



**Department of Veterans Affairs  
Office of Inspector General**

---

**Administrative Investigation  
Loss of VA Information  
VA Medical Center  
Birmingham, AL**

**To Report Suspected Wrongdoing in VA Programs and Operations  
Call the OIG Hotline – (800) 488-8244**

# Contents

	Page
<b>Executive Summary .....</b>	<b>i</b>
<b>Introduction .....</b>	<b>1</b>
Purpose.....	1
Background.....	1
Scope and Methodology .....	5
<b>Results and Conclusions .....</b>	<b>7</b>
Issue 1: Circumstances Surrounding How the Data Went Missing, the Extent and Magnitude of the Data Loss, and Whether VA Appropriately Responded to the Incident.....	7
Issue 2: Whether There Were Policies, Procedures, and Controls in Place to Properly Store and Safeguard the Missing Data .....	15
Issue 3: Whether the IT Specialist was Appropriately Authorized Access to Large Amounts of Protected Information.....	22
Issue 4: Whether the IT Specialist Complied with Research Project Protocols to Properly Safeguard Protected Information.....	34
Issue 5: Whether the Birmingham REAP Director Was Adequately Supervised, and Whether the REAP’s Director and Associate Director Adequately Managed and Supervised the Operations and Staff of the REAP .....	40
<b>Appendices</b>	
A. Under Secretary for Health Comments to Office of Inspector General’s Report ....	45
B. Assistant Secretary for Information and Technology Comments to Office of Inspector General’s Report.....	55
Attachment A .....	60
C. OIG Contact and Staff Acknowledgments.....	63
D. Report Distribution .....	64

## Executive Summary

### Introduction

On January 22, 2007, a Veterans Health Administration (VHA) Information Technology (IT) Specialist assigned to the Research Enhancement Award Program (Birmingham REAP), VA Medical Center (VAMC), Birmingham, AL, reported that a VA-owned external hard drive was missing. The external hard drive was used to back up data related to VA research projects contained on the IT Specialist's desktop computer, as well as to store other data that he was working on from a shared network. The missing external hard drive is believed to contain numerous research-related files containing personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the Centers for Medicare & Medicaid Services (CMS), Department of Health and Human Services (HHS), on over 1.3 million medical providers.

Improper disclosure of this information would be in violation of the Privacy Act of 1974, and the regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and could be used to compromise the identity of veterans and physicians and possibly used to commit Medicare billing fraud. The vast majority of the data was not password-protected or encrypted. To date, the missing external hard drive has not been recovered.

The purpose of the administrative investigation was to determine:

- The circumstances surrounding how the data went missing, the extent and magnitude of the data loss, and whether VA appropriately responded to the incident.
- Whether there were policies, procedures, and controls in place to properly store and safeguard the missing data.
- Whether the IT Specialist was appropriately authorized access to large amounts of protected information.
- Whether the IT Specialist complied with research project protocols to properly safeguard protected information.
- Whether the Birmingham REAP Director was adequately supervised, and whether the REAP Director and Associate Director adequately managed and supervised the operations and staff of the REAP.

## Results

### Issue 1

#### Notifications to VA Management and Office of Inspector General (OIG) Were Timely

Notifications of the data loss to the VAMC Information Security Officer (ISO), VA management, and OIG were timely and appropriate. The ISO quickly responded to the REAP and immediately notified the VA Security Operations Center (SOC), an organization created to track and report on data security incidents. The OIG received and reviewed the SOC report, immediately opened a criminal investigation, and arrived at the Birmingham VAMC on January 23, 2007.

#### Criminal Investigation Inconclusive in Determining How Data Went Missing

On January 23, 2007, the OIG interviewed the IT Specialist and secured his desktop computer for forensic analysis. On January 24, 2007, the Federal Bureau of Investigation (FBI) was notified and joined the investigation. Investigative efforts were also coordinated with the Birmingham Police Department. To determine how the external hard drive went missing, the criminal investigation pursued all possible leads. On February 21, 2007, OIG and FBI announced a \$25,000 reward and hotline phone number through press releases and flyers distributed in the area proximate to the Birmingham REAP. To date, no useful leads have been received by the hotline. The criminal investigation remains open.

#### Initial Notification of Magnitude of Data Loss Inaccurate

The IT Specialist's lack of candor when initially interviewed delayed accurate reporting. On February 2, 2007, following a local television newscast which announced the loss of about 48,000 records, VA issued a press release concerning the incident. The reported records were based on inaccurate information provided by the IT Specialist. The problem of providing inaccurate information on what may have been on the missing external hard drive was further compounded by the fact that the IT Specialist encrypted and/or deleted multiple files from his computer shortly after he reported the data missing, making it more difficult to determine what was stored on his desktop computer. Initially, he denied deleting and encrypting files to criminal investigators. However, after being confronted with the results of the OIG computer forensic analysis, he stated that he panicked and admitted deleting and encrypting the files in an attempt to hide the extent, magnitude, and impact of the missing data.

Recognizing that the OIG has asked VA in the past not to release specific information about data breaches without our concurrence to avoid jeopardizing the criminal investigation, the OIG notified the VA on February 10, 2007, that we had substantially pursued all significant investigative leads and that notification to all appropriate parties

would no longer compromise attempts to recover the missing data. That day, VA issued a second press release announcing that the missing data may have included sensitive VA-related information on approximately 535,000 individuals, as well as information on approximately 1.3 million physicians and other health care providers. VA and OIG made appropriate notification prior to the press release.

*Privacy Act and HIPAA Concerns Result in Letters to Veterans and Others*

On February 12, 2007, VA began sending notification letters informing each recipient that one of the files on the external hard drive may have contained his or her name, social security number (SSN), date of birth, and health information (or that of the deceased if sent to a survivor). All the letters were mailed by March 12, 2007. On April 30, 2007, VA sent additional letters to 198,760 living individuals in this group offering them the option of 1 year of free credit monitoring services.

On March 28, 2007, CMS sent a letter informing VA that there is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned, and requesting that VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring. On April 17, 2007, VA began sending notification letters to all of the 1.3 million health care providers and completed the notifications on May 22, 2007. VA also sent additional letters from May 25, 2007 to May 31, 2007, offering 1 year of free credit monitoring to 664,165 health care providers whose SSNs appear to be in the file.

*Government-wide Criteria for Assessing Risk Associated with Data Loss Lacking*

This data loss incident raises concerns over the need for Government-wide guidance and criteria on what constitutes high risk data for identity theft. Without well thought-out guidance, Federal agencies are likely to make inconsistent decisions about what protections to offer affected individuals. The question arises whether it is a prudent use of Government resources to offer a year of free credit monitoring to nearly 180,000 individuals at risk solely because their SSN was lost. Some law enforcement agencies have taken the position that release of a SSN alone does not put an individual at risk for identity theft. Because data loss is a systemic problem throughout the Government, developing criteria and guidance for assessing risk associated with a breach of sensitive data should not be relegated to any one Department. The need for Government-wide criteria is evidenced by this incident where missing data comes from more than one Federal agency.

## Issue 2

### *Birmingham REAP Managers Did Not Ensure Proper Information Security Controls to Safeguard Data Stored on External Hard Drives*

When electronic space for REAP files was nearing capacity, the Birmingham REAP Director approved the purchase of external hard drives for additional storage space. We identified no VA policy in effect at the time the external hard drive went missing that addressed the need to protect sensitive data on removable computer storage devices, unless those devices were carried outside a VA facility. However, at the local level, policies were in effect which, had they been followed, could have protected the lost data from inappropriate disclosure. On August 7, 2006, Veterans Integrated Service Network (VISN) 7 issued a policy that prohibits employees from storing sensitive data on portable devices without encryption, and assigns responsibility to local supervisors for protecting sensitive information from unauthorized disclosure.

Although VISN 7 policy required encryption on these devices, the Birmingham REAP Director did not request encryption software. Rather than utilize encryption software to protect the external hard drives, the REAP Director instituted a less reliable method of protection by depending on employees not to remove external hard drives from the office and to store them in a locked safe when not in use—measures which were not adequately monitored by managers to ensure employee compliance. In fact, several employees elected not to store their external hard drives in the safe, and at least one employee took home an external hard drive that contained privacy protected information concerning VA employees. Also, there were no records of when the safe was accessed or whether its contents were inventoried and accounted for; access to the safe was not adequately limited; and once an employee opened the safe, that employee had access to all other employees' external hard drives.

Furthermore, because the Birmingham REAP Data Security Plan did not comply with the VISN 7 policy or VA Information Resource Center (VIREC) guidance, we found that the approval of the plan by the Institutional Review Board (IRB), the Research & Development (R&D) Committee, and the Medical Center Director's office was inadequate and permitted transfer of the data when the REAP did not have adequate procedures to protect the security of the data.

### *Birmingham REAP Managers Did Not Ensure Adequate Physical Office Space Security Measures*

The Birmingham Medical Center Director moved the REAP to new office space without ensuring that its information security needs were sufficiently evaluated and ensuring that physical security measures in place at the new office were adequate. He said when he made the decision, he was unaware they stored large amounts of sensitive data on external hard drives. He did not include the ISO or the VA Police Chief in planning the

REAP move, although VISN policy requires the Director, through the ISO, to ensure that the facility meets all information technology security requirements, including adequately protecting information collected or maintained by VA.

We found physical security lacking at the new REAP site, which was located in an area noted in local media reports as requiring off-duty police patrols in the evening because of panhandlers and substance abusers. For example, there were problems securing entrance doors to the REAP. Employees reported that on several occasions in December 2006 and January 2007 the front door was not locked or was difficult to secure because it did not close properly. We were told there were several occasions during the first 3 weeks in the new location when the VA Police were called due to problems with the front door not being secure. Employees also found that the doorway from the lobby of the leased space leading into the REAP office reception area and then to an area of 25 open work cubicles was also not secured. The employees with keys to this entrance told us they routinely left at night without locking the door because of ongoing problems with the lock. These security issues were not resolved until after the external hard drive was reported missing.

#### *Position Sensitivity Level Assessments were Not Adequately Performed*

The position sensitivity level for the IT Specialist was inaccurately designated as moderate risk, which was inconsistent with his programmer privileges and resulted in a less extensive background investigation. We also noted a systemic breakdown in the involvement of managers in risk level designations. Without accurate risk designations, VA employees may receive less extensive background investigations. Furthermore, because low and moderate risk positions are not subject to periodic reinvestigation at later dates, VA may not become aware of suitability issues arising after initial hire that could call into question an employee's continued access to sensitive data. Although VA leadership directed completion of a comprehensive review of position sensitivity levels by October 31, 2006, as recommended in the OIG report dated July 11, 2006, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*, we continue to find inaccurate risk designations.

### **Issue 3**

To evaluate the process for granting the IT Specialist access to data sources and the type of data at risk, we reviewed three research projects the IT Specialist was working on. We concluded that the IT Specialist was improperly given access to multiple data sources, allowing him to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of his research projects.

PROJECT 1: The project included accessing data from several sources, including the VISN 7 Data Warehouse and the Veterans Health Information Systems and Technology Architecture (VistA). VISN 7 officials improperly gave the IT Specialist access to data from the VISN Data Warehouse that contained scrambled SSNs (known as SCRSSNS),



which are considered to be personally identifiable information. The IT Specialist was also given programmer level access to VistA at Birmingham without sufficient authorization. This allowed him to extract information from medical records, including VA employee health records and other non-veteran, non-VA employee information. In one instance, he inappropriately incorporated employee health records into a research database, compromising the privacy of VA employees and violating the terms of the protocol.

PROJECT 2: On May 17, 2004, VA entered into a Memorandum of Understanding (MOU) with CMS to obtain records on Medicare beneficiaries. VHA uses this information in research projects aimed at improving the quality and cost of VA health care. As the primary recipient of CMS data in VA, the VA Medicare Analysis Center (MAC) provides a mirror image of the data to VIREC, which then provides the Medicare data to VA researchers. MAC is also required to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it, including compliance with HIPAA and the Privacy Act.

CMS uses an independent contractor to process data requests. As such, when CMS received a data request from the MAC in 2005 for data authorized under the MOU, the request was sent to the contractor for data distribution. The contractor, however, sent VA the wrong file. Instead of sending VA the authorized Unique Physician Identification Number (UPIN) file which contains 9 fields of data, VA was sent the Medicare Physician Identification and Eligibility Registry (MPIER) file, which contains 48 fields of data that include personal identifiers and other information on over 1.3 million health care providers, nationwide. VA is not authorized to receive the MPIER file under the MOU.

While the MAC Manager believed MAC reported the improper receipt of the MPIER file to CMS or the contractor, he could not provide us with any e-mail messages or letters addressed to CMS or the contractor concerning the receipt of this file. CMS denied receiving from MAC or VHA any phone or written notification concerning the incorrect file received by MAC. Even though MAC officials were aware they were not entitled to the MPIER file, they did not return it to CMS, but retained it and sent a copy to VIREC. VIREC, in turn, inappropriately released the data to the Birmingham REAP, where it was provided to the IT Specialist. CMS officials stated that they did not learn that the wrong file was sent to VA until after the external hard drive was reported missing.

VIREC disburses Medicare data to researchers as part of a research project. This project is designed to promote the acquisition, merging, and appropriate use of Medicare and VA data for research purposes. Under this protocol, to request CMS data from VIREC the researcher must provide required justification to include IRB approval, informed consent forms, and the research project protocol that includes the use of the Medicare data requested. All data disbursed from VIREC is approved by the VIREC IRB as part of its continuing review process. In April 2006, the Birmingham REAP requested data from VIREC on health care providers for Project 2. The request listed a need for 12 data

elements, such as name, medical degree, graduation year, birth year, medical specialty, etc., for 364 medical providers. The Chairman of the Birmingham IRB approved the request in August 2006.

Despite concern over how the REAP would select the data needed for the research project out of the MPIER file, the Director of VIREC approved the release of the file on November 13, 2006. As a result, on that same day, VIREC sent the complete MPIER file containing 48 fields of data on over 1.3 million medical providers so the REAP could cull out 364 names and 12 fields of data. The MPIER file, in its entirety, was sent to the Birmingham REAP, which in turn provided it to the IT Specialist, thereby creating a situation in which he obtained far more information than entitled to under the protocol for Project 2. The IT Specialist then split the complete MPIER file into multiple databases and continued to store the original file on his desktop computer. As such, we believe the complete MPIER file is on the missing external hard drive. While this file does not contain patient health information, it does include significant amounts of sensitive information that is at risk of potentially being used to the detriment of the medical providers and Medicare.

Sending the MPIER file to the Birmingham REAP without sufficient IRB approval constituted a violation of the *Federal Policy for the Protection of Human Subjects* (45 CFR Part 46), generally known as the Common Rule. The Common Rule does not permit a researcher to initiate a change or modification to a research project protocol involving human subjects without IRB approval. The Birmingham IRB-approved project permitted researchers to obtain data on 12 variables of interest, relating to care provided by 364 physicians. The file provided by VIREC, however, contained personal identifiers on more than a million physicians who were not required for the study. This violation allowed the IT Specialist to access and store data on more than a million physicians that was not needed or approved to conduct the research, which in turn, led to the loss of Privacy Act protected information when the external hard drive went missing.

Also, because the Birmingham REAP Data Security Plan did not comply with the VISN 7 policy or VIREC guidance, we found that the approval by the IRB committee, the R&D Committee, and the Medical Center Director's Office was inappropriate and resulted in VIREC's release of the data even though the REAP did not have adequate procedures to protect the security of the data.

PROJECT 3: The IT Specialist was essentially given unfettered access to several files maintained by the VA Austin Automation Center (AAC), Austin, TX, even though the requests were not appropriately authorized. Data present on the IT Specialist's desktop computer, and believed to be stored on the missing external hard drive, allowed the linking of names, SSNs, SCRSSNs, and medical information. Much of this information most likely came from AAC files. Also the IT Specialist's access to these files did not comply with VHA policy or the Privacy Act. The failure to limit access to authorized personnel, as well as failure to develop, disseminate, and follow VHA and facility

policies and procedures governing access to multiple VA databases, created a situation in which one employee could improperly accumulate a vast amount of personally identifiable information and individually identifiable health information from multiple sources without the controls to properly safeguard the data.

#### **Issue 4**

The IT Specialist maintained data in a manner that violated the terms under which the researcher was granted a waiver from HIPAA requirements. For example, the IT Specialist did not password-protect files relating to two of the three research projects we reviewed, which was a condition for granting the waivers. The third HIPAA waiver specified that no identifiable patient information would be extracted, but the IT Specialist's files contained SSNs. In one of the projects reviewed, the IT Specialist also violated the terms of a waiver exempting the researcher from obtaining informed consent from subjects. The request for waiver indicated that patients would not be identified, yet the IT Specialist had files on his desktop computer that contained identifiers. In a second project, no waiver was granted and the informed consent stated that data would be stored on a server housed at the Birmingham Medical Center. In this instance, the IT Specialist maintained the file on his desktop, which is not a secure server. While it can be argued that the IT Specialist's desktop computer was password-protected, this protection was lost when the files were backed up on the external hard drive that went missing. Most of the files on the external hard drive were not password-protected or encrypted.

#### **Issue 5**

The Birmingham REAP Director and her subordinate managers frequently were not physically present to supervise and manage the daily operations of the REAP. The REAP Director received no supervision from the Associate Chief of Staff (ACOS) for Acute and Specialty Care, as he was the supervisor of record in name only. Also, the ACOS for Research, who is responsible for research activities at the VAMC, was not managing or supervising the activities of the REAP Director. The Medical Center Director said the REAP Director reports to the Health Services Research and Development Service, VHA Central Office, on matters relating to the governance of the REAP. He also told us that, in his opinion, the REAP Director should have no direct reporting relationship to him. However, the Chief Research and Development Officer in VHA Central Office told us he believed the facility ACOS for Research should supervise the REAP Director on most matters and be the REAP advocate within the VAMC for getting things done. Lacking any clear guidance and understanding of who is assigned responsibility to supervise the REAP Director, we believe the Medical Center Director is ultimately responsible for position management at the facility and is accountable for the supervision or lack thereof over the REAP Director.

The Birmingham REAP Director and Associate Director, both part-time physicians, did not properly manage REAP operations. Both managers elected to work primarily out of

their alternate office at the University of Alabama at Birmingham and were rarely present at the REAP. The REAP Director also did not maintain a VA e-mail account, but rather had her official VA e-mail messages automatically forwarded to a University of Alabama e-mail account. VA policy prohibits employees from keeping VA information on a non-VA system unless specifically authorized. Automatically forwarding e-mail could result in VA data being inappropriately transmitted outside VA, which could be a Privacy Act or HIPAA violation. Doing so is strictly prohibited unless specifically waived by the appropriate cyber security chain of command. We found no waiver for the REAP Director.

We believe that if these managers were more engaged in the daily operations of the REAP, the information, physical, and personnel security deficiencies cited in this report may have been prevented.

## Recommendations

### Issue 1:

**Recommendation (1):** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the IT Specialist for his inappropriate actions during the course of the investigation and for failing to properly safeguard personally identifiable information on his missing external hard drive.

**Recommendation (2):** We recommend that the Assistant Secretary for Information and Technology coordinate with the Office of Management and Budget and the President's Identity Theft Task Force to develop and issue Government-wide risk analysis criteria to determine under what conditions potential identity theft victims should be notified and offered free credit monitoring. In the interim, the Assistant Secretary for Information and Technology should re-evaluate VA policy to determine whether the loss of a solo personal identifier, such as a social security number only, would constitute a risk for identity theft for purposes of offering free credit monitoring.

### Issue 2:

**Recommendation (3):** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the Birmingham REAP Director and Associate Director for failing to take adequate security measures to protect personally identifiable information.

**Recommendation (4):** We recommend that the Assistant Secretary for Information and Technology revise VA Directive 6601 to require the use of encryption, or an otherwise effective tool, to properly protect personally identifiable information and other sensitive data stored on removable storage devices when used within VA.

**Recommendation (5):** We recommend that the Under Secretary for Health direct the Medical Center Director to re-evaluate and correct position sensitivity levels and associated background investigations for positions at the Birmingham VAMC.

**Issue 3:**

**Recommendation (6):** We recommend that the Under Secretary for Health develop, disseminate, and ensure compliance with policies regarding the release of individually identifiable health information from VISN data warehouses for research purposes to include IRB approval requirements and stress, in VHA's mandatory annual privacy training, that scrambled SSNs do not constitute de-identified data.

**Recommendation (7):** We recommend that the Assistant Secretary for Information and Technology develop and implement policies describing the conditions under which Vista programmer level access may be granted for research purposes, including whether that access is project specific or for the term of employment, and take appropriate action to remove programmer access from individuals who do not meet those conditions.

**Recommendation (8):** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the MAC and VIREC Directors for inappropriately retaining and releasing the MPIER file.

**Recommendation (9):** We recommend that the Under Secretary for Health develop a mechanism to ensure that data security plans for research projects comply with applicable information security policies and privacy policies prior to approval by the IRB.

**Recommendation (10):** We recommend that the Assistant Secretary for Information and Technology disseminate and enforce the existing Standard Operating Procedure for access to Austin Automation Center's nationwide SSN file, and issue policies and procedures regarding authorization to access all other Austin Automation Center data for research purposes.

**Issue 4:**

**Recommendation (11):** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the IT Specialist for inappropriately accessing and utilizing individually identifiable health information.

**Recommendation (12):** We recommend that the Under Secretary for Health require facility IRB compliance program audits to assess the privacy and confidentiality protections for human subjects in research, including whether the use of research data complies with information security requirements specified in HIPAA waivers or waivers of informed consent.

## Issue 5:

**Recommendation (13):** We recommend that the Under Secretary for Health ensure that the Birmingham REAP Director and Associate Director discontinue the practice of receiving their official VA e-mail at the University of Birmingham, in violation of VA policy prohibiting storage of VA information on a non-VA system, resulting in potential Privacy Act or HIPAA violations.

**Recommendation (14):** We recommend that the Under Secretary for Health assess the alignment of Birmingham REAP management positions at the Birmingham VAMC, and take action to correct the dysfunctional management structure that led to an overall breakdown of management oversight, controls, and accountability of the Birmingham REAP. This should include:

- Correction of the Birmingham REAP Director's reporting relationship from the ACOS for Acute and Specialty Care, which was in name only and resulted in the lack of actual supervision over the REAP Director's activities, to the ACOS for Research who currently has facility-wide responsibility for research programs but no line authority over REAP managers or involvement in their activities.
- Establishment of an accurate functional description and performance plan to clarify Birmingham REAP managers' responsibilities and to hold them accountable for proper administration of REAP resources, to include equipment purchases, acquisition of server space, protection of sensitive information stored on VA systems and portable devices, office space security, and compliance with applicable VA policies and procedures.
- Clarification of the Medical Center Director and ACOS for Research's responsibility and line authority over all research programs at the facility, including the Birmingham REAP.

**Recommendation (15):** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the Birmingham Medical Center Director for not ensuring appropriate management and administration of the Birmingham REAP and protection of the privacy and confidentiality of research subjects.

**Recommendation (16):** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the ACOS for Research for not ensuring appropriate management and administration of the Birmingham REAP.

## Comments

The Under Secretary for Health and the Assistant Secretary for Information and Technology concurred with our recommendations and provided acceptable implementation plans. We will follow-up to ensure all actions are fully implemented. The Under Secretary for Health suggested that our investigation did not adequately examine the responsibility of two employees outside of VHA—the CIO and the ISO—to proactively consider facility space requirements and moves to ensure that necessary IT and security requirements for government-owned and leased spaces are met. We believe that VHA managers and executives, not OI&T officials, are primarily responsible for identifying and planning for their own facility requirements, and the Medical Center Director’s actions were consistent with our understanding. The CIO’s responsibility for physical security focused on protecting network computer rooms, not user office spaces. Nevertheless, we believe that ISOs and CIOs should play a more important role in ensuring data security in VA’s research community. VHA and OI&T should continue to collaborate on such matters.

*(original signed by:)*

JAMES J. O’NEILL  
Assistant Inspector General for  
Investigations

## Introduction

### Purpose

On Monday, January 22, 2007, a Veterans Health Administration (VHA) Information Technology (IT) Specialist assigned to the Birmingham Medical Center's Research Enhancement Award Program (REAP) reported that a VA-owned external hard drive he had been using was missing. The external hard drive is believed to contain information protected by the Privacy Act of 1974 and the regulations enacted pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The VA Office of Inspector General (OIG) initiated a criminal investigation to recover the hard drive, and initiated an administrative investigation to identify the conditions existing at the Birmingham Medical Center and elsewhere that put the data at risk. The external hard drive is believed to contain personal information such as names, social security numbers (SSNs), and/or medical information on over 250,000 veterans. The hard drive is also believed to contain personal and other information on approximately 1.3 million health care providers, nationwide. To date, the external hard drive has not been recovered.

The purpose of the administrative investigation was to determine:

- The circumstances surrounding how the data went missing, the extent and magnitude of the data loss, and whether VA appropriately responded to the incident.
- Whether there were policies, procedures, and controls in place to properly store and safeguard the missing data.
- Whether the IT Specialist was appropriately authorized access to large amounts of protected information.
- Whether the IT Specialist complied with research project protocols to properly safeguard protected information.
- Whether the Birmingham REAP Director was adequately supervised, and whether the REAP's Director and Associate Director adequately managed and supervised the operations and staff of the Birmingham REAP.

### Background

The Privacy Act applies to information that is retrieved by personal identifiers and is maintained by an agency for the purpose of accomplishing its mission. The Privacy Act allows VA researchers to obtain personally identifiable information, regardless of whether it includes health information, if needed in the performance of the researcher's



official VA duties. The Privacy Act requires agencies to publish how they will use and control the data in a system of records notice in the *Federal Register*.

To improve the efficiency and effectiveness of the health care system, Congress passed HIPAA, which included provisions that required the Department of Health and Human Services (HHS) to adopt national standards for protecting the privacy of personal information. In response, HHS issued *Standards for Privacy of Individually Identifiable Health Information*, generally known as the Privacy Rule, in December 2000. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care.

The Privacy Rule applies to individually identifiable health information, or information that is created by a health care provider that relates to the medical condition of an individual and identifies the individual, or creates a reasonable basis for believing the information could be used to identify the individual. The Privacy Rule requires an individual to provide signed permission, known as an authorization, before an entity can use or disclose an individual's protected health information. Under certain circumstances the Privacy Rule permits use or disclosure of protected health information for research purposes without an individual's authorization. One way to use protected health information without an authorization is by obtaining a waiver from an Institution Review Board (IRB).

An IRB is a board, committee, or other group that reviews research proposals involving human subjects. IRBs have authority to approve, require modification to, or disapprove research activities covered by human subjects regulations. Federal agencies that are engaged in such research must comply with the *Federal Policy for the Protection of Human Subjects* (45 CFR Part 46), generally known as the Common Rule. VA is one of many Federal agencies that have adopted the Common Rule (38 CFR Part 16 – Protection of Human Subjects). As a result, all VA human subjects research must be reviewed and approved by an IRB. In order for an IRB to approve a research project, VHA Handbook 1200.5 requires that the research protocol includes "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data." Following approval of such research activities, IRBs must conduct periodic reviews of such research.

The Health Services Research and Development (HSR&D) Service, Office of Research and Development (ORD), Veterans Health Administration (VHA), provides funding to VA researchers for health care related research projects. Many of these research projects are intended to identify common organizational trends or facts from a wide variety of electronic databases and previously existing records, such as medical records of veterans who have been seen or evaluated for their health problems, which can be used to improve the quality of health care.

A REAP is a program in which VA researchers at one location who have been awarded a research grant from HSR&D Service receive additional funding for support personnel and other infrastructure items. The HSR&D Service funds seven REAPs, including the one at Birmingham VA Medical Center (VAMC). A REAP is not an organizational element in the conventional sense of a box on an organizational chart; in fact, all employees who participate in the program are officially assigned to specific services within the medical center. A REAP is headed by a Director, who is responsible for the management and integrity of all research conducted under the program. The Medical Center Director is responsible for overall operations of the facility's research service, including the REAP.

The Birmingham REAP, established in 2004, focuses on changing the practices of health care providers to ensure that they provide the latest evidence-based treatment, and on using VA databases to link the care of VA patients to more general information on the population as a whole. To achieve these objectives, the Birmingham REAP collects data on patients and medical providers from multiple sources for dozens of separate research projects. The IT Specialist responsible for the external hard drive that is missing worked on some of these projects and had information, such as names, SSNs, and addresses, that permitted him to trace individuals to medical records. When personal medical information can be traced to specific individuals for research purposes, it is considered "human subjects research."

The process of reviewing and approving human subjects research at the Birmingham VAMC begins when a principal investigator (the researcher in charge of a research project) submits a research protocol to the IRB for approval, which describes the methods the researcher will use to carry out the project. If the IRB approves the protocol, it is then submitted to the Research & Development (R&D) Committee. All research activity within the Birmingham facility is within the R&D Committee's purview. The R&D Committee, responsible for maintaining high human rights and protection standards, considers human subject protection issues as well as other matters such as the project's budget. If the protocol is approved by both the IRB and the R&D Committee, the researcher submits an application for a research grant to, for example, the HSR&D Service to fund the project. Once a research project begins, the IRB reviews it at least annually to ensure continuing compliance with the Common Rule, unless the project meets specific conditions that would exclude it from this requirement.

Dr. Warren Blackburn, Associate Chief of Staff (ACOS) for Research, Birmingham VAMC, is responsible for managing and administering the facility's research program, including implementing its Human Research Protection Program and the decisions of the IRB and R&D Committee. In particular, Dr. Blackburn is responsible for assuring the protection of human subjects in accordance with a written commitment the Medical Center Director gave to HHS, as required by Federal regulation. Dr. Blackburn is an

ex officio voting member of the R&D Committee. He is not a member of the IRB. He also does not directly supervise any Birmingham REAP employee.

At the time of our investigation, the Birmingham REAP consisted of 29 staff, including Dr. Catarina Kiefe, REAP Director; Dr. Monika Safford, Associate Director; a Data Unit; an administrative staff; and project researchers and their staff. Dr. Kiefe, a part-time VA physician with no clinical responsibilities, is required to spend 25 hours a week engaged in VA research, education, and administrative duties. She has been a VA employee since 1993. Dr. Safford, also a part-time VA physician, is required to spend 25 hours a week engaged in VA clinical, research, and administrative duties. She has been a VA employee in Birmingham since 2003. Along with the Administrative Officer, Dr. Safford is responsible for the daily administrative operations of the REAP.

The Birmingham REAP Data Unit provides researchers expertise in data gathering and statistical analysis. It consists of the Data Unit Manager, three IT Specialists, and two student program support assistants. The employee responsible for the external hard drive that went missing was one of the IT Specialists assigned to the Data Unit. He was hired effective December 14, 2003, as a full-time GS-12 employee, under a 2-year term appointment. On December 15, 2005, that term appointment was extended 1 year to December 14, 2006. On December 15, 2006, he received another 1 year extension to December 14, 2007.

The IT Specialist's duties include working with national VA databases and designing statistical programs to support Birmingham REAP research projects. While he is under the functional supervision of the Data Unit Manager, his supervisor of record is the ACOS for Acute and Specialty Care. According to the REAP Associate Director, the IT Specialist initially provided most of his support to the ACOS for Acute and Specialty Care, who also is a REAP researcher. This arrangement existed to prevent an organizational conflict of interest.

The Birmingham REAP administrative staff consists of the Administrative Officer and seven, mostly full-time, program support assistants and clerks. The Administrative Officer directly supervises three of the administrative staff. The remaining four are assigned to specific projects and report to researchers involved in those projects.

Each Birmingham REAP research project is organizationally grouped under one of five VA physicians, in addition to Dr. Kiefe and Dr. Safford, who also head research projects. The physicians do not report to Dr. Kiefe or Dr. Safford, but rather have supervisors in their respective clinical service. For example, even though Dr. Safford is the REAP Associate Director, she does not report to the REAP Director, but to her supervisor in her clinical service. Likewise, Dr. Kiefe also reports to a clinical service chief, the ACOS for Acute and Specialty Care. The research staff also includes full-time and part-time health services and nurse researchers, and health science and program specialists.

## Scope and Methodology

We interviewed the IT Specialist, Dr. Kiefe, Dr. Safford, the Data Unit Manager, other current and former REAP researchers and support staff, Dr. Blackburn, and the Medical Center Director, Mr. Y.C. Parris. We also interviewed other Birmingham Medical Center employees, including the Information Security Officer (ISO); the Chief Information Officer (CIO); the Privacy Officer (PO); the Research Service Administrative Officer; and managers and staff in the Human Resources Management Service, the Engineering Service, the Logistics Service, and the Police Service. Finally, we interviewed staff in the Office of Information and Technology (OI&T) who were stationed at the Birmingham VAMC and the Veterans Integrated Service Network (VISN) 7; the VHA Privacy Officer; the Chief R&D Officer in VA Central Office and certain of his subordinate managers; the staff in the Office of Security and Law Enforcement and the Security and Investigations Center; the Director and staff of the VA Information Resource Center (VIReC) in Hines, IL; the Director of the VA Medicare Analysis Center (MAC) in Braintree, MA; a Director in the VA Austin Automation Center (AAC); VHA Director of Healthcare Systems and Analysis; officials from the Centers for Medicare and Medicaid Services (CMS), a component of HHS; and staff at the University of Alabama at Birmingham. Nearly all the interviews were conducted in person, tape-recorded, and under oath.

We also reviewed Birmingham REAP research protocol files and IRB files; internal review reports of the data loss incident; various committee meeting minutes; documents relating to the purchase of external hard drives; personnel records; pertinent e-mail messages; and computer access documentation.

To determine the extent and magnitude of data believed to be on the missing external hard drive, we interviewed the IT Specialist, and conducted computer forensic analysis and review of the employee's desktop computer hard drive and the Birmingham REAP shared network that he accessed for additional data. To evaluate the type of data at risk, we selected three research projects for which the IT Specialist stored data on his desktop computer and the shared network drive. The IT Specialist acknowledged that he used the missing external hard drive to back up all the research data stored on his desktop hard drive and also to store additional data obtained from the shared network.

We independently verified his work on the three research projects through minutes of various meetings, IRB documents, and his project worksheet. We also located files containing specific patient identifiers and linked them with files containing protected health information. In combination, this constituted individually identifiable patient information. We compared the data on the employee's desktop computer to electronic medical records to verify that the data could be used to identify individual patients. We then evaluated the IT Specialist's access to, and use of, the data for the three projects in the context of applicable laws, regulations, policies, and procedures. These projects represent a sample of the data we believe is stored on the missing external hard drive.

Our analysis of the projects is not intended to represent a full review of all data that the IT Specialist could have stored on the missing drive.

## Results and Conclusions

### Issue 1: Circumstances Surrounding How the Data Went Missing, the Extent and Magnitude of the Data Loss, and Whether VA Appropriately Responded to the Incident

#### Findings

On January 22, 2007, a VHA IT Specialist assigned to the REAP at the Birmingham VAMC reported to his supervisors that a VA-owned external hard drive he had been using was missing from the REAP office. He had attempted to log on the internet that morning and found his wireless mouse was not working. He noticed the transmitter for the mouse and wireless keyboard was missing. He then checked the safe where he normally locked up his external hard drive and found that it was also missing. Other REAP staff noted that there were indications that someone had disturbed some of the personal objects in the office. A search of the REAP office revealed that an inexpensive micro-cassette recorder assigned to a research assistant was the only other item missing. There were no signs of forced entry of the safe or the premises.

The missing external hard drive was used to back up data contained in the IT Specialist's desktop computer, as well as other data that he was working on from a shared network. The missing external hard drive is believed to contain numerous research-related files containing personally identifiable information and individually identifiable health information involving over 250,000 veterans. The external hard drive most likely also contains information obtained from HHS on over 1.3 million medical providers. The information in question is protected by the Privacy Act and HIPAA, and could be used to compromise the identity of veterans and health care providers, and possibly be used to commit Medicare billing fraud. To date, the missing hard drive has not been recovered and there is no indication that the data on the missing external hard drive has been further compromised or used to commit Medicare fraud.

#### Notifications of VA Management and Office of Inspector General (OIG) were Timely and Appropriate

On January 22, 2007, following an unsuccessful search for the external hard drive, the Birmingham REAP Director notified the Birmingham Medical Center Director, who then notified the Birmingham VAMC ISO. The ISO quickly responded to the REAP and interviewed the IT Specialist to determine what data was on the missing external hard drive. Following the interview, the ISO immediately notified the VA Security Operations Center (SOC), an organization created by VA to track and report on data security incidents. In order to ensure timely notification of data loss cases, SOC reports are provided to the OIG on a daily basis. The OIG received and reviewed the SOC report on

January 23, 2007. VA dispatched teams from the Office of Information and Technology Oversight and Compliance Office and the Office of Research Oversight who arrived on site the week of January 28, 2007.

*Criminal Investigation Inconclusive in Determining How Data Went Missing*

On January 23, 2007, an OIG criminal investigator arrived at the Birmingham VAMC and conducted the first of four interviews of the IT Specialist, and secured the IT Specialist's desktop computer for forensic analysis. On January 24, 2007, the Federal Bureau of Investigation (FBI) was notified and joined the investigation. Investigative efforts were also coordinated with the local Birmingham Police Department.

To determine how the external hard drive went missing the criminal investigation pursued all possible leads associated with several scenarios, such as a burglary of the REAP office, the IT Specialist took the hard drive out of the office and lost it or had it stolen, a co-worker hid the drive for vengeful reasons or some other purpose, or that it was accidentally disposed of during routine housekeeping. During the course of the investigation, investigative agents visited local computer repair shops, contacted E-Bay, and questioned many individuals working or living near the REAP office, including homeless individuals who frequent the area surrounding the office. The investigation also involved conducting 48 interviews of VA, University of Alabama, and contract employees at the REAP. Latent fingerprints were developed at the REAP. Also, a number of computer forensic examinations were conducted on several VA computers in the REAP and personally-owned computers by any REAP employee thought to have some possible involvement in the loss of this drive. The fingerprint and computer forensic exams were performed with the assistance of the FBI, U.S. Secret Service, and the Birmingham Police Department. Also, two homes and five vehicles of REAP employees were searched with the permission of the owners.

Even though the IT Specialist denied ever taking the missing external hard drive from the VA facility, except for moving it from the Birmingham REAP's prior location to its current location in December 2006, investigators contacted personnel from an airline and an automobile rental company, as well as all locations in which the IT Specialist lodged during a personal vacation he took from January 11 through January 16, 2007, to determine if an external hard drive had been seen or found. All of these contacts were unsuccessful in locating the external hard drive.

On January 29, 2007, the OIG Computer Crime and Forensics Laboratory initiated a forensic analysis of the IT Specialist's desktop computer, which the ISO had identified as one of the sources of data the IT Specialist had copied to the missing external hard drive. The analysis revealed that multiple files were deleted from the IT Specialist's desktop computer during the late afternoon of January 22, 2007 (the day the external hard drive was reported missing), and that the computer recycle bin was subsequently emptied, thereby partially removing information about the deleted files. Additionally, the analysis

revealed that two files containing significant amounts of data were password-protected that same afternoon, and another one was deleted after normal business hours that same day. On January 31, 2007, during an interview with OIG investigators, the IT Specialist denied deleting and password-protecting files on January 22, 2007. However, after being confronted with the results of the forensic analysis, he stated that he panicked and admitted deleting the files in an attempt to hide the extent and magnitude of the missing data.

On February 21, 2007, OIG and FBI announced a \$25,000 reward and hotline phone number through press releases and flyers distributed in the area proximate to the Birmingham REAP. To date, no useful leads have been received by the hotline. We also investigated all reports of veterans' identity thefts in the area, one of which resulted in the identification of three individuals responsible for one of the identity thefts. Two of these individuals were subsequently arrested by the Montgomery, AL, Police Department, and indictment of the third is imminent. We were able to confirm that none of the reported identity theft issues were related to the Birmingham data loss incident. The criminal investigation of the missing external hard drive remains open.

Analysis of the Missing Data

It was reported that the missing external hard drive was used to back up data contained on the IT Specialist's desktop computer, as well as other data he was working on from a shared network. To determine the nature and extent of data believed to be stored on the missing external hard drive, the OIG, with cooperation and assistance from the Birmingham ISO and a VA database specialist, initiated a data review on February 1, 2007.

The analysis identified a total of 439 electronic folders containing 3,583 files of data. While 11 of these files were password-protected, we were able to open and review 8 of them. Other than the three files that remain protected, we opened and reviewed all remaining files. Based on our review, we identified 79 folders that contained personally identifiable information and/or individually identifiable health information. Most notably, we identified 72 folders that contained 535,103 SSNs; and 17 folders that contained the name, address, SSN, date of birth (DOB), phone number, and/or medical information, such as medical diagnosis and drug prescriptions, of 17,812 veterans. Following is a more detailed breakout of the analysis.

<b>Folders</b>	<b>Records</b>	<b>Personal Identifiers</b>
2	92	Name, SSN, DOB, and Medical Information
3	8,082	Name, SSN, and Medical Information
5	1,819	Full Name, SSN, and Medical Information
4	14,527	SSN and DOB
16	477,696	SSN
42	32,887	SSN and Year of Birth
2	3,861	Name, Address, Phone Number, and Medical Information
2	5,034	Name, Address, and Medical Information
1	829	Name, Phone Number, and Medical Information
2	42	Name and Medical Information



We also identified a file that contained a significant amount of information on over 1.3 million health care providers, nationwide. This file was originally provided to VA from the Centers for Medicaid & Medicare Services (CMS), HHS (see Issue 3 for a more detailed discussion of this data). The data in this file is provided to VA primarily for research purposes. For each provider there are 48 fields of data that, collectively, could be potentially used to compromise the identity of physicians and other health care providers and possibly commit Medicare billing fraud. To date, there is no indication that the data has been used to commit Medicare fraud.

On February 7, 2007, OIG provided the OI&T electronic copies of all files, as well as our analysis of the data, to allow the Department to further analyze the contents for notification and credit monitoring responsibilities.

#### Notification of Congress and the Media

Following a February 2, 2007, newscast by a local Birmingham television station reporting the data loss, VA issued a press release announcing that “an employee reported a government-owned, portable hard drive used by the employee at a Department facility in Birmingham, Ala. – and potentially containing personal information about some veterans – is missing and may have been stolen.” VA advised Congress that the loss involved approximately 48,000 records, of which 28,000 were password-protected. VA based this estimate on the information the IT Specialist provided the ISO on January 22, 2007.

Recognizing that the OIG has asked VA in the past not to release specific information about data breaches without our concurrence to avoid jeopardizing the criminal investigation, the Inspector General notified the VA Chief of Staff on February 10, 2007, that the OIG had substantially pursued all significant investigative leads and that notification to all appropriate parties would no longer compromise OIG attempts to recover the missing data.

On February 10, 2007, VA issued a second press release announcing that the Department had learned that “data files the employee was working with may have included sensitive VA-related information on approximately 535,000 individuals...” as well as “information on approximately 1.3 million non-VA physicians – both living and deceased...” VA and OIG made appropriate notification prior to the press release.

#### Risk Analysis and Notification of Impacted Parties

The Privacy Act requires notification to individuals who may have had their personally identifiable information compromised. Likewise, HIPAA requires notification to individuals who may have had their individually identifiable health information improperly released. Also, with enactment of the Veterans Benefits, Health Care, and Information Technology Act of 2006, on December 22, 2006, (P.L. 109-461, Title IX,

Information Security Matters), VA is required, in the event of a data breach with respect to sensitive personal information, to obtain a risk analysis of the data. Based on the potential for misuse of the data, VA is to provide credit protection services. The law also required VA to prescribe interim regulations for satisfying the provisions of the law pertaining to, among other things, the data breach analysis, notification, and credit monitoring.

Subsequent to the reported loss of the Birmingham REAP data but prior to receiving the results of the OIG analysis of this data on February 7, 2007, VA senior management concluded that anyone whose SSN was thought to be contained in any of the missing files, irrespective of the ability of anyone possessing this data to match an SSN with a name or any other personal identifier, should be notified and offered credit protection. The basis for this decision was a memorandum issued on November 7, 2006, by the VA Assistant Secretary for Information Technology. The memorandum, issued to all VA Under Secretaries, Assistant Secretaries, and Other Key Officials, defined personally identifiable information as the following:

- Name and date of birth
- Name and full social security number
- Full social security number only
- Name, full social security number, and date of birth

The memorandum states that “in the event of a data loss involving individual and personal information as defined above, VA officials have a responsibility to notify the individual(s) of the loss in a timely manner and to offer these protection services.”

This approach was consistent with Office of Management and Budget (OMB) guidance. On September 20, 2006, the OMB Deputy Director for Management issued a memorandum to the Heads of Departments and Agencies, offering recommendations for identity theft related data breach notifications, which stated that “an SSN standing alone can generate identity theft.”

Analysis of Lost VA Data: After analyzing the VA research files thought to be on the missing external hard drive, VA was able to identify 254,330 unique SSNs. This was refined down from the 535,103 SSNs in the OIG data by eliminating duplicate SSNs. VA determined that each of these individuals or their survivors should be notified of the data loss, and those individuals still living should be offered one year of free credit protection services. VA matched the SSNs from the missing data files with a VA system in order to obtain names and current addresses for each individual or their survivor.

On February 12, 2007, VA sent the first of these notification letters informing each recipient that “one of the files on the portable hard drive may have contained your name, social security number, date of birth, and health information (or that of the deceased if sent to a survivor).” The last of these notification letters were mailed on March 12, 2007. On April 30, 2007, VA sent letters to the 198,760 living individuals in this group offering them the option of 1 year of free credit monitoring services.

Loss of CMS Data: Following verification that the missing external drive most likely contained the CMS file with information on approximately 1.3 million health care providers, VA requested assistance from HHS to do a risk analysis of the CMS data. On March 28, 2007, the CMS Chief Information Officer & Director, Office of Information Services, sent a letter to the VA Assistant Secretary for OI&T informing him that, based on the information provided, there is a high risk that the loss of the personally identifiable information may result in harm to the individuals concerned. The letter requested that “VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file.” In response, on April 17, 2007, VA began sending notification letters to all of the 1.3 million health care providers and completed the notification process on May 22, 2007. VA also sent additional letters from May 25, 2007 to May 31, 2007, offering 1 year of free credit monitoring to those 664,165 health care providers whose SSNs appear to be in the file.

### Lack of Government-wide Criteria

This data loss case raises concerns over the lack of Government-wide guidance and criteria on how to make such assessments. Without well thought-out and planned guidance, Federal agencies are likely to continue to make inconsistent decisions about what protections to offer affected individuals. This is critical in that a very liberal use of high risk levels can result in spending millions of dollars in taxpayer money needlessly. For example, some law enforcement agencies have taken the position that release of a SSN alone does not put an individual at risk for identity theft. On the other hand, being too conservative in defining the criteria for risk levels associated with misuse of specific types of data may result in under-notification and lack of credit protection services to those who need and deserve it.

Developing the criteria and guidance for assessing risk associated with a breach of sensitive information should not be relegated to any one Department. An example of why Government-wide criteria is needed is evidenced in the Birmingham data loss case, where the missing data is from more than one Federal agency.

On April 30, 2007, the Government Accountability Office (GAO) issued a report (GAO-07-657) titled “Privacy: Lessons Learned about Data Breach Notification,” in which they recommended that “the Director of OMB develop guidance for federal

agencies on conducting risk analyses to determine when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring to assist individuals at risk of identity theft as a result of federal data breach.” This report references another GAO report (GAO-06-833T) titled “Privacy: Preventing and Responding to Improper Disclosures of Personal Information,” which noted the following:

- Notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion.
- Sending too many notices, based on overly strict criteria, could render all such notices less effective, because consumers could become desensitized to them and fail to act when risks are truly significant.
- The costs associated with notification are not insignificant for either agencies or individuals.

The OIG preliminary analysis of the 3,583 VA research files believed to be on the missing external hard drive indicated that, with the exception of the CMS health care provider file, only about 10,000 of the individuals in these files could be identified by name and SSN.

## **Conclusion**

Upon notification on January 22, 2007, of the disappearance of an external hard drive, notification within VA was both timely and appropriate. The SOC notification procedures facilitated the prompt January 23, 2007, response by OIG law enforcement personnel to Birmingham. The complexity of the data file structure extended the time it took OIG and VA to fully understand what personal identifiers may have been lost. Additionally, the IT Specialist’s lack of candor when initially interviewed delayed accurate reporting of the true magnitude of the loss to Congress, veterans, health care providers, and the public.

Our review of the IT Specialist’s desktop computer and network share data disclosed 3,583 files of data that may be on his external hard drive. Only 11 files had been encrypted or password-protected. On February 7, 2007, OIG provided VA the results of our data analysis. On February 12, 2007, VA began sending notification letters informing each recipient that one of the files on the portable hard drive may have contained the recipients’ name, SSN, DOB, and health information (or that of the deceased if sent to a survivor). All letters were mailed by March 12, 2007. On April 30, 2007, VA sent additional letters to 198,760 living individuals in this group offering them the option of 1 year of free credit monitoring services.

On March 28, 2007, CMS sent a letter informing VA that there is a high risk that the loss of the personally identifiable information may result in harm to the individuals concerned, and requesting that VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file. In response, on April 17, 2007, VA began sending notification letters to all of the 1.3 million health care providers and completed the notification process on May 22, 2007. VA also sent additional letters from May 25, 2007 to May 31, 2007, offering 1 year of free credit monitoring to those 664,165 health care providers whose SSNs appear to be in the file.

This data loss incident raises concerns over the lack of Government-wide guidance and criteria on what constitutes high risk data for identity theft and credit protection services. Without well thought-out guidance, Federal agencies are likely to make inconsistent decisions about what protections to offer affected individuals. The question arises whether it is a prudent use of Government resources to offer a year of free credit monitoring to nearly 180,000 individuals at risk solely because their SSN was lost in this breach. For example, some law enforcement agencies have taken the position that release of a SSN alone does not put an individual at risk for identity theft. Because data loss is a systemic problem throughout the public and private sector, developing criteria and guidance for assessing risk associated with a breach of sensitive information should not be relegated to any one Department. An example of why Government-wide criteria is needed is evidenced in the Birmingham data loss case, where some of the missing data is from another Federal agency.

## **Recommendations**

**Recommendation (1).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the IT Specialist for his inappropriate actions during the course of the investigation and for failing to properly safeguard personally identifiable information on his missing external hard drive.

**Recommendation (2).** We recommend that the Assistant Secretary for Information and Technology coordinate with the Office of Management and Budget and the President's Identity Theft Task Force to develop and issue Government-wide risk analysis criteria to determine under what conditions potential identity theft victims should be notified and offered free credit monitoring. In the interim, the Assistant Secretary for Information and Technology should re-evaluate VA policy to determine whether the loss of a solo personal identifier, such as a social security number only, would constitute a risk for identity theft for purposes of offering free credit monitoring.

## **Issue 2: Whether There Were Policies, Procedures, and Controls in Place to Properly Store and Safeguard the Missing Data**

### **Findings**

Birmingham REAP managers did not take adequate information, physical, or personnel security measures to protect sensitive data from potential loss or disclosure. External hard drives were purchased with little consideration given to how sensitive data would be secured. Rather than utilize encryption software to protect data stored on external hard drives, managers instituted a less reliable method of protection by depending on employees not to remove external hard drives from the office and to store them in a safe when not in use—measures which were not adequately monitored by managers to ensure employee compliance. Physical security concerns at the new REAP office site went unaddressed until the data loss was reported, and procedures to determine position sensitivity levels resulted in inaccurate assessments of position risk and less extensive background investigations

#### *Local Policies Not Followed in the Purchase or Use of External Hard Drives and Birmingham REAP Managers Did Not Ensure Proper Security Controls Were in Place to Safeguard Data*

When space for REAP files on the Birmingham VAMC server was nearing capacity, the REAP Director approved the purchase of external hard drives as an interim solution to accomplish their work. In making her decision, she relied on the REAP Associate Director; the IT Specialist; and the Data Unit's former Program Analyst, who she believed all met with the ISO in August 2006, in determining to use portable external hard drives to satisfy their need for additional electronic storage space. The ISO told us, however, that he was not aware of the REAP's need for additional server space, was not involved in the decision to purchase the hard drives, and did not know that they had been purchased until the external hard drive was reported missing.

Although some attempts to obtain additional server space were made, we found that no one actually made a timely request to the local Chief Information Officer (CIO), the local IT Network Manager, or ISO for additional space and none was obtained. Both the local CIO and ISO told us that the REAP could have had additional server space had someone officially requested it. Had this been done there would have been no reason to purchase the external hard drives.

The Birmingham REAP Director told us that she agreed to the purchase and believed it was a viable solution to their data storage problem because the external hard drives were never to be taken offsite and were to be locked in the office safe when not in use. Other officials involved in the purchase process included the Research Service Administrative

Officer, Birmingham VAMC; the VHA Research and Development Computing Center Network Administrator, ORD, Baltimore, MD; and a representative in the Compliance Management Division, Office of Cyber and Information Security (OCIS), OI&T, VA Central Office. However, these officials limited their review to such factors as the completeness of the request, accuracy of pricing, and whether the item was a banned technology or posed a risk to the VA infrastructure. They did not focus on data security.

We identified no VA policy in effect at the time the external hard drive was discovered missing that addressed the need to protect sensitive data on removable computer storage devices, unless those devices were carried outside a VA facility. In February 2007, after this incident occurred, the VA Secretary issued Directive 6601, which requires all employees to have permission from their supervisor and ISO to use removable storage devices, and requires that removable devices containing sensitive information have protective features approved by the local senior OI&T official. However, the policy requires encryption only if the removable device is taken outside a “VA protected environment.” VHA policy was limited to a June 27, 2006, memorandum to the VA research community from the Principal Deputy Under Secretary for Health and the Chief Research and Development Officer, who asked each Research Office to ensure that as little sensitive information as possible be stored on portable computer hardware regardless of its location.

At the local level, policies were in effect which, had they been followed, could have protected the lost data from potential risk. For example, the Birmingham REAP Data Security Plan for protected health information, prepared by Data Unit employees, requires that data “be stored only on a computer operating within the VA network, which is protected by a firewall maintained by the VA Central Office and...accessed only by use of a password.” The REAP plan further states that “all data will be kept on a secure VA drive.”

VISN 7 Automated Information System Operational Security Policy Memorandum 10N7-115, dated August 7, 2006, prohibits employees from storing sensitive data on portable devices without encrypting them; assigns responsibility to local supervisors for protecting sensitive information generated or used by their staff from unauthorized disclosure and limiting employee access to sensitive data to the minimum necessary to carry out their assigned duties; and provides that ISOs fully participate in the risk analysis of new equipment acquisitions. Although VISN 7 policy required encryption on these devices, the Birmingham REAP Director did not request encryption software when the drives were purchased because the IT Specialist told her that VA had not approved any encryption software for external drives. She said the fact that the drives were to be used only on-site made encryption less of an issue.

Further, according to the Data Unit Manager, who had assumed her position by the time the last external hard drives were received, any encryption software the Birmingham REAP used had to be VA-approved and installed. We confirmed that at the time the

drive was reported missing VA had no agency-wide approved encryption software for external hard drives. However, the local CIO told us VA employees were allowed to encrypt their external hard drives prior to VA approving agency-wide encryption software. He said that if the REAP had told him they had purchased the external hard drives, he would have identified appropriate software and authorized them to install it. He also told us that after the external hard drive was reported missing he did identify encryption software that could have been made available for their use.

The Birmingham REAP Director and Associate Director believed that external hard drives were a viable solution to the REAP's data storage problem because the drives were never to be taken off-site and were to be locked in the office safe. This solution, however, was not well-founded. The REAP Director and Associate Director did not ensure that employees consistently followed the REAP's internal procedures of locking their external hard drives in the safe. Several employees who were assigned an external hard drive told us they stored it in a locked cabinet rather than the safe. An inventory performed by Birmingham REAP employees on January 22, 2007, revealed that only 6 of the 15 drives were secured in the safe at that time. Employees told us that of the remaining nine drives, four were in locked cubicle storage in the open office space, three were in locked private offices, one was at the Administrative Officer's residence, and one was missing. The Administrative Officer acknowledged he had taken his external drive home and, although he told us he did not have sensitive data on that drive, our review of its contents disclosed that VA employee SSNs were in some of the files.

Also, access to the safe was not adequately limited; according to the Birmingham REAP Administrative Officer, seven employees had the combination to the safe. There were no records of when the safe was accessed or whether its contents were inventoried and accounted for. Once an employee opened the safe, he or she had access to any of the external hard drives or other sensitive media stored there. The practice of using the safe to secure the drives was not adequate to prevent an employee with the safe combination from borrowing another employee's external hard drive and accessing its data.

#### *Birmingham REAP Managers Did Not Take Adequate Physical Office Space Security Measures*

We noted deficiencies in facility security, both in planning for the REAP's move to new space in December 2006 and after the move occurred. The Birmingham Medical Center Director moved the REAP to new office space without ensuring that its information security needs were sufficiently evaluated and without ensuring that physical security measures in place at the new office were adequate. He said when he made the decision to move the REAP, he was unaware they stored large amounts of sensitive data on external hard drives. He did not include the ISO or the VA Police Chief in planning the REAP move, although the VISN Automated Information Systems (AIS) Operational Security Policy requires the Director, through the ISO, to ensure that the facility meets all information technology security requirements, including adequately protecting



information collected or maintained by VA. While the Director claimed that the Police Chief conducted a full physical security survey prior to the move, the Police Chief told us he conducted no such survey and that VA Handbook 730 does not require annual surveys for leased office space.

We found physical security lacking at the new REAP site, which was located in an area with vacant buildings, restaurants, and nightclubs, and noted in local media reports as requiring off-duty police patrols in the evening and attracting panhandlers and substance abusers. Only two lockable doors were between the street and the office where the external hard drives were stored. In addition to the fact that not all external hard drives were locked in the safe, the safe was neither sufficiently heavy nor anchored to prevent someone from removing it from the building.

There were also problems securing entrance doors to the REAP. Employees reported that on several occasions in December 2006 and January 2007 the front door was not locked or was difficult to secure because it did not close properly. The Administrative Officer told us there were several other occasions during the first 3 weeks in the new location when the VA Police were called due to problems with the front door not being secure. Employees also found that the doorway from the lobby of the leased space leading into the REAP office reception area and then to an area of 25 open work cubicles was not secured. The employees with keys to this entrance—the Administrative Officer and two administrative employees—told us they routinely left at night without locking the door because of an ongoing problem with the lock.

These security issues were not addressed and resolved until after the external hard drive was reported missing because no one brought them to the landlord's attention and the Birmingham REAP Administrative Officer did not follow up with other VA entities to ensure reported problems were being adequately addressed.

#### *Position Sensitivity Level Assessments Not Adequately Performed*

The IT Specialist, who had programmer privileges with the ability to access, edit, and delete sensitive information in the Veterans Health Information Systems and Technology Architecture (VistA) system at the Birmingham VAMC, occupied a position that was incorrectly designated as moderate risk. This decision resulted in completion of a less extensive background investigation, which does not subject the employee to periodic reinvestigation at a later date unless disqualifying suitability issues occur. Another IT Specialist whose responsibility was limited to developing and maintaining research websites was also designated as moderate risk by the VAMC Personnel Security Officer (PSO) in 2006, even though the Network Human Resource Officer had earlier designated this position as high risk. Other Birmingham REAP positions with access to large volumes of sensitive information were designated as low risk. These inaccuracies arose because of a breakdown in communication among the facility's PSO, the ISO, and REAP managers.

Inaccurate risk designations continue to exist despite VA-wide efforts to review and correct them as a result of recommendations in OIG report dated July 11, 2006, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*, where we found that VA employees either did not have appropriate sensitivity level designations or designations were inaccurate.

VA Directive 710 requires the identification of a position as a high, moderate, or low risk level based on the potential to adversely impact the efficiency and integrity of the Federal service. Accurate risk level designations are important because they are used to determine the scope of the background investigation required for the employee who occupies the position. Facility directors are required to ensure that risk level designations are periodically reviewed by appropriate officials, including each organization's ISO. A VHA policy supplement suggests risk designations for common occupational titles, noting that designations may need to be adjusted for uniqueness, uniformity, and information technology risks. VISN 7 policy, AIS Operational Security Policy, dated August 2006, requires that local managers participate with the ISO and the Human Resources Management Officer to determine the appropriate sensitivity level designation for positions under their control.

Beginning in 2005, a PSO was hired to correct serious problems in the Birmingham VAMC personnel suitability program due to the lack of risk designations. While our review of the records for selected Birmingham REAP employees showed that risk level designations and background investigations were completed, we found instances where the levels of potential risk were inconsistent with employees' actual job duties and responsibilities. Overall, we noted a systemic breakdown in communication with managers in the determination of risk levels—the PSO told us that he relied on the ISO to communicate with service chiefs about a position's unique risk factors, but the ISO told us that he did not consult with service chiefs during this process.

We found that the IT Specialist position was inaccurately designated as moderate risk in spite of the granting of programmer privileges in 2004. This inaccuracy occurred even after the Administrative Officer for the Research Service initiated inquiries with the Network ISO and the facility's Acting Chief of Human Resources Management to ensure the IT Specialist was assigned the proper risk level and had the appropriate clearance enabling him to access the data as a programmer. When the PSO reviewed the position in January 2006, he assigned the position a moderate risk level without receiving input from REAP managers; rather, he based the decision on the position description and the VHA policy supplement. The ISO told us the IT Specialist's position was clearly high risk based on programmer privileges but that he overlooked this and concurred with the PSO's moderate risk assessment.

Without accurate risk designations, VA employees may receive less extensive background investigations. Furthermore, because low and moderate risk positions are not subject to periodic reinvestigation at later dates, VA may not become aware of suitability

issues arising after initial hire that could call into question an employee's continued access to sensitive data. Although VA leadership directed completion of a comprehensive review of position sensitivity levels and background investigations by October 31, 2006, we continue to find the same problem of inaccurate risk designations outlined in our July 11, 2006, report.

## **Conclusion**

Medical Center managers' failure to adopt information, physical, and personnel security practices at the Birmingham REAP office put protected personal and health care information at risk of loss or compromise. The REAP Director and others decided to purchase external drives with insufficient consideration given to data security needs.

We identified no VA policy in effect at the time the external hard drive was discovered missing that addressed the need to protect sensitive data on removable computer storage devices, unless those devices were carried outside a VA facility. At the local level, policies were in effect which, had they been followed, could have protected the lost data from potential risk.

REAP management believed that external hard drives were a viable solution to their data storage problem because the drives were never to be taken offsite and were to be locked in the office safe. This approach, however, was not effectively implemented or monitored. Access to the safe was not adequately limited; there were no records of when the safe was accessed or whether its contents were inventoried and accounted for, and once an employee opened the safe, he or she had access to any of the external hard drives or other sensitive media stored there. Also, management did not ensure that employees consistently followed the REAP's internal security procedures of locking their external hard drives in the safe. Several employees stored their external hard drive in a locked cabinet rather than the safe, and at least one employee took an external hard drive home that contained VA employee SSNs.

While we could identify no VA policy prohibiting the use of a safe as a means to help secure external hard drives, the procedures instituted by the REAP Director and Associate Director for using the safe were insufficient for limiting employee access to sensitive data in the safe to the minimum necessary to carry out their assigned duties as required by VISN 7 policy. Furthermore, allowing such extensive access to the safe by REAP employees would permit those employees to access personal health information related to other research projects without prior IRB approval. Had the external hard drives been encrypted or access to the safe limited, employees would not have had this degree of unfettered access. The procedures associated with using the safe were inconsistent with generally accepted security business practices. Therefore, we find the procedures used by the REAP to secure its external hard drives in the safe were clearly an inadequate substitute for encryption protection.

Physical security of the building and office space was also inadequate. When the REAP moved to a new office location, basic security measures were not instituted and the Medical Center Director did not involve the Police Chief or ISO in security planning. Problems with the security of two REAP entrance doors were not resolved in a timely manner.

Lastly, the position sensitivity level of the IT Specialist's position was inaccurately designated as moderate risk, which was inconsistent with his programmer privileges and resulted in a less extensive background investigation. We also noted a systemic breakdown in the involvement of managers in risk level designations. Without accurate risk designations, VA employees may receive less extensive background investigations. Furthermore, because low and moderate risk positions are not subject to periodic reinvestigation at later dates, VA may not become aware of suitability issues arising after initial hire that could call into question an employee's continued access to sensitive data. Although VA leadership directed completion of a comprehensive review of position sensitivity levels and background investigations by October 31, 2006, as recommended in our July 11, 2006, report, we continue to find inaccurate risk designations.

### **Recommendations**

**Recommendation (3).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the Birmingham REAP Director and Associate Director for failing to take adequate security measures to protect personally identifiable information.

**Recommendation (4).** We recommend that the Assistant Secretary for Information and Technology revise VA Directive 6601 to require the use of encryption, or an otherwise effective tool, to properly protect personally identifiable information and other sensitive data stored on removable storage devices when used within VA.

**Recommendation (5).** We recommend that the Under Secretary for Health direct the Medical Center Director to re-evaluate and correct position sensitivity levels and associated background investigations for positions at the Birmingham VAMC.

### **Issue 3: Whether the IT Specialist was Appropriately Authorized Access to Large Amounts of Protected Information**

#### **Findings**

To evaluate the process for granting the IT Specialist access to data sources and the type of data at risk, we reviewed three research projects the IT Specialist was working on. We concluded that the IT Specialist was improperly given access to multiple data sources, allowing him to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of the projects he was working on. We believe much of this information was stored on the missing external hard drive. Following are the results of our review of each project.

**Project 1: This project involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medications to improve glucose levels, cholesterol, and blood pressure.**

The protocol for Project 1 included accessing data from several sources, including the VISN 7 Data Warehouse and VistA. VISN 7 officials improperly gave the IT Specialist access to data from the VISN Data Warehouse that contained SCRSSNS, which are considered to be personally identifiable information according to VHA Handbook 1605.1, Appendix C. The IT Specialist was earlier given programmer level access to the VistA system at Birmingham without sufficient authorization. This allowed him to extract information from medical records, including VA employee health records and other non-veteran, non-VA employee records, as well. In one instance, he inadvertently incorporated employee health records into a research database, compromising the privacy of VA employees.

#### *IT Specialist Inappropriately Obtained Individually Identifiable Health Information from the VISN 7 Data Warehouse and the Medical Center's VistA Database*

VHA Handbook 1200.5, *Requirements for the Protection of Human Subjects in Research*, issued July 15, 2003, requires Institutional Review Board (IRB) approval for research involving human subjects. The IT Specialist's access to the VISN 7 Data Warehouse was in violation of this policy.

In February 2001, VISN 7 developed the Data Warehouse for general administrative purposes. The Data Warehouse contains information on medical care provided to individual veteran patients from multiple VA medical facilities. In September 2003, the VISN established procedures for researchers to access the Data Warehouse. However, based upon concerns raised by the Office of Research Oversight (ORO), VISN 7 suspended direct access on April 9, 2004. ORO's concern stemmed from their

interpretation of Federal regulations that indicated if researchers were to obtain personal patient identifiers from the Data Warehouse, the researchers would need approval from a VISN IRB or from every IRB at those facilities contributing to the Data Warehouse.

If individual personal identifiers were not to be released, then approval of the researcher's local IRB and R&D Committee would be sufficient. In an undated memorandum, the former Director of VISN 7 stated that the data would be extracted into spreadsheets and forwarded without personal identifiers to individual researchers. ORO recommended developing a Standard Operating Procedure (SOP) that included a clear definition of the procedure for de-identifying and de-linking data, and that a SCRSSN would not be acceptable.

In response, VISN 7 approved the *SOP to Accompany the VISN 7 Data Warehouse for Research Policy* in September 2004, requiring as a condition of data release that the use of the data not qualify as human subjects research. This means the data could not contain personal identifiers, such as the patient's name or SSN, and medical information. The SOP included a direct assurance that no personal identifiers would be released to researchers. If no personal identifiers were released, there would be no need for VISN IRB approval.

On March 30, 2006, the Birmingham IRB approved a general request from a Birmingham researcher for data from the VISN 7 Data Warehouse. The request included the need for current VISN data for a research project. The general request contained an assurance that the SOP regarding VISN 7 data would be fully complied with. Access to the Data Warehouse was granted in May 2006.

In documents obtained from the VISN 7 Data Warehouse, we determined that the IT Specialist used this approval to obtain data that included personal individual identifiers. The personal identifiers obtained by the IT Specialist included SCRSSNs. VHA Handbook 1605.1 states that scrambled names and SSNs are not considered de-identifying health information. The Data Warehouse Manager indicated that he was not aware that scrambling of SSNs did not constitute de-identification of the data. As a result, personal identifiable data in the form of SCRSSNs and associated health information was released to the IT Specialist in violation of VISN 7 Data Warehouse SOPs. VISN 7 data was found on his desktop computer and is believed to be on the missing external hard drive.

#### *Birmingham VAMC Inappropriately Granted IT Specialist Programmer Level Access*

In addition to inappropriately obtaining patient identifiers from the VISN 7 Data Warehouse, the IT Specialist also received programmer level access to the VistA system at the Birmingham Medical Center without sufficient authorization. Programmer level access at the facility level grants the user the ability to create, delete, or alter medical records, and write computer programs to extract information from those records.

The Medical Center provided us with a copy of the IT Specialist's application for programmer access, dated December 15, 2003. There were two attachments to the application. The first document labeled Attachment C was signed by the Administrative Officer for Research and the Chief of Information Resources Management, and granted VistA privileges which did not include programmer level access. The second document, also labeled Appendix C, requested programmer level access. This attachment, however, was not signed by anyone. The two forms were dated 3 days apart. We were told that both forms were part of the same application package. While the Accounts Manager for IT support could not tell us who authorized programmer level access for the IT Specialist, other Birmingham Medical Center officials told us approval could have verbally come from the former VISN Chief Information Officer, although this is not confirmed. The current ISO indicated that he would not have accepted the unsigned form as authorization to grant programmer level access.

Nevertheless, the IT Specialist was granted programmer level access. This access permitted him to inadvertently incorporate VA employee health records into research data sets in the course of writing programs to extract data for research projects. Project 1 specified that the local sample of patients would be veterans. The protocol for this project in no way referenced any need for employee health records, or that non-veteran employees would be included in the patient sample. His desktop computer contained individually identifiable health information of at least 295 non-veteran VA employees.

Online VistA access generally includes an electronic warning for the user when an employee health record is accessed, indicating that it is a sensitive record. However, if an individual accesses the system as a programmer, it does not present the warning. This means that the programmer, in this case the IT Specialist, would not receive this warning. A VISN official stated that, "Once they drop...into the programmer mode, they can change their credentials or do whatever they want to do. It's pretty much carte blanche." It was also reported that the facility cannot track the specific activities of an individual using programmer mode and there is no way of knowing what programs are being run or what data is being extracted.

Further, the Accounts Manager stated that an employee's programmer level access expires only at the termination of the employee's employment or employee contract; it is not project-specific. Because programmer level access is not project-specific, the Birmingham IRB determines only what type of information can be used under a certain protocol, not the process by which the individual obtains the access. Therefore, we found that the IT Specialist's programmer level access was not subject to IRB approval and created a situation that not only compromised the privacy of employees but permitted the inclusion of research subjects not within the study population as defined by the protocols.

**Project 2: This project involved examining the quality of care to patients following myocardial infarction (MI), and attempted to determine whether certain demographic characteristics of the medical providers, such as their age, impacted the care rendered to these patients.**

For this project the IT Specialist was given access to Medicare files after officials at the MAC inappropriately released those files to the VIREC, and VIREC, in turn, inappropriately released the data to the Birmingham REAP. VA obtains Medicare files from the Centers for Medicare & Medicaid Services (CMS) at HHS. One of these files in particular, called the Medicare Physician Identification and Eligibility Registry (MPIER) file, contains records that include personal identifiers and other information on over 1.3 million health care providers.

*IT Specialist's Access and Use of Medicare Data Violated the Common Rule*

On May 17, 2004, CMS and VHA Office of the Assistant Deputy Under Secretary for Health Policy and Planning (ADUSH) signed a Memorandum of Understanding (MOU) accompanied by a Data Use Agreement (DUA) for CMS data containing personal individual identifiers. The MOU permits VHA to obtain Medicare records of both veteran and non-veteran Medicare beneficiaries. VHA uses this information to compare health care services, cost factors relating to non-VHA and VHA hospitals, and outcomes of certain procedures, as well as various demographics of physicians involved in these procedures. The goal is to improve the quality and cost of VA health care. The MOU included a provision that VA would comply with HIPAA and the Privacy Act.

As the primary recipient of the CMS data, MAC provides a mirror image of the data received from CMS to VIREC, a secondary VA recipient, who then provides Medicare data to VA research investigators. The Manager of the MAC is responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in the DUA to prevent unauthorized use, and for the day-to-day operations and for the receipt and release of data by MAC. MAC is also required to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. MAC is organizationally responsible to the ADUSH who has primary oversight for compliance with HIPAA and the Privacy Act.

MAC inappropriately released files not covered under the DUA to VIREC. The DUA lists 16 individual CMS files to be received annually and 5 additional files covering certain years. The files listed included personal identifying information on patients such as names, SSNs, and health care provider files. Files covered under the DUA ranged in size from 95,000 records to 45 million unique records. The DUA could be changed only by written modification or by the parties entering into a new agreement. In addition, VHA agreed that access to the data covered in the agreement would be limited to the



minimum number of individuals necessary to achieve the purpose stated in this section and to those individuals on a need-to-know basis only.

One of the files listed in the DUA is the Unique Physician Identification Number (UPIN) file. This file consists of nine data elements including first, middle, last name; suffix of the physician; business zip code; physician state code; physician's credential code; primary specialty code; and the physician's UPIN. The UPIN is used for Medicare billing purposes. MAC received the UPIN file for the years 2001-2003. The UPIN file is a subset of the MPIER file which consists of 49 data elements to include: the health care provider's SSN, the UPIN, full name, date of birth or death, medical school, date of graduation, medical credentials, state license number, primary and secondary medical specialty, business address, Medicare billing number, multiple record link number, and others. The multiple record link number is also referred to as the Employer Identification Number or a Federal Tax Identification number of the provider.

In 2005, CMS arranged for an independent contractor to process data requests. CMS received data requests from the MAC and then sent those requests to the contractor for data distribution. MAC requested the most recent UPIN 2004 file. The contractor, however, sent the complete MPIER file, not the UPIN subset agreed to under the terms of the DUA. The MPIER file is not authorized for release to VA under the MOU.

While the MAC Manager believed MAC reported the improper receipt of the MPIER file to CMS or the contractor, he could not provide us with any e-mail messages or letters addressed to CMS or the contractor concerning the receipt of this file. CMS denied any contact from MAC or VHA via phone or written notification concerning the incorrect file received by MAC. Even though MAC was aware they were not entitled to the MPIER file under the terms of the DUA, they sent it to VIREC anyway. CMS officials stated that they did not learn that the wrong file was sent until after the external hard drive was reported missing.

VIREC released data to the Birmingham REAP without adequate IRB authorization. When VIREC received the MPIER file, the Director of VIREC knew that the data was different than data received in previous years. We were provided with no evidence that VIREC questioned the receipt of data vastly in excess of data received within the UPIN file in previous years. Instead of requesting clarification from the MAC they also decided to keep the file. Recognizing that the file contained the SSNs of approximately 1.3 million medical providers, VIREC removed the Physician SSN data field before making the file available for use by VA researchers. The SSN was only one of 49 fields of data reported in the file. What VIREC did not realize was that one of the other fields, the multiple record link number, also contained the SSNs of over 600,000 providers.

VIREC is responsible for disbursing data to individual requestors (researchers). The VA Medicare Data Merge Initiative is a research project at VIREC which governs the use and

release of Medicare data. This project is approved by the IRB at the Hines VA Medical Center. The initial proposal submitted to the IRB for approval included VIREC's standard operating procedures, which were approved by the IRB as part of its protocol review.

VIREC policies and procedures require a researcher requesting data to complete VIREC's "Request for VA-Medicare Data" form to include: the principal investigator and contact person information, description of the project, the IRB number and dates of approvals, and the source of funding. The requestor must provide a signed DUA, local R&D committee approval letter, original IRB application with the IRB approval, an IRB approved Data Security Plan, Informed Consent Forms or a Waiver of Informed Consent, a HIPAA Authorization Form or a Waiver of Authorization, and the full research project protocol that includes the use of the Medicare data requested. This package is checked by the Program Manager of the VA Medicare Project at VIREC with assistance from a data analyst. Once the protocol package is complete, the Program Manager sends the package to two data reviewers from the Data Request Review Board (DRRB) of VIREC for their concurrence. The final approval is granted by the Director of VIREC.

In addition, VIREC submits quarterly reports to the Hines IRB containing all disbursements of data for that quarter. These reports are reviewed and approved retrospectively by the IRB as part of its continuing review process. In April 2006, the Birmingham REAP requested data from VIREC on health care providers for Project 2. The IRB Submission form listed 12 data elements containing the following statement: "Provider characteristics such as degree, graduation year, birth year, specialty, board name (last, first, middle, and suffix), and certificate name (last, first, middle, and suffix) are important variables to this analysis." The Chairman of the Birmingham IRB approved the IRB Submission form in August 2006.

The DRRB reviewed the request which included the IRB approval. One reviewer stated that the proposal was vague in the description of the use of the UPIN file, however the IRB request is clear. Project 2 did not specify how investigators would identify the specific providers involved in the study from the comprehensive list of providers requested from VIREC. The Director of VIREC stated on the Leadership Review form, "... not clear how the study will use the UPIN file. No details indicating how it can be linked are provided...."

On October 31, 2006, VIREC requested clarification of how the Birmingham REAP would link the 364 medical providers stipulated in the research project to MPIER file. The REAP responded that because they did not have individual UPIN numbers, they would need the entire MPIER file with the name and location of the providers to do their linkage. As a result, on November 13, 2006, the VIREC Director approved release of the complete MPIER file containing 48 fields (49 minus the SSN field) of data on over 1.3 million medical providers so the REAP could pull out 364 names and 12 fields of data.

The DRRB reviewers were not aware at the time of their review that the MPIER file contained 48 fields of data on over 1.3 million medical providers. We asked multiple officials at VIREC if there were any discussions to send only the data fields requested in the protocol for Project 2. We were told that no discussion occurred since it is their practice to send the complete file and not a data extract. When asked whether the principal researcher amended the protocol for Project 2 to specify a need for the MPIER file and if the IRB approved such an amendment, he responded that he could not remember. We determined that no amendment was created or approved.

VIREC released the MPIER file to the Birmingham REAP which, in turn, released it in its entirety to the IT Specialist, thereby creating a situation in which he obtained far more data than entitled to under the protocol for Project 2. Under the Common Rule, IRBs have a responsibility to protect the privacy and confidentiality of research subjects. The Hines IRB approved this request as part of the FY 2007 First Quarter Report from the Data Request Review Board. The Hines IRB Chairperson wrote on the bottom of the submission: “reviewed—include for discussion at IRB meeting.” We note that the IRB reviews these data releases retrospectively.

Because VIREC did not obtain adequate IRB approval from Birmingham for the release of the MPIER file, it violated the terms of its own protocol operating under IRB approval from Hines. The Manager of VIREC, as the principal investigator of the Medicare Data Merge Initiative, is responsible for this protocol violation.

Upon obtaining the file, the IT Specialist then split the complete MPIER file into multiple databases and continued to store the original file on his desktop computer. As such, we believe the complete MPIER file is on the missing external hard drive. While this file does not contain patient health information, it does include significant amounts of sensitive information that is at risk of potentially being used to the detriment of the medical providers and Medicare. Because the information the IT Specialist obtained from this file was not required under the protocol or authorized by the Birmingham IRB, its approval by the Hines IRB was inappropriate and violated Common Rule protections for the privacy and confidentiality of research subjects.

#### *Birmingham REAP Data Security Plan Not In Compliance with VISN Policy To Protect Data*

In addition to the problems previously mentioned in this report, additional concerns associated with inadequate management and supervision of Birmingham REAP activities included development of the REAP’s Data Security Plan that did not comply with the VISN 7 policy or VIREC guidance. The IRB and the R&D Committee inappropriately approved the Birmingham REAP Data Security Plan. Under the facility’s Human Research Protection Program, the ACOS for Research is responsible for the operations of the R&D Committee and its subcommittees (which would include the IRB) and for

implementation of their decisions. The ACOS for Research also must assure that all research staff adhere to the ethical conduct of research.

The IRB and R&D Committee are required to approve the REAP Data Security Plan submitted as a condition of the REAP obtaining Medicare data. VIREC requires an IRB approved data security plan as a condition for release of data to researchers. To this end, the VIREC website offers guidance that researchers should work with their Systems Administrator, local ISO, and Privacy Officer to develop a comprehensive data security plan. VIREC guidance, however, does not prohibit researchers from maintaining data on their desktop computers, provided they are in a locked office with access limited to project staff and not connected to a network.

In June 2006, a reviewer from the DRRB voiced concerns about this guidance by stating, "I am troubled by having this data sit on a desktop that can be picked up and walked off...I have not kept data on my workstation machine for years since the servers have become larger and faster...I would encourage the VIREC to change their policy on this before another theft takes place." Also, the VA Southeast Network Information Security Program VISN 7 AIS Operational Security Policy, issued in August 2006, stated mobile and portable systems should be protected commensurate with the sensitivity of the data stored on them. Employees will not store sensitive data on laptops or other portable devices without encryption.

The Data Security Plan written by the Birmingham REAP did not mandate encryption for portable devices as required by the VISN 7 policy. It also did not prohibit storage of data on desktop computers or portable devices. Despite this, the IRB approved the REAP data security plan on August 17, 2006. In our interview with the Chairperson of the IRB, he acknowledged that there are no members of the IRB committee who are IT experts. Using the analogy of radiation safety, the IRB Chairperson said that if a protocol requests multiple x-rays, the protocol would be sent to a Radiation Safety committee for review. He added: "So maybe it should be that automatically IT should see anything that is related to cyber security."

When we interviewed the writers of the Birmingham REAP Data Security Plan, they were not aware of the VISN 7 policy. We obtained no evidence that the REAP staff consulted the Privacy Officer, ISO, or local Systems Administrator in the development of the data security plan. Also, the Medical Center Director told us that he did not see the REAP Data Security Plan prior to the incident even though a secretary in the Director's office approved and signed the minutes of the October 12, 2006, R&D Committee meeting, which included language approving the REAP data security plan, on behalf of the Director.

Because the Birmingham REAP Data Security Plan did not comply with the VISN 7 policy or VIREC guidance, we find that the approval by the IRB committee, the R&D Committee, and the Director's Office was inappropriate and permitted VIREC to release

the data when the Birmingham REAP did not have adequate procedures to protect the security of the data.

**Project 3: This project involved using a patient survey to identify use of over-the-counter medications in patients taking prescription medications and link the information obtained to various VA databases to determine whether patients suffered any adverse effects from the combination of these medications.**

The IT Specialist was granted access to several files maintained by AAC, even though the requests did not have the appropriate authorizing signatures.

*IT Specialist's Access to AAC Not In Compliance with VHA Policy or the Privacy Act*

The Privacy Act mandates public notice in the *Federal Register* when establishing a system of records. A system of records is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" [5 U.S.C. § 552a(a)(5)]. An agency's *Federal Register* notice must include name and location of the system, categories of individuals and records in the system, routine uses of the records, and the policies and practices of the agency regarding retrievability and access controls [5 USC §552a(e)(4)].

VA published a System of Records Notice on April 7, 2004, describing methods for access, maintenance, and retrieval of records contained within VA databases, including records in the AAC National Patient Care Database (NPCD). Since October 1, 1996, VHA facilities have been required to report all electronic data concerning the provision of services in VHA facilities, which included outpatient data, to NPCD. The *Federal Register* notice describing this system of records included the requirement that information security officers and system data stewards review and authorize data access requests.

Files maintained in the NPCD include the MDP/MED/MEDIPP Analysis File, the Nationwide SSN Data File, and the DSS Scrambled SSN Only File. The DSS Scrambled SSN Only File includes SCRSSNs linked to health care data for subject areas such as pharmacy, inpatient admissions, and laboratory. The MDP/MED/MEDIPP Analysis File contains SCRSSNs linked to inpatient and outpatient workload data and enrollment information. According to the Director, National Data Systems, Austin, TX, researchers may obtain data including SCRSSNs and SSNs by a process that "is completely controlled by the local facility." The Nationwide SSN Data File allows access to real SSNs for all of the files contained within the MDP/MED/MEDIPP file. Individuals seeking access to the Nationwide SSN file are required to complete an Automated Customer Registration System (ACRS) Time Sharing Request Form (VA Form 9957) and to obtain the signature of an approving official, as well as the approval of the VHA

Privacy Office. The ACRS form must also be completed for access to other files, but this access requires only the approval of local facility officials.

During the course of our review, we found that the IT Specialist had access to several files in Austin, including the Nationwide SSN Data, the DSS Scrambled SSN Only File, and the MDP/MED/MEDIPP Analysis files. The facility granted the IT Specialist access following completion of three VA Form 9957s. Neither the VHA Privacy Office nor the AAC could provide us with any policy describing the process for approving general access to AAC files. However, guidance posted on the VIREC website outlines a process for Nationwide SSN access that requires approval by the local facility and by a representative of ORD.

We requested any applicable policies and procedures from the VHA Privacy Office which might restrict access to real SSNs through Austin. The Privacy Office supplied us with an unsigned, undated document, "Standard Operating Procedure for Obtaining National Real SSN Access." This document included the following language:

VA employees requesting National Real SSN access will need to submit a completed VA Form 9957 . . . with signatures from the supervisor of the requesting individual, facility or program office director and director of program at Headquarters level. If all signatures are not there VHA Privacy Office will not approve access.

We requested information as to whether the Birmingham Medical Center received this SOP from the Privacy Office. We were provided with an e-mail indicating that the ISO at Birmingham attended a conference at which the SOP was presented, but they could not verify whether he attended the actual session involved.

The facility provided us with three ACRS Time Sharing Request Forms for the IT Specialist, dated January 10, 2006, October 16, 2006, and January 10, 2007. The Administrative Officer (AO) of the Birmingham REAP signed two of these requests as the IT Specialist's supervising official. However, the AO was not the IT Specialist's supervisor. None of the three forms had signatures on the lines for either the approving official or the second approving official. The January 10, 2007, form included a request for access to Nationwide SSN data. The ISO had not approved the access. An ORD representative informed us that ORD had not approved the IT Specialist's access. At the facility level, a business office representative indicated that the approving official at the Birmingham VAMC would be the Medical Center Director, who also had not signed the form. Nevertheless, the ACRS point of contact at Birmingham VAMC granted the IT Specialist access to Nationwide SSN data on January 10, 2007.

The IT Specialist last accessed AAC data on January 4, 2007. Therefore, he did not access Nationwide SSN data prior to the data loss since he was not authorized to obtain access to this file until January 10, 2007. However, the IT Specialist did obtain

and utilize his access to other Austin files prior to the date that he reported the external hard drive missing. Therefore, despite the lack of completed VA Form 9957's with appropriate supervisory and authorizing signatures, the IT Specialist obtained access to multiple NPCD files, creating a potential violation of the system of records notice made in accordance with the terms of the Privacy Act and resulting in a situation in which the data could have been stored on the missing external hard drive.

## **Conclusion**

The failure to limit individually identifiable health information to authorized personnel as well as failure to develop, disseminate, and follow VHA and facility policies and procedures governing access to multiple VA databases created a situation in which one employee could accumulate a vast amount of individually identifiable health information from multiple sources. The three research projects we reviewed that were on the IT Specialist's desktop computer involved the use of data from multiple sources, including the AAC, VIREC, the VISN 7 Data Warehouse, and the Birmingham VAMC VistA system. Data present on the IT Specialist's desktop computer allowed the linking of names, SSNs, SCRSSNs, and medical information for these projects. We believe much of this information was stored on the missing external hard drive.

We found that the Birmingham REAP's use of data, not requested by the researchers or approved by the IRB, constituted a violation of the Common Rule. The Common Rule does not permit a researcher to initiate a change or modification to a research project protocol involving human subjects without IRB approval. A violation occurs when the protocol is changed without IRB approval. In this case, researchers at Birmingham obtained the MPIER file for use in an IRB approved research project. The IRB approved project permitted researchers to obtain data on 12 variables of interest, relating to care provided by approximately 364 VA physicians. The VA Medicare Data Merge Initiative, VIREC's research protocol under which the data was released to the Birmingham REAP, also required adequate IRB approval as a condition of release of the data. The file provided by VIREC, however, contained personal identifiers on more than a million physicians that were not required for the study. This constituted a protocol violation which resulted in a violation of the Common Rule requirement that an IRB must approve all changes to or modifications in a research protocol involving human subjects. It also allowed the IT Specialist to access and store data on more than a million physicians that was not needed or approved to conduct the research.

In addition, because the MPIER file contained 48 variables compared with the 9 variables contained within the UPIN file, researchers also obtained more information than required to conduct the research on the physicians who actually were enrolled in the study. This constituted a violation of the privacy of human subjects engaged in research because researchers obtained information in excess of that approved by the IRB and described in the protocol. This led to a situation in which 48 data fields on more than one million physicians could be compromised by the loss of one IT Specialist's external hard drive.

Also, because the Birmingham REAP Data Security Plan did not comply with the VISN 7 policy or VIREC guidance, we find that the approval by the IRB committee, the R&D Committee, and the Medical Center Director's Office was inappropriate and permitted VIREC to release the data when the REAP did not have adequate procedures to protect the security of the data.

## **Recommendations**

**Recommendation (6).** We recommend that the Under Secretary for Health develop, disseminate, and ensure compliance with policies regarding the release of individually identifiable health information from VISN data warehouses for research purposes to include IRB approval requirements and stress, in VHA's mandatory annual privacy training, that scrambled SSNs do not constitute de-identified data.

**Recommendation (7).** We recommend that the Assistant Secretary for Information and Technology develop and implement policies describing the conditions under which VistA programmer level access may be granted for research purposes, including whether that access is project specific or for the term of employment, and take appropriate action to remove programmer access from individuals who do not meet those conditions.

**Recommendation (8).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the MAC and VIREC Directors for inappropriately retaining and releasing the MPIER file.

**Recommendation (9).** We recommend that the Under Secretary for Health develop a mechanism to ensure that data security plans for research projects comply with applicable information security policies and privacy policies prior to approval by the IRB.

**Recommendation (10).** We recommend that the Assistant Secretary for Information and Technology disseminate and enforce the existing Standard Operating Procedure for access to Austin Automation Center's nationwide SSN file, and issue policies and procedures regarding authorization to access all other Austin Automation Center data for research purposes.



## **Issue 4: Whether the IT Specialist Complied with Research Project Protocols to Properly Safeguard Protected Information**

### **Findings**

To determine whether the IT Specialist complied with research project protocols to properly safeguard information, we evaluated the same three research projects discussed in Issue 3. We concluded that the IT Specialist violated the terms and conditions under which the IRB granted HIPAA waivers for the involved protocols. In doing so, the IT Specialist failed to properly safeguard individually identifiable health information, thereby placing vast amounts of HIPAA and Privacy Act protected information at risk. We believe much of this information was stored on the missing external hard drive, and most of it was not password-protected or encrypted.

The IRB at VA medical centers is a subcommittee of each facility's Research and Development (R&D) Committee. At VA medical centers, the IRB ensures that the requirements of HIPAA and the Common Rule are met by the research protocol, including: (1) that the subjects give their informed consent to participate in the research or that certain conditions for waiving informed consent are met; (2) that the subjects either sign a written authorization to release their medical records to the researchers or that the requirements for a waiver of the written authorization (HIPAA waiver) are met; and (3) that the privacy and confidentiality of the subjects are protected by the terms of the protocol.

#### **IT Specialist Failed to Properly Protect Individually Identifiable Health Information in Violation of the HIPAA Privacy Rule**

While the use of individually identifiable health information for research purposes generally requires written authorization from the individual, the HIPAA Privacy Rule (45 CFR 164.512 (i)) offers a waiver to obtain this information without written authorization if the IRB determines that the study involves minimal risk to human subjects. Minimal risk for privacy purposes requires the IRB to make several findings, including the following:

The use or disclosure of the requested information involves no more than a minimal risk to the privacy of individuals based on, at least, the presence of the following elements:

- a) An adequate plan to protect the identifiers from improper use and disclosure.
- b) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or

research justification for retaining the identifiers or such retention is otherwise required by law.

In addition, to comply with the HIPAA Privacy Rule, documentation supporting IRB approval of a HIPAA waiver must include a description of the individually identifiable health information without access to, and use of, the IRB has determined that the research could not be practically conducted. Based on our review of the three research projects, we found the following.

Project 1 indicated that the investigators would use SSNs, dates of birth, and names as individual identifiers for this study. The IRB granted a HIPAA waiver based on the plan to protect the information from improper use or disclosure by creating a password-protected file containing individuals' SSNs and dates of birth. We found files for this study on the IT Specialist's desktop computer containing SSNs, patient identification numbers, and dates of birth. They were not password-protected, violating the conditions under which the IRB granted a HIPAA waiver. While the desktop computer itself was password-protected, we believe this protection was lost when the files were backed-up on the external hard drive that went missing. Most of the files on the external hard drive were not password-protected or encrypted.

Project 2 sought a means of improving provider utilization and adherence to standard-of-care practice guidelines for the management of post-MI patients. This required the use of medical provider data as well as patient data. Data collection would occur at 48 sites within VHA. While the requests for HIPAA waivers submitted by individual project researchers at the different sites varied slightly in wording, most of them implied that the waivers were based on no identifiable patient information being extracted. For example, a sample waiver from one of the sites incorporated the following: "No individually identifying information will be extracted..." However, we located on the IT Specialist's desktop computer a file containing SSNs and SCRSSNs associated with Project 2. We selected a patient at random from this file and verified that the SSN matched a post-MI patient at one of the involved facilities. As such, the IT Specialist maintained patient identifiers, including SSNs, in violation of the terms and conditions of the HIPAA waiver associated with this project.

Project 3 involved mailing a patient survey to individuals known to have prescriptions for a certain type of medication. The survey would record use of over-the-counter medications in patients taking prescription medications and link that data to pharmacy data at the Birmingham VAMC and at another medical center as well as to the Patient Treatment Files and the Outpatient Care Files at the AAC. This information would then be used to determine whether patients suffered any adverse effects from the combination of those medications. Data would be compiled at the Birmingham VAMC, de-identified, and then forwarded to the other medical center involved in the study. However, the plan indicated that SCRSSNs would be retained in the data which did not constitute de-identification of the data. HIPAA waivers are conditioned on the requirement that the

researcher has an adequate plan to protect the data. The protocol indicated that data would be stored on VA password-protected computers in order to safeguard it from internal and external unauthorized access.

Files contained on the IT Specialist's desktop computer and believed to be on the external drive included files that contain patient SSNs with SCRSSNs, which can be linked to files with patient names and other files containing medical information. Again, while the desktop was password-protected, we believe these files were copied to the external hard drive and were not adequately password-protected. An indicator that the IT Specialist knew he had not properly safeguarded research data was evidenced by the fact that he attempted to delete or encrypt several files after he reported the external hard drive missing. Therefore in Project 3, the IT Specialist kept the data in a manner not consistent with the terms and conditions of the protocol's HIPAA waiver.

#### *IT Specialist's Utilization of Data Violated Informed Consent Requirements*

Generally, a researcher may not involve a human subject in research unless informed consent is obtained from the subject or his or her legal representative. An IRB may, however, waive this requirement for some or all subjects, if it finds either: (a) that the only record linking the subject and the research would be the consent document and the principal risk to the subject would be potential harm resulting from a breach of confidentiality. Each subject must be asked whether the subject wants documentation linking the subject with the research, and the subject's wishes will govern; or (b) that the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.

Project 1 received a waiver of informed consent for patients enrolled in the studies. Project 2 required written informed consent at the Birmingham VAMC from providers. We reviewed the waivers and informed consent in these projects to determine if the IT Specialist violated any provisions which may have contributed to the data loss.

Project 1 requested a waiver of informed consent for patients enrolled in the study. In the request for the waiver, the investigator stated that "patients will not be able to be identified in the database." This was in response to the question of whether waiving or altering the informed consent adversely affected the subjects' rights and welfare. However, we found files on the IT Specialist's desktop computer that contained the names, SSNs, SCRSSNs, patient numbers, and information extracted from the local VistA system, including race data and information pertaining to homelessness. The database that the IT Specialist possessed contained multiple identifiers as it contained extracts from health records in the same data set as patient identifiers. This violated the terms and conditions of the waiver of informed consent.

For Project 2, written informed consent was required at the Birmingham VAMC for providers enrolled in the study. The written informed consent stated that the data "will be

stored on a server housed in the Birmingham VAMC and will be aggregated at the Community Based Outpatient Clinic (CBOC) level and encrypted . . . Information collected via the website will be sent directly to a secure server and any identifiers removed.” On the IT Specialist’s desktop computer, however, we found a file containing the names, degrees, facility name, CBOC name, and some UPIN numbers of VA providers associated with this study. This was not on a secure server, and because all personal identifiers had not been removed in accordance with the informed consent, this created a condition that allowed personal information of VA providers to be compromised when the external hard drive was lost or stolen.

*Access to Individually Identifiable Health Information Not Limited to Authorized Staff*

To meet VHA and Federal requirements for IRB review, VHA Handbook 1200.5 specifies that IRBs must maintain written standard operating procedures. The Birmingham Medical Center’s Standard Operating Procedures (SOP), dated November 15, 2005, include a statement that the IRB evaluates proposals to ensure that investigators are “adequately providing provisions to protect the privacy of subjects and to maintain the confidentiality of data.” The IRB established guidelines for protection of confidential information that included the following:

- Limit recording of personal information to that which is absolutely essential to the research.
- Store personally identifiable data securely and limit access to the principal investigator and authorized staff.

The IT Specialist’s worksheets and minutes from the Data Unit Meeting Minutes reflected that he was involved in data analysis for a research project that involved abstracting data on patients admitted to five different VA medical centers who died while hospitalized, and surveying family members and caregivers to obtain their subjective reactions to health care delivery at the end of life. Patients were recruited by searching electronic medical records, with confidentiality of records to be maintained by entering data into a database with a unique code used for identification rather than name or SSN. Data extracted from the records, however, contained patient names and SSNs.

The facility supplied us with IRB documents pertinent to this protocol. The IT Specialist was not listed as authorized study personnel on any of these documents. We therefore find that access to protocol-related individually identifiable health information was not limited to authorized staff only, in violation of the guidelines established by the facility IRB SOP, creating a situation in which the data could be put at risk for loss on the missing external hard drive.

*Facility's Compliance Program Did Not Require a Review of Privacy and Confidentiality*

To prevent noncompliance with the Common Rule, facility IRBs are required to maintain procedures for auditing study protocols. These audits are performed by the Compliance Officer of the Research Service. Audits at Birmingham VAMC include reviewing the informed consent process, inclusion and exclusion criteria for the study, advertisements, subject recruitment materials, and examining files for any unanticipated problems or serious adverse events not reported to the IRB. The facility supplied us with a list of items audited. The list did not include issues pertaining to privacy, confidentiality, or information security. We were told that none of the research projects discussed in this report had been audited, so we obtained a sample audit conducted on a project not on the missing external hard drive. This audit also did not review privacy, confidentiality, or information security issues.

The facility Compliance Officer informed us that she relied on the VISN Research Compliance Officer for advice and interpretation of human subjects protection regulations. The VISN Research Compliance Officer indicated that she had never advised the facility compliance officer to specifically include a review of privacy and confidentiality in the audit. VHA Handbook 1200.5, which describes the requirements for protection of human subjects in research, does not specify what elements should be included in a protocol audit.

Failure to include a review of privacy and confidentiality issues in the facility's program to ensure compliance with human subjects protection regulations prevented the Research Service from potentially identifying and addressing some of the problems noted in this report prior to the data loss. This is particularly relevant in light of the Informed Consent and HIPAA waiver documents submitted to the IRB which clearly indicated that researchers at the facility did not realize SCRSSNs constituted individually identifiable health information. Even the IRB Chairperson indicated that he had only recently become aware that SCRSSNs were considered identifiable data for privacy purposes.

## **Conclusion**

The IT Specialist maintained data in a manner that violated the terms under which the researcher was granted a waiver from HIPAA requirements. For example, the IT Specialist did not password-protect files relating to two of the three research projects we reviewed, which was a condition for granting the waivers. The third HIPAA waiver specified that no identifiable patient information would be extracted, but the IT Specialist's files contained social security numbers. In one of the projects reviewed, the IT Specialist also violated the terms of a waiver exempting the researcher from obtaining informed consent from subjects. The request for waiver indicated that patients would not be identified, yet the IT Specialist had files on his desktop computer that contained identifiers. In a second protocol, no waiver was granted and the informed consent stated that data would be stored on a server housed at the Birmingham VAMC.

In this instance, the IT Specialist maintained the file on his desktop, which is not a secure server. While it can be argued that the IT Specialist's desktop computer was password-protected, we believe this protection was lost when the files were backed-up on the external hard drive that went missing. Most of the files on the external hard drive were not password-protected or encrypted.

## **Recommendations**

**Recommendation (11).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the IT Specialist for inappropriately accessing and utilizing individually identifiable health information.

**Recommendation (12).** We recommend that the Under Secretary for Health require facility IRB compliance program audits to assess the privacy and confidentiality protections for human subjects in research, including whether the use of research data complies with information security requirements specified in HIPAA waivers or waivers of informed consent.

## **Issue 5: Whether the Birmingham REAP Director Was Adequately Supervised, and Whether the REAP's Director and Associate Director Adequately Managed and Supervised the Operations and Staff of the REAP**

### **Findings**

Many of the problems described in this report might have been prevented if the daily operations of the REAP were effectively managed and supervised. However, the REAP Director and her subordinate managers frequently were not physically present at the REAP to supervise and manage daily operations, and the REAP Director's supervisor of record, the ACOS for Acute and Specialty Care, in fact, was the supervisor in name only and provided no supervision. The Associate Chief of Staff for Research, though responsible for all research programs at the Birmingham VAMC, has no line authority over the REAP and did not supervise the REAP Director. While the Medical Center Director is ultimately responsible for position management at the facility, he also did not ensure adequate supervision over REAP operations.

#### *Birmingham REAP Director Not Properly Supervised by Medical Center Management*

The performance of the Birmingham REAP Director was not supervised. Her supervisor of record was the ACOS for Acute and Specialty Care, but both he and the Medical Center Director told us the ACOS was the designated supervisor of the REAP Director for hiring and credentialing and privileging purposes only. The ACOS acknowledged he was supervisor in name only and did not supervise the REAP Director and did not oversee REAP activities. He also told us he was not responsible for preparing the REAP Director's proficiency report (annual performance appraisal) even though he signed her report as the rating official for calendar years 2001 through 2004. When questioned about this discrepancy, he told us he did not remember signing the proficiency reports. No performance appraisals were on file for the REAP Director for the past 2 years.

The ACOS for Research is responsible for administering and managing the research program facility-wide, but had no line authority over the REAP. He told us he did not supervise the REAP Director's activities nor did he maintain a professional relationship with her, although he did acknowledge interacting with individual researchers. He said the Research Service was responsible for issues at the REAP involving human subjects protection, and for administrative matters such as payroll, time and attendance, and purchasing. But he said he was not aware of the concerns about physical security at the new office, nor was he aware of the need for more server space or the purchase of the external hard drives. The REAP Director told us she did not go to the ACOS for Research for assistance if she could help it. The lack of a professional relationship between the facility's two most senior research officials created the situation where the

resources and expertise of the Birmingham VAMC were not brought to bear on the REAP's need for additional secure data storage.

The Medical Center Director confirmed that the REAP Director did not report to the ACOS for Research and said she reported to HSR&D in VHA Central Office on matters relating to the governance of the REAP program. He also told us that, in his opinion, the REAP Director should have no direct reporting relationship to him. Finally, the Chief Research and Development Officer in VHA Central Office told us he believed the facility ACOS for Research should supervise the REAP Director on most matters and be the REAP's advocate within the VAMC for getting things done. Lacking any clear guidance and understanding of who is assigned responsibility to supervise the REAP Director, we believe the Medical Center Director, is ultimately responsible for position management at the facility and is accountable for the supervision or lack thereof over the REAP Director.

*Birmingham REAP Director and Associate Director Did Not Properly Manage REAP Operations*

Although the Birmingham REAP Director was required to work 25 non-clinical hours for VA each week, her part-time physician service agreement, approved in May 2006, permitted her to be physically located at an alternate work site at the University of Alabama at Birmingham, during these hours. The REAP Director acknowledged that, in a typical week during calendar year 2006, she was in the REAP office only a "couple of hours." She said she did most of her REAP work in her University office, including programmatic work, scientific decision-making, grant writing, staff mentoring, manuscript preparation, and directing analyses. She preferred working at the University because that is where she kept her books and research files, and she did not believe she needed to be at her REAP office to accomplish her job. The VAMC part-time physician audits of the REAP Director's attendance during her core hours, performed between January and November 2006, documented that she was at her University office on three of five occasions, and in the REAP office attending meetings on the remaining two occasions.

Another indication that the Birmingham REAP Director was rarely present at VA was that she had her official VA e-mail automatically forwarded to her account at the University of Alabama, in violation of VA policy. Regarding this practice, VA policy prohibits employees from keeping VA information on a non-VA system unless specifically approved by an appropriate supervisor. Further, in a May 2004 memorandum, the Assistant Secretary for Information and Technology advised key officials that automatically forwarding e-mail outside VA could result in violations of the Privacy Act or HIPAA and, effective 30 days from the date of the memorandum, would be strictly prohibited unless specifically waived by the appropriate cyber security chain of command. We found no waiver for either the REAP Director or her Associate Director.



The Birmingham REAP Director told us she considered her function as REAP Director to be primarily that of providing scientific leadership, not running the day-to-day operations of the program, which she said she relied on both the REAP Associate Director and the Administrative Officer to do. For example, she told us she did not become personally involved in requesting additional computer server space; was not responsible for ensuring compliance with policies; was not involved in planning the office's move to new space; and was not responsible for addressing issues relating to office space security.

The Birmingham REAP Director's failure to recognize and accept accountability for overall management and administration of the REAP is directly related to the failure of her superiors to clearly define her role and responsibilities. Fundamental management tools such as a position description (a Functional Statement for Title 38 employees) or current performance appraisal (a Proficiency Report for Title 38 employees) were non-existent. A credentialing and privileging document was the only record we were given that discussed what she would perform. This was limited to the clinical procedures she was allowed to perform as a physician in the Acute and Specialty Care Service. However, both the Medical Center Director and the ACOS for Acute and Specialty Care admitted to us that she has no actual clinical responsibilities.

Her status as a clinician resulted in her being placed under an ACOS who had no knowledge of her Birmingham REAP activities. The ACOS gave her no direction and rendered her relatively free from supervision with respect to the REAP. This, however, should not excuse the REAP Director for exercising poor judgment when she failed to follow VISN 7 policy when she approved the purchase of the external hard drives.

The Birmingham REAP Associate Director was also present on an infrequent basis. The Associate Director is required to spend 10 of her 25 weekly VA-duty hours on clinical duties, not REAP activities. She told us, however, that she was physically present in the REAP office at least once a day for meetings and a variety of other activities. The Associate Director was also authorized to perform her VA work at her University of Alabama at Birmingham office. The VAMC's part-time physician audits of her attendance during her core hours, all performed on Tuesday mornings between March and December 2006, documented that she was in a VA clinic each time. The Associate Director also did not maintain a VA e-mail account, but rather received her official VA e-mail messages on a University of Alabama account. As noted, this practice is against VA policy.

The Birmingham REAP Data Unit Manager, who was scheduled to work 20 hours a week in her capacity as the manager, told us that, prior to the REAP's move to new office space, she was physically present at least one 8-hour day a week and that, beginning in January 2007, she was present in the new office space 30 hours or more a week. However, in February 2007, one REAP staff member in the Data Unit told us she thought the Associate Director was now her supervisor because it had been such a long time since she had seen the Data Unit Manager, and that she was not certain if the Data Unit

Manager worked there at all. The IT Specialist who reported the missing external hard drive also works in the Data Unit.

## Conclusion

The Birmingham REAP Director and her subordinate managers frequently were not physically present to supervise and manage the daily operations of the REAP. The REAP Director received no supervision from the ACOS for Acute and Specialty Care, as he was the supervisor of record in name only. Also, the ACOS for Research, who is responsible for research activities at the VAMC, was not engaged in managing or supervising the activities of the REAP Director. The Medical Center Director said the REAP Director reports to HSR&D in VHA Central Office on matters relating to the governance of the REAP program. He also told us that, in his opinion, the REAP Director should have no direct reporting relationship to him. However, the Chief Research and Development Officer in VHA Central Office told us he believed the facility ACOS for Research should supervise the REAP Director on most matters and be the REAP advocate within the VAMC for getting things done. Lacking any clear guidance and understanding of who is supposed to supervise the REAP Director, we believe the Medical Center Director is ultimately responsible for position management at the facility and is accountable for the supervision or lack thereof over the REAP Director.

The Birmingham REAP Director and Associate Director, both part-time physicians, did not properly manage REAP operations. Both managers elected to work primarily at their alternate office at the University of Alabama at Birmingham and both were rarely present at the VAMC REAP. The REAP Director had her official VA e-mail messages automatically forwarded to a University of Alabama e-mail account. The Associate Director had her official VA e-mail sent to her University of Alabama e-mail account. VA policy prohibits employees from keeping VA information on a non-VA system unless specifically authorized. Automatically forwarding e-mail outside VA could result in VA data being inappropriately transmitted outside VA in violation of the Privacy Act or HIPAA. Doing so is strictly prohibited unless specifically waived by the appropriate cyber security chain of command. We found no waiver for either the REAP Director or Associate Director. We believe that if these managers were more engaged in the daily operations of the REAP, the information, physical, and personnel security deficiencies cited in this report may have been prevented.

## Recommendations

**Recommendation (13).** We recommend that the Under Secretary for Health ensure that the Birmingham REAP's Director and Associate Director discontinue the practice of receiving their official VA e-mail at the University of Birmingham, in violation of VA policy prohibiting storage of VA information on a non-VA system, resulting in potential Privacy Act or HIPAA violations.

**Recommendation (14).** We recommend that the Under Secretary for Health assess the alignment of Birmingham REAP management positions at the Birmingham VAMC, and take action to correct the dysfunctional management structure that led to an overall breakdown of management oversight, controls, and accountability of the Birmingham REAP. This should include:

- Correction of the Birmingham REAP Director's reporting relationship from the ACOS for Acute and Specialty Care, which was in name only and resulted in the lack of actual supervision over the REAP Director's activities, to the ACOS for Research who currently has facility-wide responsibility for research programs but no line authority over REAP managers or involvement in their activities.
- Establishment of an accurate functional description and performance plan to clarify Birmingham REAP managers' responsibilities and to hold them accountable for proper administration of REAP resources, to include equipment purchases, acquisition of server space, protection of sensitive information stored on VA systems and portable devices, office space security, and compliance with applicable VA policies and procedures.
- Clarification of the Medical Center Director and ACOS for Research's responsibility and line authority over all research programs at the facility, including the REAP.

**Recommendation (15).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the Birmingham Medical Center Director for not ensuring appropriate management and administration of the Birmingham REAP and protection of the privacy and confidentiality of research subjects.

**Recommendation (16).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the ACOS for Research for not ensuring appropriate management and administration of the Birmingham REAP.

## Under Secretary for Health Comments

**Department of  
Veterans Affairs**

**Memorandum**

**Date:** June 26, 2007

**From:** Under Secretary for Health (10)

**Subject:** **OIG Draft - Administrative Investigation, Loss of VA Information, VA Medical Center, Birmingham, AL**

**To:** Assistant Inspector General for Investigations (51)

1. I have reviewed the draft report and concur with the recommendations. I appreciate the willingness of the investigations team to work with Veterans Health Administration (VHA) staff to address our concerns with the draft report.

2. The loss of information at the Birmingham Research Enhancement Award Program (REAP) is a disturbing incident given the Veterans Health Administration's (VHA) focus on data security over the past year. While it is encouraging to know that to date there are no reports of fraud or identity theft resulting from this event, I am unwavering in my commitment to learn from this incident and further improve data security controls and access within VHA. I can assure you that following our review of the evidence received from your office appropriate administrative actions will be taken against those responsible for this serious security breach.

3. While I concur with the recommendations, there are some points of clarification in the report findings that I believe are important to state. Essential to the development of research projects aimed at improving the quality of care in VA and the Nation are the data sharing agreements with the Department of Health and Human Services (HHS) and the Centers for Medicare and Medicaid Services (CMS). That this incident should compromise these sharing agreements in any way is of

paramount concern to me and your report will assist VHA in strengthening these agreements to ensure that such errors are prevented in future.

4. The chart shown on page 10 of the draft report does not show that after VHA analyzed the files thought to be on the missing hard drive, the number of unique social security numbers identified was reduced to 254,330 from 535,103. Although this is mentioned later in the draft report, I think it is important to provide that information as part of the discussion on page 10 as well.

5. This report also highlights that Chief Information Officers (CIOs) and Information Security Officers (ISOs) have a responsibility for and should be proactive in being aware of facility space requirements and moves to ensure that the necessary information technology and security requirements for government owned and/or leased space are met. Clearly that was not the case at this facility and I am disappointed that this was not pursued more thoroughly by the investigation team.

6. As a result of this incident, VHA initiated several actions to ensure effective information security in research. Beginning on March 15, 2007, and running through June 12, 2007, a mandatory educational program highlighting applicable information security and privacy policies began for all research staff. The Office of Research and Development (ORD) also provided training on April 11, 2007, to VA Information Security Officers at the InfoSec 2007 conference in Jacksonville, FL. In addition, ORD and the VHA Privacy Office developed a Research Privacy Review Checklist that was distributed to field facilities and discussed on a national teleconference held June 1, 2007. VHA will also be reevaluating and correcting position sensitivity levels for associated risk level designations.

7. Also, the need to re-evaluate and correct position sensitivity levels for associated risk level designations is highlighted in this report. Upon the receipt of this final report, the Birmingham VA Medical Center will issue memos to all service chiefs on an annual basis, informing them of current position sensitivity levels of employees, and outlining

essential differences between the levels. An additional annual memo will also be sent concurrently to the local CIO and ISO regarding their responsibilities, upon the receipt of this report. Based on the success of this process in Birmingham, I will consider standardizing this process throughout VHA.

8. Along with these actions, a detailed action plan addressing each recommendation is included in this response. Thank you for the opportunity to review the report. If you have any questions, please contact Margaret M. Seleski, Director, Management Review Service (10B5) at (202) 565-7638.

*(original signed by:)*

Michael J. Kussman, MD, MS, MACP

Attachment

## **Under Secretary for Health Comments to Office of Inspector General's Report**

The following Under Secretary for Health comments are submitted in response to the recommendations in the Office of Inspector General's Report:

### **OIG Recommendations**

**Recommendation (1).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the IT Specialist for his inappropriate actions during the course of the investigation and for failing to properly safeguard personally identifiable information on his missing external hard drive.

Concur      **Target Completion Date:** October 1, 2007

Following receipt and review of the evidence, an appropriate administrative action will be initiated.

**Recommendation (3).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the Birmingham REAP Director and Associate Director for failing to take adequate security measures to protect personally identifiable information.

Concur      **Target Completion Date:** October 1, 2007

Following receipt and review of the evidence, an appropriate administrative action will be initiated.

**Recommendation (5).** We recommend that the Under Secretary for Health direct the Medical Center Director to re-evaluate and correct position sensitivity levels and associated background investigations for positions at the Birmingham VAMC.

Concur      **Target Completion Date:** August 2007 and on-going

The Birmingham VA Medical Center Office of Human Resources will issue memos to all service chiefs on an annual basis informing them of current position sensitivity level of employees, and outlining essential differences between the levels. The first issuance will occur upon receipt of the OIG report and on an annual basis thereafter. A thirty day response will be required of services. The memo to the ISO and CIO regarding their responsibilities will also be sent upon receipt of the report and annually thereafter.

**Recommendation (6).** We recommend that the Under Secretary for Health develop, disseminate, and ensure compliance with policies regarding the release of individually identifiable health information from VISN data warehouses for research purposes to include IRB approval requirements and stress, in VHA's mandatory annual privacy training, that scrambled SSNs do not constitute de-identified data.

Concur      **Target Completion Date:** October 1, 2007

VHA's Chief Information Officer will develop access policies for VISN data warehouses to delineate processes for research access to individually identifiable information. A Directive will be drafted within 60 days from publication of this report, with the expectation of obtaining VHA concurrence by October 1, 2007.

VHA's Chief Information Officer will also develop a fact sheet reiterating VHA Handbook 1605.1 policy on de-identification of data in accordance with the HIPAA privacy rule. This information will also be announced on research and privacy national conference calls, and disseminated by e-mail to the research and privacy mail groups by July 30, 2007.

**Recommendation (8).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the MAC and VIREC Directors for inappropriately retaining and releasing the MPIER file.

Concur      **Target Completion Date:** October 1, 2007

Following receipt and review of the evidence, an appropriate administrative action will be initiated.



**Recommendation (9).** We recommend that the Under Secretary for Health develop a mechanism to ensure that data security plans for research projects comply with applicable information security policies and privacy policies prior to approval by the IRB.

Concur **Target Completion Date:** October 1, 2007

Deputy Under Secretary for Health for Operations and Management (DUSHOM), in collaboration with the Chief Research and Development Officer (CRADO), will develop a memorandum to the field, within 30 days of receipt of this report, requiring inclusion of a Privacy Officer and an Information Security Officer (ISO) on the Institutional Review Board (IRB). This inclusion will give them a more substantive role in the research oversight process. VHA will request the VA Chief Information Officer (CIO) to also sign the memorandum, since the ISOs report to the Department's Office of Information and Technology. Within 45 days of the issuance of the memo, sites will have 45 days to transition IRB representation to include the ISO and a Privacy Officer.

**Recommendation (11).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the IT Specialist for inappropriately accessing and utilizing individually identifiable health information.

Concur **Target Completion Date:** October 1, 2007

Following receipt and review of the evidence, an appropriate administrative action will be initiated.

**Recommendation (12).** We recommend that the Under Secretary for Health require facility IRB compliance program audits to assess the privacy and confidentiality protections for human subjects in research, including whether the use of research data complies with information security requirements specified in HIPAA waivers or waivers of informed consent.

Concur **Target Completion Date:** 90 days from the publication of the OIG Report

- (1) Within 90 days from publication of the OIG report, the Office of Research and Development will issue a VHA Directive to include a requirement that the local VA facility establish written procedures for “conducting periodic audits of approved research to access compliance with privacy, confidentiality, and information security requirements, including requirements under waivers of HIPAA authorization or informed consent.” The local procedures should specify which office or entity at the facility is responsible for these audits.
- (2) The Chief Research and Development Officer (12) will issue Interim Guidance from requiring written procedures described above, within 30 days from publication of the OIG report.
- (3) Within 60 days from publication of the OIG report, VHA Directive 1058 will be modified to include Research Information Security among oversight responsibilities of the Office of Research Oversight (ORO).
- (4) Checklists for Research Privacy and Confidentiality and Research Information Security will be provided on Office of Research Oversight (ORO) Website, upon publication of the OIG report.
- (5) Within 90 days from publication of the OIG report, the Office of Research and Development (12) and the Office of Research Oversight (10R) will incorporate Research Privacy and Confidentiality and Research Information Security requirements into curriculum for Office of Research and Development (ORD) Local Accountability Education Workshops and Office of Research Oversight (ORO) Technical Assistance Workshops for Facility and Network Research Compliance Officers.
- (6) ORO has already initiated a program to include Research Privacy and Confidentiality and Research Information Security in all of its on-site reviews and has developed an aggressive schedule of site visits with this focus.

**Recommendation (13).** We recommend that the Under Secretary for Health ensure that the Birmingham REAP Director and Associate Director discontinue the practice of receiving their official VA e-mail at the University of Birmingham, in violation of VA policy prohibiting storage of VA information on a non-VA system, resulting in potential Privacy Act or HIPAA violations.

Concur **Target Completion Date:** May 2004  
and on-going

Responsibility lies with the VA Office of Information and Technology (OI&T) to ensure all users comply with VA's May 2004 issued policy, VA Memorandum: Limits on the Use of Certain E-mail Features and Configurations. This policy strictly prohibits auto-forwarding of e-mail messages to addresses outside the VA network. In addition to monitoring and filtering through VA national gateways to ensure compliance, VA policy requires auditing and monitoring of e-mail traffic locally to verify compliance with the policy. Waivers to this existing policy must be requested through the Facility's Information Security Officer (ISO). Upon receipt of the OIG report, compliance with this policy will be emphasized during the National IRM and ISO conference calls.

**Recommendation (14).** We recommend that the Under Secretary for Health assess the alignment of Birmingham REAP management positions at the Birmingham VAMC, and take action to correct the dysfunctional management structure that led to an overall breakdown of management oversight, controls, and accountability of the Birmingham REAP. This should include:

- Correction of the Birmingham REAP Director's reporting relationship from the ACOS for Acute and Specialty Care, which was in name only and resulted in the lack of actual supervision over the REAP Director's activities, to the ACOS for Research who currently has facility-wide responsibility for research programs but no line authority over REAP managers or involvement in their activities.

- Establishment of an accurate functional description and performance plan to clarify Birmingham REAP managers' responsibilities and to hold them accountable for proper administration of REAP resources, to include equipment purchases, acquisition of server space, protection of sensitive information stored on VA systems and portable devices, office space security, and compliance with applicable VA policies and procedures.
- Clarification of the Medical Center Director and ACOS for Research's responsibility and line authority over all research programs at the facility, including the Birmingham REAP.

Concur                      **Target Completion Date:** 90 days from  
Publication of OIG report

Deputy Under Secretary for Health for Operations and Management (DUSHOM), in collaboration with the Chief Research and Development Officer (CRADO), will develop guidance as well as other materials (e.g. draft functional descriptions and performance plans) to assist REAPs, Centers of Excellence, VA medical centers, and Networks in delivering clear expectations of management oversight, controls, and accountability for research directors.

**Recommendation (15).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the Birmingham Medical Center Director for not ensuring appropriate management and administration of the Birmingham REAP and protection of the privacy and confidentiality of research subjects.

Concur                      **Target Completion Date:** October 1, 2007

Following receipt and review of the evidence, an appropriate administrative action will be initiated.

**Recommendation (16).** We recommend that the Under Secretary for Health ensure that appropriate administrative action is taken against the ACOS for Research for not ensuring appropriate management and administration of the Birmingham REAP.

Concur      **Target Completion Date:** October 1, 2007

Following receipt and review of the evidence, an appropriate administrative action will be initiated.

## Assistant Secretary for Information & Technology Comments

**Department of  
Veterans Affairs**

**Memorandum**

**Date:** June 27, 2007  
**From:** Assistant Secretary for Information and Technology (005)  
**Subject:** **Draft OIG - Administrative Investigation, Loss of VA Information, VA Medical Center, Birmingham, AL**  
**To:** Assistant Inspector General for Investigations (51)

I am responding to your draft report issued May 23, 2007, regarding the loss of VA information at the Birmingham Medical Center. The attached response addresses your recommendations to the Office of Information and Technology. If you have questions or would like additional information, please call Adair Martinez, Deputy Assistant Secretary for Information Protection & Risk Management, at 202-273-5645.

*(original signed by:)*  
Robert T. Howard

Attachment

## **Assistant Secretary for Information and Technology Comments to Office of Inspector General's Report**

The following Assistant Secretary for Information and Technology comments are submitted in response to the recommendations in the Office of Inspector General's Report:

### **OIG Recommendations**

**Recommendation (2).** We recommend that the Assistant Secretary for Information and Technology coordinate with the Office of Management and Budget and the President's Identity Theft Task Force to develop and issue Government-wide risk analysis criteria to determine under what conditions potential identity theft victims should be notified and offered free credit monitoring. In the interim, the Assistant Secretary for Information and Technology should re-evaluate VA policy to determine whether the loss of a solo personal identifier, such as a social security number only, would constitute a risk for identity theft for purposes of offering free credit monitoring.

Concur      **Target Completion Date:** December 07, 2007

On April 19, 2007, Secretary Nicholson concurred with the GAO Privacy report, stating in his response: "VA also agrees with GAO's recommendations that the Director of the Office of Management and Budget develop guidance for Federal agencies on conducting risk analyses to determine when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft as a result of a Federal data breach." The Secretary also referenced The Department's new Public Law 109-461 which requires that a non-VA entity or VA OIG conduct an independent risk analysis to determine the level of risk associated with the data breach. Based on the findings of the risk analysis, the statute requires that the Secretary provide notification to the affected individuals

and may provide one or more of the following: credit monitoring, fraud resolution services, and identity theft insurance. Attachment A is the June 15 memo for the record documenting the reasons the Assistant Secretary for Information and Technology (005) offered credit monitoring services to over 864,000 veterans, employees, and CMS healthcare providers affected by the Birmingham VA Medical Center data breach incident. VA is a member of the President's Identity Theft Task Force. The Task Force's April 2007 Strategic Plan recommended that federal agencies should reduce the unnecessary use of Social Security numbers (SSN), the most valuable commodity for an identity theft. VA continues working on this issue per the May 22, 2007 OMB M-07-16 Memorandum Subj: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

**Recommendation (4).** We recommend that the Assistant Secretary for Information and Technology revise VA Directive 6601 to require the use of encryption, or an otherwise effective tool, to properly protect personally identifiable information and other sensitive data stored on removable storage devices when used within VA.

Concur      **Target Completion Date:** December 07, 2007

Changes will be made to VA Directive 6601 to further strengthen the policy regarding the protection of removable storage devices when used within VA.

Several directives already require added protection for the storage of sensitive information. Among these is VA Directive 6601, "Removable Storage Media", which states that if (Removable Storage Media) is used to store sensitive information it must contain protective features that have the approval of the local senior OI&T official. "All VA sensitive information must be in a VA protected environment at all times, or it must be encrypted. OI&T must approve the protective conditions being employed." OI&T also implemented policies in 2006 prior to VA Directive 6601, which addressed the requirements to protect the personal data of all individuals, including veterans, dependents and



employees. Those protections extend to all data formats and media, including electronic, paper, and oral information. Secretary Nicholson's VA IT Directive 06-2, dated June 6, 2006, further states:

"3. Employees who are authorized to remove confidential and Privacy Act-protected data from the Department are required to take all precautions to safeguard that data until it is returned.

4. Employees authorized to remove electronic data must consult with their supervisors and Information Security Officers (ISOs) to ensure that the data is properly encrypted and password-protected in accordance with VA policy."

IT Directive 06-06, Safeguarding Removable Media, signed by Secretary Nicholson on September 29, 2006 also addresses guarding VA protected information stored on government furnished equipment in a mobile environment carried out of a VA office or a PC in an alternative work site; approved encryption software must be used.

**Recommendation (7).** We recommend that the Assistant Secretary for Information and Technology develop and implement policies describing the conditions under which VistA programmer level access may be granted for research purposes, including whether that access is project specific or for the term of employment, and take appropriate action to remove programmer access from individuals who do not meet those conditions.

Concur      **Target Completion Date:** September 30, 2007

VISN DATA WAREHOUSE – OI&T has been working in collaboration with VHA, Director, Health Data & Informatics on a decision memo which will realign the VHA National Data Warehouse Team under IT Field Operations (from VHA to OI&T) and place all VHA VISN Data Warehouse initiatives under a single management. This will facilitate the standardization of management and access. This effort is a result of the VA CIO's "Restricted Administrative Rights" directive, which calls for the tightening of controls for

high level access/rights and better management of and implementation of “Roles Based Access.” The implementation of restricted Administrative Rights is currently being implemented across VA.

PROGRAMMER ACCESS TO VISTA – Again, in accordance with the VA CIO’s “Restricted Administrative Rights” directive, this type level of access is in the process of being removed from all non OI&T staff and only assigned to OI&T staff who actually have appropriate “role based” need.

**Recommendation (10).** We recommend that the Assistant Secretary for Information and Technology disseminate and enforce the existing Standard Operating Procedure for access to Austin Automation Center’s nationwide SSN file, and issue policies and procedures regarding authorization to access all other Austin Automation Center data for research purposes.

Concur      **Target Completion Date:** September 30, 2007

Although the decision as to the need for the data will continue to be made by the Privacy Officer for Veterans Health Administration, the Corporate Data Center at Austin will modify the ability of anyone outside of Austin to grant this access through the ACRS system. We will republish procedures for obtaining access to these resources.

**Attachment A**

**Department of  
Veterans Affairs**

**Memorandum**

Date: June 15, 2007

From: Assistant Secretary for Information and Technology (005)

Subj: Credit Monitoring for Veterans, Employees, and CMS Healthcare Providers  
Impacted by the Birmingham VAMC Data Breach (WebCims 383001)

1. This memo is to serve as a record of the decision made by the Veterans Affairs (VA) to initiate credit monitoring services to veterans, employees and CMS healthcare providers affected by the Birmingham, Alabama, VA Medical Center (VAMC) data breach incident.
2. In January, 2007, Birmingham VAMC officials reported that a VA research external hard drive was missing, and that the external hard drive probably contained the personal information on over 254,000 deceased and living veterans and employees, and 1.37 million healthcare providers. The personal information on healthcare providers came from the Centers for Medicare and Medicaid Services (CMS).
3. The VA, VA Office of Inspector General (OIG) and Federal Bureau of Investigation (FBI) reacted immediately with a joint, coordinated investigation of the data breach. At VA's request under 38 USC 5724(a), CMS conducted an independent risk analysis for the CMS healthcare providers' data loss. On March 28, CMS provided VA with the written results, conclusions and recommendations of its independent risk analysis. CMS determined that there was a high risk that the loss of the personally identifiable information of the CMS' health care providers may result in harm to the individuals concerned, including identify theft. CMS requested that the VA "immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the drive."
4. In deciding under 38 USC 5724 whether VA would offer any credit protection services to the veterans, employees and CMS providers whose data was on the missing external hard drive, I also considered the following factors.

5. The President's Identity Theft Task Force (ITTF) issued a set of recommendations which recommended that Federal and Private entities be required to protect PII information to the fullest extent possible. The report is available at <http://www.ftc.gov/opa/2007/04/idtheft.shtm>

6. The Department of Justice (DoJ) issued a Memorandum on Identity Theft September 19, 2006, which recommended that personal information included individual data such as..."An SSN standing alone can generate identify theft."

<http://www.usdoj.gov/ittf/index.html> The Office of Management and Budget (OMB) issued a supporting memorandum and concurred with the ITTF on their personal information recommendation.

7. Moreover, based on the recommendations of the President's Identity Theft Task Force, the ITTF and OMB Memorandum, concerns expressed by the VA's congressional oversight committees after the May 2006 data loss, and the generally-available literature concerning identity theft and the utility of various categories of data to commit identity theft, on November 7, 2006, I issued a Memorandum that clearly articulates that VA will rapidly and effectively respond when there is evidence that individual's identities are at risk. Credit monitoring, fraud resolution and insurance protection will be made available to individuals whose identifiable personal information leaves VA control through loss or theft. The Memorandum outlines data loss as sensitive information that leaves VA control through loss or theft. Personally Identifiable Information (PII) is defined as information that at a minimum includes:

- Name and date of birth
- Name and full social security number
- Full social security number only or
- Name, full social security number and date of birth

8. Finally, the definition of sensitive personal information in 38 USC 5727(19), which is used in section 5724 determination whether to offer individuals credit protection services, includes data that was on the missing external hard drive.

9. Carefully considering the risks associated with the protection of PII data, and discussions with General Counsel, the VA executed a contract, on March 30, 2007, to provide credit monitoring services to the over 864,000 affected veterans, employees, and CMS healthcare providers whose full SSN numbers may be at risk. The decision was driven by the information available to me at that time, the need to pro-actively protect individuals from possible identity theft based on the sensitive personal information from possible identify theft.

10. I note that on May 22, 2007, OMB issued a Memorandum for all Federal agencies entitled “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”. The Memorandum is available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>. This memorandum also supports the decision made to offer credit protection services in this case. The Memorandum directs all Federal agencies to review their use of SSNs and within 120 days of the date of the OMB Memorandum establish a plan to eliminate the unnecessary collection and use of SSNs within eighteen months of May 22, 2007. (It is reasonable to conclude that OMB would not issue such instructions with such a short time line for compliance if the risk associated with SSNs was minimal.) The memorandum states “Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother’s maiden name.” Attachment 3, paragraph B4d. The Memorandum also states in part in footnote 41 that “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.” These statements, as well as the thrust of the memorandum as a whole supports the decision to offer credit protection services in this case.

*(original signed by:)*  
Robert T. Howard

## OIG Contact and Staff Acknowledgments

---

OIG Contact	James J. O'Neill (202) 565-7938
-------------	---------------------------------

---

Acknowledgments	Andrea Buck, MD, JD Stephen Jones Judy Shelly Brian Tullis Steven Wise Debbie Crawford Marisa Casado, RN Harvey Hittner
-----------------	--

## Report Distribution

### VA Distribution

Office of the Secretary  
Veterans Health Administration  
Veterans Benefits Administration  
National Cemetery Administration  
Assistant Secretaries  
Office of General Counsel  
Under Secretary for Health  
Assistant Secretary for Information and Technology  
Director, Veterans Integrated Service Network 7

### Non-VA Distribution

House Committee on Veterans' Affairs  
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies  
House Committee on Oversight and Government Reform  
Senate Committee on Veterans' Affairs  
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies  
Senate Committee on Homeland Security and Governmental Affairs  
National Veterans Service Organizations  
Government Accountability Office  
Office of Management and Budget  
U.S. Senate: Richard Shelby, Jeff Sessions  
U.S. House of Representatives: Spencer Bachus, Artur Davis

This report will be available in the near future on the OIG's Web site at <http://www.va.gov/oig/52/reports/mainlist.htm>. This report will remain on the OIG Web site for at least 2 fiscal years after it is issued.