CMS Director of the Office of E-Health Standards and Services (OESS) as the *only* non-Department level permanent voting member of the HHS PIRT (due to their expertise in e-health standards.) In this role, the director of OESS sits on OPDIV-level privacy incidents (for ALL OPDIVs). However, when an OPDIV experiences a significant incident or a series of incidents, the HHS PIRT will include the applicable OPDIV CISO in PIRT meetings and communications to gather and share information and to validate response plans.

- Serve as the lead organization for coordinating CMS-wide cybersecurity information sharing, analysis, and response activities.
- Report CMS information security and privacy incidents to HHS CSIRC.
- Serve as CMS' primary point of contact with HHS CSIRC.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.10; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.14.

2.4.1 CMS IT SERVICE DESK

For the purposes of incident response coordination, the *CMS IT Service Desk* is a sub-component of the CMS CSIRT, whose responsibilities include but are not limited to the following:

- Act as the first point-of-contact for security incidents or anomalies, and record information provided by the system user, Business Owner, or On-site Incident Response Authority, depending on alert source.
- Generate a CMS incident ticket to document the incident for CMS records.
- Determine if the incident relates to PII.
- Immediately refer security incidents to the CSIRT.

The *CMS IT Service Desk* may be contacted via phone at (410) 786-2580 and/or by sending an email to mailto:CMS_IT_Service@cms.hhs.gov.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.10; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.14.

2.4.2 CMS SECURITY OPERATIONS CENTER (SOC)

For the purposes of incident response coordination, the CMS SOC is a sub-component of the CMS CSIRT, whose responsibilities include but are not limited to the following:

- Coordinate and optimize CMS SOC Continuous Monitoring resources during the incident *Response Phase* to minimize enterprise impact during security and privacy incidents.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.10; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.14.

2.4.3 ON-SITE INCIDENT RESPONSE (IR) AUTHORITY

The responsibilities of the *On-site IR Authority*, who is acting as a sub-component of the CSIRT, include but are not limited to the following:

- Report (or coordinate the reporting of) the incident to the *CMS IT Service Desk* (if not already reported.)
- Serve as the system or function's focal point for security incidents for the *Identification, Response,* and *Recovery Phases*.
- Prepare organizational-level plans and procedures to address security incidents in accordance with CMS requirements.
- Provide technical support and advice for incident handling, impact assessment, and technical system management, including actions taken should standard operating procedures not cover the circumstances.
- Assist CMS CSIRT in information gathering, forensics, and reporting activities.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.10; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.14.

2.5 CMS SENIOR OFFICIAL FOR PRIVACY (SOP)

The SOP title was extended by the Department to each OPDIV to effectively meet the reporting requirements outlined in OMB M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The Department requirement for the title is outlined in OMB M-05-08, *Designation of Senior Agency Officials for Privacy*.

The responsibilities of the CMS SOP include but are not limited to the following:

- Chair the CMS Data Governance Board (DGB).
- Participate on the CMS BAT and provide direction for incidents involving compromise of individually identifiable information.
- Participate as a member of the Senior Core Leadership for Breach Notification.
- Comment on proposed notification letters.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.16.

2.6 CMS BREACH ANALYSIS TEAM (BAT)

2.6.1 CMS PRE-BREACH ANALYSIS TEAM (PRE-BAT)

The CMS Pre-BAT, managed by the CMS CSIRT, with the assistance from the Business Owner and SOP staff as necessary, reviews and triages privacy incidents, and refers to the CMS Full-BAT for a formal risk assessment. The Pre-BAT responsibilities include but are not limited to the following:

- Triage privacy incidents using the CMS Data Governance Board (DGB) -provided *Assessment Guidelines*, to properly and immediately dispose of known *privacy* incident types that, by definition, do not rise to the level of *Breach*, thus not requiring *notification*.
- Convene the Full-BAT for those PHI and/or PII-related incidents requiring a formal risk assessment, including providing background information on each incident and resource materials.
- Coordinate with the CSIRT on tracking, updating, and reporting PHI and/or PII-related incidents.
- Determine and recommend appropriate policy to apply for Pre-BAT evaluation.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Section 5.10; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.14.

2.6.2 CMS FULL BREACH ANALYSIS TEAM (FULL-BAT)

The CMS *Full-BAT* comprises management designees and senior staff appointed by the *Senior Core Leadership for Breach Notification* with the exception of the CMS CIO, the CMS CISO, the CMS Privacy Officer, and the CMS SOP who represent themselves in the CMS BAT. The manager representing the Business Owner component should be at the Group Director/Deputy level. The CIO and the SOP both hold positions as the BAT co-chairs. The voting members of the BAT are the CIO, SOP, CISO, CMS Privacy Officer, and the applicable Business Owner executive. The responsibilities of the CMS Full-BAT include but are not limited to the following:

- Analyze the risk of identity theft or health insurance fraud in accordance with OMB requirements and Departmental guidelines[39].
- Ensure reporting of a privacy incident to any other affected business or system owner.
- Conduct assessments of privacy incidents to determine recommended 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).
- Develop Government cost estimates of notification and/or credit protection services.

[39] OMB Memorandum M-07-16 provides detailed guidance including specific factors that the CMS BAT should consider in assessing the likely risk of harm caused by the breach.

- Draft 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.
- Determine and recommend how the letter and/or public notice is disseminated (e.g., by the agency, a contractor, another agency).
- Assist Business Owners in preparing scripts for Medicare call center operations and/or frequently asked questions to post, if necessary.
- Investigate credit protection services/costs for business components.
- Determine and document the likely risk of harm caused by the breach using OMB guidelines and HITECH requirements, when necessary, for breach notification.
- Recommend whether to provide notification and whether to recommend:
  - Credit protection services be offered to affected individuals in the case of PHI and/or PII-related incidents.
  - Refer BAT findings to the CMS Center for Program Integrity for further investigation.
- Provide BAT findings, including recommendations on whether to notify, to the *CMS Senior Core Leadership for Breach Notification*.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Sections 5.7 and 5.10; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Sections 5.14, 5.14, and 5.15.

2.6.3 CMS DATA GOVERNANCE BOARD (DGB)

The *CMS Data Governance Board (DGB)* provides executive leadership for developing data management principles and policies that support and improve the operation of CMS' programs. The DGB operates under the auspices of the CMS Office of the Administrator (OA).

The DGB is led by the CMS SOP, and is comprised of the executive leadership (director or deputy) of the CMS components that have a direct and substantial programmatic stake in the use of CMS data, including privacy and confidentiality. The DGB Charter reflects the make-up of the DGB.

For the purposes of *privacy* incident response, the responsibilities of the DGB include but are not limited to:

- Ensure CMS' business needs and data management practices are aligned with the agency's mission and in compliance with privacy and security protections.
- Develop criteria to ensure Business Owners and custodians of data are identified and accountable for administering data use and disclosure policies, procedures, and agreements.
- Develop and maintain *Assessment Guidelines*, for use by the CMS Pre-BAT to immediately define and ameliorate known *privacy* incident types that, by definition, do not rise to the level of *Breach*, thus not requiring *notification*.

Policy/Requirements Traceability: HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* (as amended), Sections 5.7 and 5.10;

HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Sections 5.14 and 5.16.

2.7 CMS BUSINESS OWNER

The responsibilities of the CMS Business Owner[40] include but are not limited to the following:

- Notify the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Sections 5.21, 5.22, 5.23, and 5.25.

2.8 CMS SYSTEM DEVELOPER AND MAINTAINER

The responsibilities of the CMS System Developer/Maintainer include but are not limited to the following:

- Notify the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.26.

2.9 CMS SYSTEM/NETWORK ADMINISTRATORS

The responsibilities of CMS System/Network Administrators[41] include but are not limited to the following:

- Recognize potential security violations and take appropriate action to report any such incident as required by federal regulation, and mitigate any adverse impact.
- Develop and/or execute a system termination plan to ensure that IT security breaches are avoided during shutdown, and that long-term protection of archived resources is achieved.
- Report any suspected or actual computer incidents, including the loss of control of PII and PHI, immediately to the CMS CSIRT.
- Notify the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.27.

[40] The CMS Role of *Business Owner* maps to the HHS role of System Owner, and the NIST SP 800-37 Rev. 1 role of Information System Owner. In addition, the NIST SP 800-37 Rev. 1 role of *Information Owner/Steward* and the HHS role of *Contingency Planning Coordinator* may also be fulfilled by CMS Business Owner.
[41] *System/Network Administrator* roles are inclusive of other types of administrator roles such as application administrator, Web administrator, and database administrator.

2.10 CMS CONTRACTING OFFICERS (CO) AND CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVES (COTR)

The responsibilities of the CMS COs and COTRs include but are not limited to the following:

- Notify the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.28.

2.11 CMS OFFICE OF OPERATIONS MANAGEMENT (OOM)

The responsibilities of CMS OOM include but are not limited to the following:

- Participate at the request of the CMS CSIRT and HHS CSIRC in the investigation of federal employees with regard to security incidents.
- Participate at the request of the HHS PIRT in the investigation of federal employees relative to privacy incidents and violations.
- Notify the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.30.

2.12 CMS SUPERVISORS

The responsibilities of CMS Supervisors include but are not limited to the following:

- Report any suspected or actual computer security incidents, including the loss of control of PII and PHI, immediately to the CMS CSIRT.
- Notify the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.31.

2.13 CMS FEDERAL EMPLOYEES AND CONTRACTORS

The responsibilities of CMS' employees and contractors operating on behalf of CMS include but are not limited to the following:

- Report any suspected or actual computer security incidents, including the loss of control of PII and PHI, immediately to the CMS CSIRT.

- Notify the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.32.

3 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's category.

3.1 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 required types of information for logging are:

1. Dates and times of incident-related phone calls.
2. Dates and times when incident-related events were discovered or occurred.
3. Amount of time spent working on incident-related tasks.
4. The entity or people the component has contacted or who have contacted the component.
5. Names of systems, programs, or networks affected by the incident.
6. Impact analysis.
7. The Business Owner or On-site Incident Response Authority shall maintain a chronology of the significant activities and narrative summary for final incident reports.
8. Upon recommendation for closure of an incident, *CMS IT Service Desk* and the HHS Cybersecurity Program must receive all documentation.

4 APPLICABLE LAWS/GUIDANCE

- HHS-OCIO-2010-0004, *HHS Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response*, dated April 5, 2010.
- HHS-OCIO-2008-0001.003, *HHS Policy for Responding to Breaches of PII*, dated November 2008.
- HHS-OCIO-2010-0004, *HHS Policy for IT Security and Privacy Incident Reporting and Response*, dated April 2010.

- OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006.
- NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*, dated March 2008.

5 APPROVED

Teresa Fryer
CMS Chief Information Security Officer and
Director, Enterprise Information Security Group

This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at mailto:ciso@cms.hhs.gov.