IT Security and Personally Identifiable Information (PII) Incident Response within HHS and IHS

Mark Brown
Deputy Chief Information Security Officer
Department of Health and Human Services

Ryan Chapman
Information Security Specialist
IHS Office of Information Technology

December 18, 2008

Table Of Contents

Breach Response at HHS: Definition

Breach Defined:

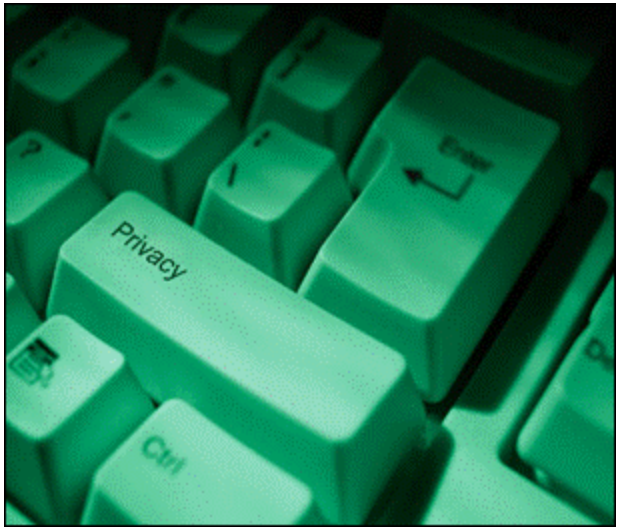
*A breach is the "loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authoized purpose have access or potential access to personally identifiable information whether physical or electronic."**

- Types of breaches include, but are not limited to:
  - Losing federal, contractor, or personal electronic devices that store PII (e.g., laptops, cell phones that can store data, disks, thumb-drives, flash drives, compact disks, etc.)
  - Sharing paper or electronic documents containing PII with unauthorized individuals
  - Posting PII to a public Website (intentionally or unintentionally)
  - Mailing hard copy documents containing PII to the incorrect address
  - Leaving documents containing PII exposed in an area where individuals without approved access could read, copy, or move for future use

* Office of Management and Budget (OMB) Memorandum (M) 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

Breach Response at HHS: Legislative History

- Congress and the Executive Branch are specifying standards and holding Agencies accountable for IT security and privacy
  - Privacy Act of 1974
  - E-Government Act of 2002 - Federal Information Security Management Act (FISMA)
  - President's Management Agenda (PMA)
  - Executive Order 13402, *Strengthening Federal Efforts to Protect Against Identity Theft*
  - Office of Management and Budget (OMB) Memoranda (M):
    - *Recommendations for Identity Theft Related Data Breach Notification*, dated September 20, 2006
    - M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007
- In response to federal mandates, HHS created a Breach Response Team (BRT) and corresponding documents
  - HHS Policy for Responding to Breaches of PII, dated November 17, 2008
  - PII BRT Charter, dated November 17, 2008
  - PII BRT Standard Operating Procedures (SOP), dated October 31, 2008



Breach Response at HHS: The Consequences

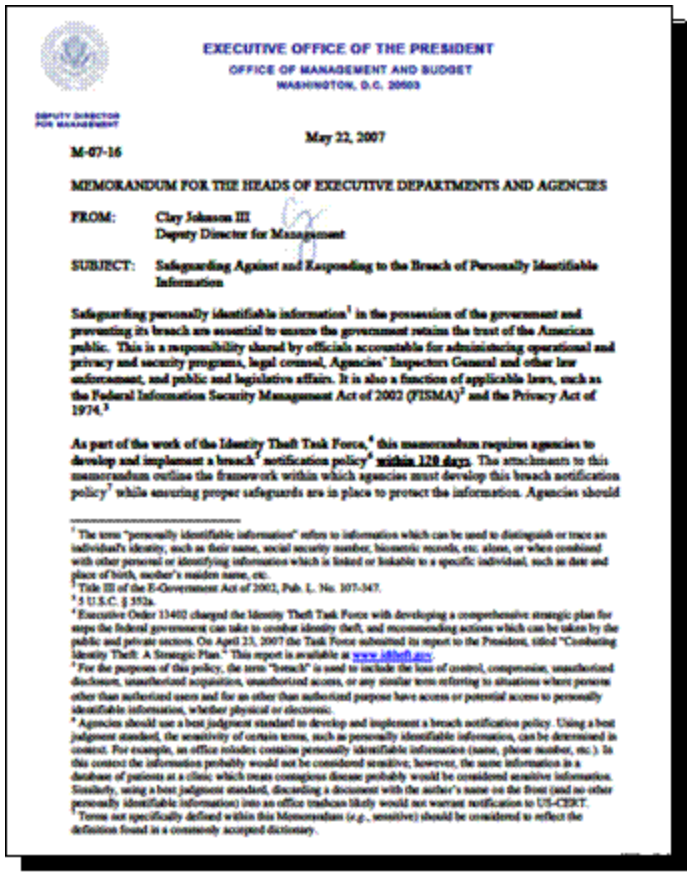
- **Consequences of IT Security and Privacy Risks:**
  - Risks to Agency / Department Reputation
    - Loss of public trust and confidence
    - Loss of credibility
    - Inability to meet its mission and vision
  - Risks to Operations
    - Breach of national security
    - Shutdown of services
  - Risk of Congressional and Oversight Scrutiny
    - Initiation of Government Accountability Office (GAO) audit
    - Summons to testify

  - Risk of Legal Action
  - Risk to Sensitive Information and Privacy
    - Shift of focus from security to legal action
    - Loss / misuse of sensitive medical information
    - Loss / misuse of proprietary information
    - Loss / misuse of intellectual capital
  - Risk of Financial Loss
    - Loss of OMB funding

Breach Response at HHS: History of the BRT

- HHS established a BRT in compliance with two OMB memoranda
  - Recommendations for Identity Theft Related Data Breach Notification, released on September 20, 2006
  - M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, released on May 22, 2007
- The BRT is comprised of several of the Department's senior leaders
- Senior leadership engages in risk analysis to determine whether a potential or confirmed breach of PII poses problems related to identity theft and/or any applicable federal law or policy

Additional information can be found within the BRT Charter, Policy, and Standard Operating Procedures located on Secure One HHS Online (http://intranet.hhs.gov/infosec/)



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR FOR MANAGEMENT

May 22, 2007

M-07-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Safeguarding personally identifiable information[1] in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA)[2] and the Privacy Act of 1974.[3]

As part of the work of the Identity Theft Task Force,[4] this memorandum requires agencies to develop and implement a breach[5] notification policy[6] within 120 days. The attachments to this memorandum outline the framework within which agencies must develop this breach notification policy[7] while ensuring proper safeguards are in place to protect the information. Agencies should

[1] The term "personally identifiable information" refers to 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 specific individual, such as date and place of birth, mother's maiden name, etc.
[2] Title III of the E-Government Act of 2002, Pub. L. No. 107-347.
[3] 5 U.S.C. § 552a.
[4] Executive Order 13402 charged the Identity Theft Task Force with developing a comprehensive strategic plan for steps the federal government can take to combat identity theft, and recommending actions which can be taken by the public and private sectors. On April 23, 2007 the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at www.idtheft.gov.
[5] For the purposes of this policy, the term "breach" is used to include the 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 personally identifiable information, whether physical or electronic.
[6] Agencies should use a best judgment standard to develop and implement a breach notification policy. Using a best judgment standard, the sensitivity of certain terms, such as personally identifiable information, can be determined in context. For example, an office rolodex contains personally identifiable information (name, phone number, etc.). In this context the information probably would not be considered sensitive; however, the same information in a database of patients at a clinic which treats contagious disease probably would be considered sensitive information. Similarly, using a best judgment standard, discarding a document with the author's name on the front (and no other personally identifiable information) into an office trashcan likely would not warrant notification to US-CERT.
[7] Terms not specifically defined within this Memorandum (e.g., sensitive) should be considered to reflect the definition found in a commonly accepted dictionary.

Photo Source: Whitehouse.gov

Breach Response at HHS: BRT's Primary Roles & Responsibilities

- Evaluate breaches or suspected breaches of personal information
- Evaluate all alternatives that are directly proportional to the incident to decide what actions should be taken
- Ensure proper and timely reporting, notification, and follow-up with stakeholders
- Work closely with the HHS Information Security and Privacy Program to coordinate Departmental response activities and data collection, as needed
- Refer Health Insurance Portability and Accountability Act (HIPAA) incidents to the Office for Civil Rights, or Centers for Medicare & Medicaid Services (CMS) Office of E-Health Standards and Services (OESS), as appropriate
- Notify appropriate internal HHS stakeholders, as directed
- Provide notification and assessment of breaches to the Risk Management and Financial Oversight Board (RMFOB)

Breach Response at HHS: Incident Response Capability

- Maintaining an incident response capability is beneficial in: *
  - Responding to incidents systematically so that the appropriate steps are taken
  - Helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services
  - Using knowledge gained during incident handling to prepare for future incidents and provide stronger protection for systems and data
  - Addressing legal issues that may arise during incidents

*National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Revision 1

Photo Source: USA.gov

Breach Response at HHS: Process

What happens when an incident involving PII is reported?

1. Operating Division (OPDIV) contact reports the incident to the HHS Computer Security Incident Response Center (HHS CSIRC) via the Internal Incident Summary form*

2. BRT Coordinator determines if the information is complete and sufficient to support the OPDIV's initial assessment

   – BRT may request CIRSC obtain additional information from the OPDIV on the details specified within the Internal Incident Summary form

3. BRT Coordinator performs initial risk assessment to determine the likelihood of losing PII, and the impact to the OPDIV if PII is exploited

Breach Response at HHS: Process (continued)

4. BRT Coordinator uses these results, plus the Risk Matrix*, to determine the overall risk level to the OPDIV and / or the Department

5. BRT Coordinator requests that the OPDIV develop a Risk Assessment and Breach Response Plan
   - BRT Coordinator forwards the Risk Assessment and Breach Response Plan to the BRT for review and comment
   - The incident is also included in the Department's PII Weekly Breach Report , which the BRT members must review and acknowledge whether any action is necessary on the open items within the report

6. BRT Coordinator informs the OPDIV of the approved documents or advises of any further recommendations

7. OPDIV implements approved risk assessment, Breach Response Plan, and additional recommendations
   - BRT determines if notification is necessary, and if so, informs the OPDIV

* The Risk Matrix can be found in the BRT Standard Operating Procedures

Table Of Contents

- Breach Response at HHS
- **Breach Response at IHS**
- Hypothetical PII Breach

Breach Response at IHS

Ryan Chapman

Information Security Specialist

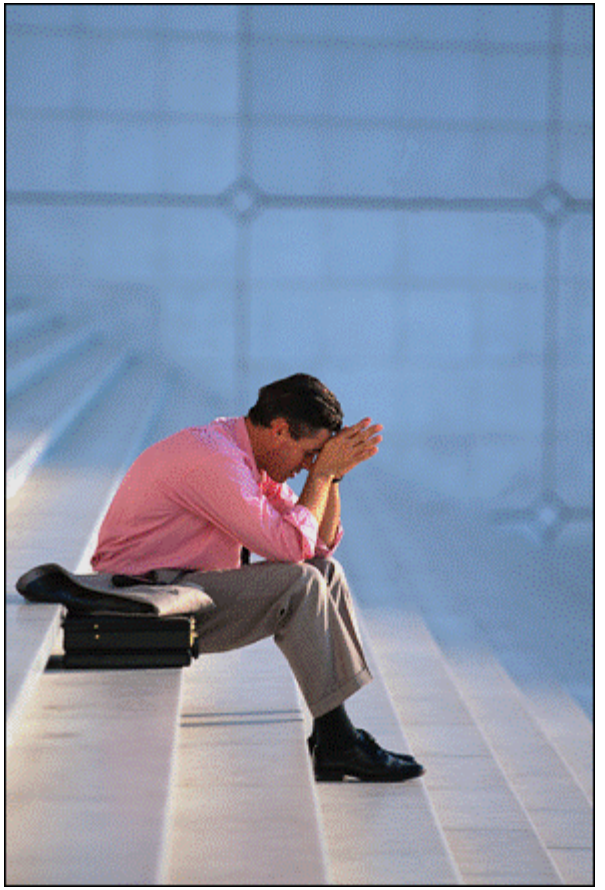
IHS Office of Information Technology

Table Of Contents

- Breach Response at HHS
- Breach Response at IHS
- **Hypothetical PII Breach**

Hypothetical PII Breach: Background

- IHS employee believes that an unencrypted Universal Serial Bus (USB) thumb drive has been lost or stolen
  - Person does not believe the USB thumb drive contained work-related materials
- Two months pass, and the employee recalls saving files from a study that may have contained PII
- Employee reports the missing USB thumb drive to IHS managers



Hypothetical PII Breach: Initial Notification of the Breach to HHS CSIRC

- IHS Managers go through the OPDIV's own breach response plan and designate it as a low risk incident
- IHS Managers complete the *Internal Incident Summary* and send the it to HHS CSIRC
  - IHS indicates that the USB drive contained the PII of more than 50,000 individuals

Hypothetical PII Breach: HHS CSIRC and BRT Involvement

- HHS CSIRC identifies the incident as containing PII and classifies it as a medium risk
- HHS CSIRC sends the *Internal Incident Summary* to the BRT
  - HHS CSIRC includes the incident in the *PII Weekly Breach Report*
- BRT Coordinator requests HHS CSIRC obtain additional information from IHS regarding the type of PII on the USB thumb drive

Hypothetical PII Breach: BRT Evaluates the Risk

- IHS provides additional information to the BRT via HHS CSIRC
- BRT convenes via teleconference to discuss the incident and requests an IHS representative join the call
  - New information revealed during the discussion indicates that the USB thumb drive was most likely stolen from a locked drawer inside an secure IHS facility
- BRT reviews the facts, discusses the potential outcomes of the lost data, and discusses the affect to the Department
- BRT categorizes the incident as a high risk given the likelihood, considering the nature and cause of threats and vulnerabilities, and the impact or potential harm that could come from a threat exploitation
- BRT requests IHS to develop a Breach Response Plan

Hypothetical PII Breach: Mitigating the Risk

- BRT asks IHS to carry out their Breach Response Plan, and draft a notification letter to the affected individuals for the BRT to review prior to release
- The IHS draft letter includes:
  - Information on the facts of the breach
  - Steps taken to remedy the situation
  - Options for affected individuals to monitor and protect their credit
- BRT approves letter and it is released to the affected individuals
- BRT will continue to follow-up and provide guidance, as necessary

EQUIFAX experian TransUnion

Failure to establish and maintain integrated security and privacy practices can have a significant impact on government agencies

IN THE HEADLINES…

Walter Reed says patient data may be compromised
The Associated Press, June 2, 2008
"Sensitive information on about 1,000 patients at Walter Reed Army Medical Center and other military hospitals was exposed in a security breach."

Man arrested in theft of 1.8 million Social Security numbers
The Associated Press, November 16, 2007
"About 1.8 million SSNs from the U.S. Department of Veteran Affairs uncovered from a home computer."

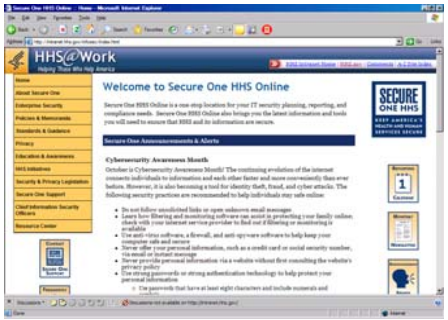
TSA seeks hard drive, personal data for 100,000
USA Today, May 5, 2007
"Personal and financial records of 100,000 TSA employees lost."

"Stolen computer hard drive contained bank account numbers, SSNs, names, and birth dates"

Secure One HHS has multiple resources to help OPDIVs implement robust information security programs

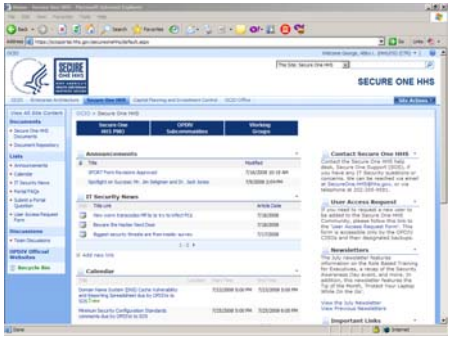
- **Secure One HHS Intranet**
  - Provides an internal online resource (http://intranet.hhs.gov/infosec/index.html)
- **Secure One HHS Internet**
  - Provides an external online resource (http://www.hhs.gov/ocio/securityprivacy/index.html)
- **Secure One HHS Portal**
  - Provides an online collaboration workspace (https://ocioportal.hhs.gov/secureonehhs/default.aspx)
- **Secure One Support (SOS)**
  - Provides support for the HHS Information Security Program
    via email at: **SecureOne.HHS@hhs.gov**
    or via phone at: **202.205.9581**

INTRANET



INTERNET

PORTAL



SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Secure One Support
SecureOne.HHS@hhs.gov
(202) 205 - 9581