



August 2016

ELECTRONIC HEALTH INFORMATION

HHS Needs to Strengthen Security and Privacy Guidance and Oversight

GAO Highlights

Highlights of [GAO-16-771](#), a report to the Committee on Health, Education, Labor, and Pensions, U.S. Senate

Why GAO Did This Study

As a digital version of a patient's medical record or chart, an EHR can make pertinent health information more readily available and usable for providers and patients. However, recent data breaches highlight the need to ensure the security and privacy of these records. HHS has primary responsibility for setting standards for protecting electronic health information and for enforcing compliance with these standards.

GAO was asked to review the current health information cybersecurity infrastructure. The specific objectives were to (1) describe expected benefits of and cyber threats to electronic health information, (2) determine the extent to which HHS security and privacy guidance for EHRs are consistent with federal cybersecurity guidance, and (3) assess the extent to which HHS oversees these requirements. To address these objectives, GAO reviewed relevant reports, federal guidance, and HHS documentation and interviewed subject matter experts and agency officials.

What GAO Recommends

GAO is making five recommendations, including that HHS update its guidance for protecting electronic health information to address key security elements, improve technical assistance it provides to covered entities, follow up on corrective actions, and establish metrics for gauging the effectiveness of its audit program. HHS generally concurred with the recommendations and stated it would take actions to implement them.

View [GAO-16-771](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

August 2016

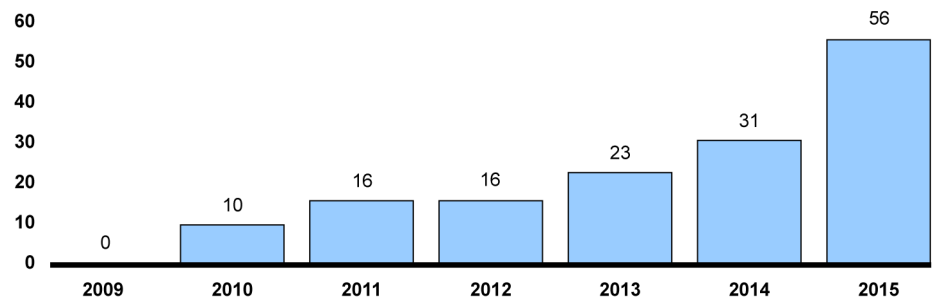
ELECTRONIC HEALTH INFORMATION

HHS Needs to Strengthen Security and Privacy Guidance and Oversight

What GAO Found

The use of electronic health information can allow providers to more efficiently share information and give patients easier access to their health information, among other benefits. Nonetheless, systems storing and transmitting health information in electronic form are vulnerable to cyber-based threats. The resulting breaches—involving over 113 million records in 2015—can have serious adverse impacts such as identity theft, fraud, and disruption of health care services, and their number has increased steadily in recent years, from 0 in 2009 to 56 in 2015 (see figure).

Number of Reported Hacking and Information Technology Breaches Affecting Health Care Records of 500 or More Individuals



Source: GAO analysis of Department of Health and Human Services data. | GAO-16-771

The Department of Health and Human Services (HHS) has established guidance for covered entities, such as health plans and care providers, for use in their efforts to comply with HIPAA requirements regarding the privacy and security of protected health information, but it does not address all elements called for by other federal cybersecurity guidance. Specifically, HHS's guidance does not address how covered entities should tailor their implementations of key security controls identified by the National Institute of Standards and Technology to their specific needs. Such controls include developing risk responses, among others. Further, covered entities and business associates have been challenged to comply with HHS requirements for risk assessment and management. Without more comprehensive guidance, covered entities may not be adequately protecting electronic health information from compromise.

HHS has established an oversight program for compliance with privacy and security regulations, but actions did not always fully verify that the regulations were implemented. Specifically, HHS's Office of Civil Rights investigates complaints of security or privacy violations, almost 18,000 of which were received in 2014. It also has established an audit program for covered entities' security and privacy programs. However, for some of its investigations it provided technical assistance that was not pertinent to identified problems, and in other cases it did not always follow up to ensure that agreed-upon corrective actions were taken once investigative cases were closed. Further, the office has not yet established benchmarks to assess the effectiveness of its audit program. These weaknesses result in less assurance that loss or misuse of health information is being adequately addressed.

Contents

Letter		1
	Background	3
	Electronic Health Information Can Offer Substantial Benefits but Faces a Variety of Security and Privacy Threats	7
	HHS Security and Privacy Guidance Does Not Fully Address Important Controls Outlined in Federal Guidance	16
	HHS Oversight Actions Did Not Always Ensure the Security and Privacy Rules Were Implemented	22
	Conclusions	29
	Recommendations for Executive Action	29
	Agency Comments and Our Evaluation	30
Appendix I	Objectives, Scope, and Methodology	32
Appendix II	Comments from the Department of Health & Human Services	34
Appendix III	GAO Contacts and Staff Acknowledgments	38
Table		
	Table1: Potential Adverse Impacts and Threat Sources Related to Health Care Information Systems	15
Figures		
	Figure 1: Number of Reported Hacking and Information Technology Breaches Affecting Health Care Records 500 Individuals or More	10
	Figure 2: Number of Health Care Records Compromised for All Reported Breaches Affecting 500 Individuals or More	11

Abbreviations

CMS	Centers for Medicare & Medicaid Services
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
EHR	electronic health record
ePHI	electronic protected health information
HHS	Department of Health and Human Services
FBI	Federal Bureau of Investigation
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH Act	Health Information Technology for Economic and Clinical Health Act
HSR	HIPAA Security Rule
IT	information technology
NIST	National Institute of Standards and Technology
OCR	Office of Civil Rights
ONC	Office of the National Coordinator for Health Information Technology
PHI	protected health information
PII	personally identifiable information
Privacy Rule	Standards for Privacy of Individually Identifiable Health Information
Security Rule	Security Standards for the Protection of Electronic Protected Health Information
UCLA	University of California, Los Angeles

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



August 26, 2016

The Honorable Lamar Alexander
Chairman
The Honorable Patty Murray
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate

Recent data breaches¹ at hospitals, insurance companies, and other entities in the health care industry have highlighted the importance of ensuring the security and privacy of electronic health information, including electronic health records (EHR). Two laws, The Health Insurance Portability and Accountability Act of 1996² (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act,³ provide for the creation, enforcement, and monitoring of information security and privacy standards for electronic health data. Under these two laws, the Department of Health and Human Services (HHS) has primary responsibility for setting standards for protecting electronic health information and enforcing standards that protect electronic health information.

To determine if the standards and guidance issued by HHS to protect electronic health records are consistent with federal information security guidance and if HHS oversight efforts are being effectively executed, you requested that we conduct a study of the current health information cybersecurity infrastructure. Our objectives were to (1) describe the expected benefits and cyber threats to electronic health information; (2) determine the extent to which HHS security and privacy guidance for electronic health records reflect and align with federal guidance; and (3)

¹The term “data breach” generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive information. A data breach can leave affected individuals vulnerable to identity theft or other fraudulent activity.

²Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9).

³Pub. L. No. 111-5, Div. A, Title XIII, 123 Stat. 115, 226-279 and Div. B, Title IV, 123 Stat. 467-496 (Feb. 17, 2009).

assess the extent to which HHS oversees compliance with HHS information security and privacy requirements at covered entities.

To address our first objective, we analyzed prior GAO reports that identified benefits of electronic health records. To identify major risks that can affect systems that collect, maintain, and share electronic health information, we analyzed prior GAO reports that identified security and privacy threats to data and information systems. We also reviewed third-party analyses of the threat landscape affecting electronic health data and systems and interviewed stakeholders and subject matter experts from organizations that collect and analyze data on this subject. Further, we analyzed information reported by HHS on health care data breaches affecting 500 or more individuals and interviewed knowledgeable HHS officials about the data. We determined that the data were sufficiently reliable for our purposes by interviewing knowledgeable agency officials and reviewing the data for obvious outliers.

For our second objective, we reviewed relevant information security and privacy laws and National Institute of Standards and Technology (NIST) standards and guidance to identify federal security and privacy control recommendations. We also obtained key documents from a representative sample of Security and Privacy Rules investigations conducted by the HHS Office of Civil Rights (OCR) that were closed between January 1, 2015, and December 10, 2015.

Regarding our third objective, we analyzed actions OCR took to close the representative sample of investigations that we used for the second objective. We compared OCR's actions with its stated mission of enforcing compliance with the Security and Privacy Rules and helping to ensure the security and privacy of electronic health information. We also interviewed knowledgeable OCR officials about their enforcement role and activities.

We conducted this performance audit from June 2015 to August 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Appendix I discusses our objectives, scope, and methodology in greater detail.

Background

Digitizing health information has many potential benefits including reducing costs and increasing medical accuracy. One key example of digitized health information is an electronic health record (EHR). An EHR is a digital version of a patient's paper medical record or chart. EHRs ideally make information available instantly and securely to authorized users. They can contain the medical and treatment history of a patient, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results. These records can also give a provider access to evidence-based tools for making decisions about a patient's care and can automate certain workflows.

System software for managing EHRs is typically purchased by providers (such as physicians, hospitals, and health systems) from vendors that develop the systems. When these systems are interoperable, information can be exchanged—sent from one provider to another—and then integrated into the receiving provider's EHR system, allowing the provider to use that health information to inform clinical care.

HIPAA Establishes Responsibilities for Developing and Enforcing Security and Privacy Standards

HIPAA required the Secretary of HHS to develop regulations protecting the privacy and security of health information. To fulfill this requirement, HHS published Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule) in December 2000 and Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) in February 2003.⁴

The Privacy Rule establishes national standards for safeguarding protected health information (PHI). PHI is individually identifiable health information⁵ that is transmitted or maintained in any form or medium. The Privacy Rule states that PHI may be used or disclosed to other parties by

⁴The HIPAA Privacy and Security Rules were promulgated at 45 C.F.R. Parts 160 and 164 and were updated at 78 Fed. Reg. 5566 (Jan. 25, 2013) and 79 Fed. Reg. 7290 (Feb. 6, 2014).

⁵Individually identifiable health information is information, including demographic information collected from an individual, that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) relates to the past, present, or future physical or mental health or condition of the individual or the provision of or payment for health care to the individual; and (3) can be used to identify the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103.

“covered entities”⁶ or their business associates only under specified circumstances or conditions, and generally requires that a covered entity or business associate make reasonable efforts to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose.

The Privacy Rule governs the use and disclosure of individuals’ health information and also provides individuals with privacy rights with regard to their health information. For example, the Privacy Rule provides the right to request restrictions on uses and disclosures of PHI, the right to adequate notification of privacy practices, the right of access to PHI, and the right to request amendments to inaccurate or incomplete PHI. The Privacy Rule also requires that covered entities and business associates employ appropriate safeguards for protecting PHI.

The Security Rule establishes nationwide standards for safeguarding PHI that is held or transferred electronically. It operationalizes the protections contained in the Privacy Rule by specifying administrative, technical, and physical security practices to secure individuals’ electronic protected health information (ePHI).⁷ For example, the Security Rule requires organizations to complete an enterprise-wide risk assessment and to create a risk management plan to address identified risks.

In the Security Rule, HHS distinguishes between “required” and “addressable” implementation controls. Required controls must be implemented. In contrast, the requirement to implement “addressable controls” is more open-ended. Organizations do not have to implement these controls if they determine they are not “reasonable and appropriate” and can document their reasons. However, they are required to implement equivalent alternative measures to achieve a comparable level of security assurance. Thus, while some action is required with regard to

⁶Covered entities are defined in regulations implementing the Health Insurance Portability and Accountability Act of 1996 as health plans that provide or pay for the medical care of individuals, a health care clearinghouse, and a health care provider who transmits any health information in electronic form in connection with a transaction covered by the regulations. 45 C.F.R. § 160.103.

⁷All individually identifiable health information a covered entity or business associate creates, receives, maintains or transmits in electronic form is referred to as ePHI, a subset of information covered by the Privacy Rule.

addressable controls, a wide variety of interpretations and alternative implementations is possible. Further, a variety of factors, such as implementation cost and organizational size, can be considered when making decisions on implementing addressable controls.

The HITECH Act was intended to promote the adoption and meaningful use of health information technology. Subtitle D of the act includes enhanced security and privacy protections associated with the electronic transmission of health information, in part through several provisions that strengthen the civil enforcement of the HIPAA rules. Further, the act requires HHS to establish an audit function to ensure the implementation of the Security and Privacy Rules by covered entities and business associates. Also, pursuant to the HITECH Act, HHS has issued the Interim Final Rule for Breach Notification for Unsecured Protected Health Information, effective September 23, 2009.⁸

Several components within HHS have responsibilities associated with implementing HIPAA and the HITECH Act. For example, one of the Centers for Medicare & Medicaid Services' (CMS) responsibilities under the HITECH Act is the administration of the Medicare and Medicaid Electronic Health Records program, which provides incentives for eligible entities that adopt and meaningfully use certified EHR technology. Additionally, the Office of the National Coordinator is responsible for setting standards for the implementation of systems that process electronic health records.

OCR's role is to implement and enforce the Privacy, Breach Notification and Security Rules. The office is divided into eight separate regions and a headquarters office in Washington, D.C. Each regional office has the authority to investigate cases which can either be opened by the regional office or assigned from the central intake unit located in headquarters. In addition to investigating potential HIPAA violations, OCR is also responsible for performing HIPAA compliance audits called for under the HITECH Act.

⁸The Breach Notification Rule governs when covered entities are required to provide notice of a breach of unsecured protected health information. 74 Fed. Reg. 42740-42770 (Aug. 24, 2009), amending 45 C.F.R. parts 160 and 164.

Health Care Is a Sector of the U.S. Critical Infrastructure

U.S. critical infrastructure is the necessary services that support the nation's society and serve as the backbone of our economy, health, and security. Critical infrastructure is comprised of systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the national public health or safety, nation's security, or national economic security. The critical infrastructure sectors were defined in Presidential Policy Directive 21 and consist of 16 sectors, one of which is health care and public health.

Public-private efforts to strengthen critical infrastructure help the public sector enhance security and rapidly respond to and recover from hazard events and assist the private sector in restoring business operations and minimizing losses. Because most critical infrastructure assets are owned and operated by the private sector, effective partnerships between private and public sectors are key to protecting them. In addition to health care, other sectors include financial services, communications, and information technology.

The President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013. The intent of the directive was to strengthen the security and resilience of critical infrastructure against evolving threats, while incorporating strong privacy and civil liberties protections into cybersecurity initiatives. It called for an updated national framework to reflect the increasing role of cybersecurity in securing physical assets. The order directed NIST to work with stakeholders to develop a voluntary framework, based on existing standards and industry best practices, for reducing cyber risks to critical infrastructure.

In response, in February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*.⁹ Created through collaboration between government and the private sector, the Cybersecurity Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective

⁹NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, Md.: Feb. 12, 2014).

approach of the framework is designed to help owners and operators of critical infrastructure apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.

Executive Order 13636 directed sector-specific federal agencies to establish, in coordination with the Department of Homeland Security, a voluntary program to support the adoption of the NIST Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities; create incentives to encourage owners and operators of critical infrastructure to participate in the voluntary program; and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

HHS was designated as the sector-specific agency for the health care and public health sector. As a sector-specific agency, HHS is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities for the sector. The health care and public health sector protects the health of the population before, during, and after any incident with actual or potential consequences. The sector consists of direct health care, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.

Electronic Health Information Can Offer Substantial Benefits but Faces a Variety of Security and Privacy Threats

Electronic Health Information Provides Many Benefits to Patients and Providers

The use of health information technology, including EHR systems, has the potential to allow health care providers and others to share health care information electronically, which may lead to improved health care quality and reduced costs. Electronic sharing of health information is especially important because the health care system is highly fragmented, with care and services provided in multiple settings, such as

physician offices and hospitals, that may not be coordinated. Because of this fragmentation, providers may lack ready access to critical information needed to coordinate the care of patients and to ensure that informed decisions are made about the best treatment options. Lack of care coordination can lead to inappropriate or duplicative tests and procedures that can increase health risks to patients and poorer patient outcomes. As we previously reported, estimates of this spending increase have ranged from \$148 billion to \$226 billion per year.¹⁰

EHR systems can overcome many of the limitations of manual health records. Sharing clinical data using manual methods such as faxing paper records can be time consuming and costly and may be unavailable at the point of care. In addition, data shared via manual methods are generally not formatted so that they can be easily accessed by other electronic systems or stored in EHRs. Lacking the ability to access and store manual data in their systems, providers may not be able to easily find the information they need or electronically transmit it to another provider. In contrast, effective electronic sharing of health information has the potential to bring patient information directly from an EHR to the health care professional providing the care, regardless of where the care or services are delivered or when the information is needed.¹¹

Electronically exchanging information is also important in new approaches to health care delivery, such as accountable care organizations, because of the need for providers in different settings to have ready access to information needed to manage and coordinate care. Accountable care organizations, as defined by the Centers for Medicare & Medicaid Services, are groups of doctors, hospitals, and other health care providers who collaborate to give coordinated care to Medicare patients. The goal of this coordinated care is to ensure that patients receive the right care at the right time while avoiding unnecessary duplication of

¹⁰GAO, *Electronic Health Records: HHS Strategy to Address Information Exchange Challenges Lacks Specific Prioritized Actions and Milestones*, [GAO-14-242](#) (Washington, D.C.: Mar. 24, 2014).

¹¹For more about the benefits of electronic health information exchange, see GAO, *Electronic Health Record Programs: Participation Has Increased, but Action Needed to Achieve Goals, Including Improved Quality of Care*, [GAO-14-207](#) (Washington, D.C.: Mar. 6, 2014); and *Electronic Health Records: Nonfederal Efforts to Help Achieve Health Information Interoperability*, [GAO-15-817](#) (Washington, D.C.: Sept. 16, 2015).

services and preventing medical errors. Electronic health records have the potential to improve the quality of care patients receive from such organizations and to reduce health care costs.

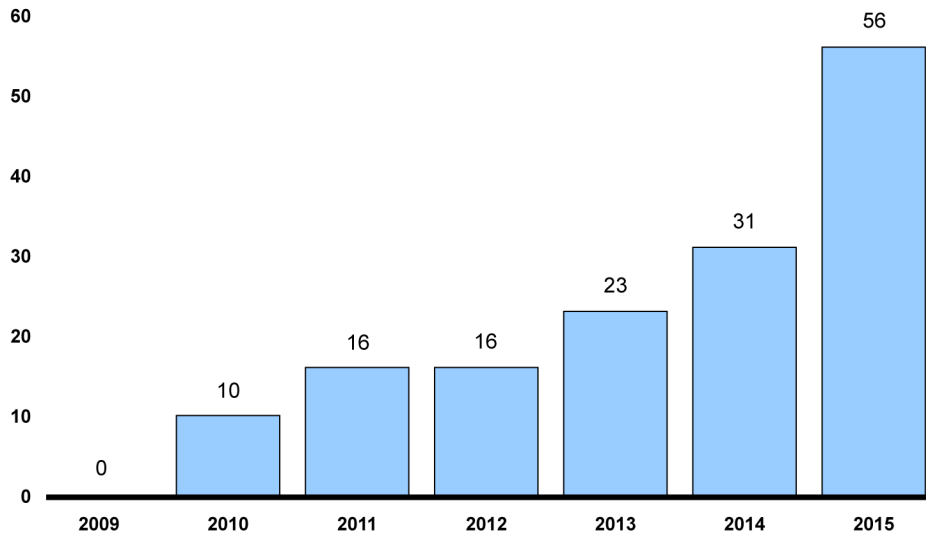
Finally, according to the Office of the National Coordinator for Health Information Technology, electronic exchange of health information is also important to patients themselves. The interoperable electronic exchange allows consumers to securely find and use vital health information, enhancing care delivery, public health, and research, and empowering them to make informed decisions regarding their health.¹²

The Number of Incidents Resulting in the Loss of Electronic Health Information Is Increasing

While electronic health information can offer many potential benefits, it can be vulnerable to security lapses that can jeopardize its confidentiality, integrity, and availability. More individuals' ePHI was compromised in 2015 than in any previous year following the establishment of the HITECH Act in 2009, according to data that health care providers reported to HHS. Based on these data, over 113 million individual health care records were compromised in 2015 due to hacking or other incidents. As figures 1 and 2 show, both the total number of reported breaches involving health care records as well as the number of individual records compromised have increased significantly since 2013.

¹²[GAO-15-817](#).

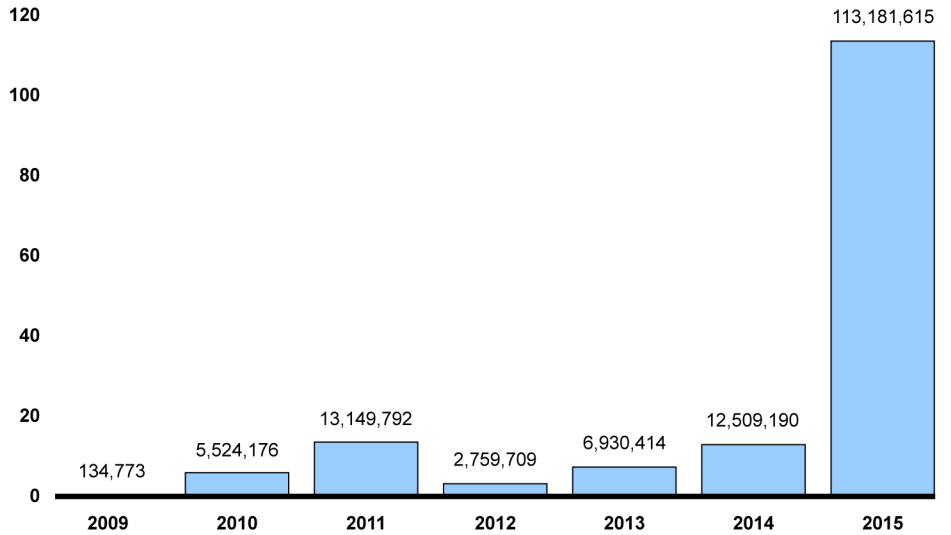
Figure 1: Number of Reported Hacking and Information Technology Breaches Affecting Health Care Records of 500 Individuals or More



Source: GAO analysis of Department of Health and Human Services data. | GAO-16-771

Note: In January 2015, the Office of Civil Rights (OCR) provided additional guidance to reporting entities which directed them to report some breaches as hacking or IT incidents instead of as theft as they may have previously reported.

Figure 2: Number of Health Care Records Compromised for All Reported Breaches Affecting 500 Individuals or More



Source: GAO analysis of Department of Health and Human Services data. | GAO-16-771

Note: These numbers of records are totals for reported breaches of 500 or more individuals.

The following are examples of recent large data breaches involving health care information.¹³

- In May 2015, the University of California, Los Angeles (UCLA) Health network discovered that records in its possession had been compromised in a cyberattack on its information technology (IT) systems. According to the UCLA Health website, the attackers accessed parts of the UCLA Health network that contained personally identifiable information (PII) such as names, addresses, dates of birth, Social Security numbers, medical record numbers, Medicare or health plan ID numbers, and some medical information. UCLA Health stated that it had notified the Federal Bureau of Investigation (FBI) regarding the cyberattack and pursued help from computer forensic experts to investigate the incident. According to UCLA Health, it offered affected individuals 12 months of identity theft recovery and restoration

¹³HHS officials have stated that these incidents are currently being actively investigated by OCR.

services as well as a \$1,000,000 insurance reimbursement policy and additional health care identity protection. In addition, individuals whose Social Security number or Medicare identification number was stored on the parts of the network that had been compromised were given 12 months of credit monitoring at no cost.

- In January 2015, Anthem, Inc. learned of a large-scale cyberattack on its IT systems. According to Anthem, the cyber-attackers obtained PII for approximately 79 million individuals with Anthem accounts and individuals who receive health care services in any of the areas that Anthem serves, including names, dates of birth, Social Security numbers, health care ID numbers, home addresses, e-mail addresses, and employment information such as income data. Anthem reported that, after discovering the attack, it contacted the FBI, began working to close the security vulnerability, and contracted with a cybersecurity firm to assist in the investigation and to strengthen the security of its systems. Anthem also set up a website with information specific to the incident and arranged to have identity protection services provided to compromised individuals at no cost for 2 years.
- Also in January 2015, Premera Blue Cross, which provides insurance primarily to individuals in Alaska and Washington, discovered that cyber attackers had gained unauthorized access to its IT systems. Premera reported the initial attack had occurred in May 2014 and that approximately 11 million records of patients and individuals who do business with Premera were affected. According to Premera, cyber attackers were able to access information such as names, addresses, e-mail addresses, telephone numbers, dates of birth, Social Security numbers, member identification numbers, medical claims information, and bank account information. Premera reported that it was cooperating with the FBI's investigation into the attack and was working with a cybersecurity contractor to remove the infection created by the attack.
- In July 2014, Community Health Systems, Inc. confirmed that its computer network had been the target of a cyberattack. Community Health Systems said that it engaged a cybersecurity contractor and was working with federal law enforcement authorities. According to its website, approximately 4.5 million individuals were affected, including those who were referred for or received services within the previous 5 years. The data included patient names, addresses, birthdates, telephone numbers, and Social Security numbers. Community Health Systems said it notified affected patients and regulatory agencies and

offered no-cost identity theft protection services to affected individuals.

These incidents reflect an increase in attacks against health information that has been reported by organizations that monitor global information security trends. For example, a study conducted by Mandiant reported that health care IT breaches, which had previously been a minor portion of their investigations, emerged in 2014 as a notable target for criminals.¹⁴ Likewise, a study done by KPMG reported in 2015 that a survey of health care executives indicated that health care organizations are frequently targeted compared to other types of organizations and the magnitude of the threat against health care information has grown exponentially.¹⁵ Specifically, four-fifths of executives at health care providers and payers told KPMG that their IT systems had been compromised by cyberattacks. In its own study of historical health care industry data breaches, Verizon reported that breaches of personally identifiable health information were diverse and affected more industries than just health care.¹⁶ In 2014, the FBI issued a warning to health care providers that the health care industry was not as resilient to cyber intrusions as the financial and retail sectors, increasing the potential for cyber intrusions.

¹⁴Mandiant, *M-Trends 2015: A view from the front lines*.

¹⁵KPMG, *Health Care and Cyber Security: Increasing Threats Require Increased Capabilities*.

¹⁶Verizon reported that their dataset included incidents from 25 countries, with 90 percent of the top-level North American Industry Classification System (NAICS) industry codes represented. In this dataset, health care is the industry with the largest reported breach size. See Verizon, *2015 Protected Health Information Data Breach Report*, 4-5.

Threats to Electronic Health Information Come from Multiple Sources and Can Have Significant Adverse Impacts

Threats to the security of systems containing health information can come from a variety of sources.¹⁷ Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, threat actors, foreign nations engaged in espionage, and health care industry insiders. These threat sources vary in terms of the capabilities, their willingness to act, and their motives, which can include monetary gain or other motives.

According to subject matter experts, the increasing extent to which electronic health information is subject to cyberattack reflects the increased value of the compromised data on the black market. According to these experts, criminals are aware that obtaining complete health records are often more useful than isolated financial information, such as credit information. Electronic health records often contain extensive amounts of information about an individual. Cyber criminals seeking access to health information for its resale value may use a variety of readily available software tools to carry out attacks, such as intercepting and capturing data as they are transmitted, exploiting known vulnerabilities¹⁸ in commercially available software, and using e-mail phishing techniques to gain unauthorized access to systems and information.

In addition to the threat of cyberattack, health IT systems face significant threats from insiders. While all of the breaches of over 1 million records in 2015 were attributed to outside attackers, a health care industry representative told us that insiders are consistently identified as the biggest threat. In addition to the threat of health care professionals and staff directly accessing medical records for unauthorized purposes, insiders may also fall victim to phishing attacks and other forms of social engineering that could provide outside attackers with unauthorized access to IT systems that they would not otherwise be able to obtain.

¹⁷Threats are any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

¹⁸Vulnerabilities are weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Finally, health information systems also face unintentional threats. According to Verizon, 45 percent of breaches of personally identifiable health information since 1994 have involved lost or stolen equipment that contained unencrypted information. Another 20 percent of breaches were attributable to errors such as mis-delivered documents, improper disposal, and publishing errors.

Table 1 summarizes potential adverse impacts as well as the types of groups or individuals that could pose threats to health information systems.

Table1: Potential Adverse Impacts and Threat Sources Related to Health Care Information Systems

Potential adverse impact	Potential threat source	Description
Identity theft	Criminal organizations	<p>Criminal organizations may attempt to obtain electronic health information and resell the data for monetary gain. Verizon reported that health records containing detailed personal information make it easy for criminals to engage in identity theft.^a</p> <p>Further, sensitive data can be unintentionally compromised when equipment containing unencrypted health information is discarded or misplaced. This information could then be used to facilitate identify theft.</p>
Insurance fraud	Criminal organizations	<p>Criminal organizations may attempt to gain unauthorized access to treatment information to commit medical insurance fraud.</p> <p>Verizon reported that criminals can use detailed health records to engage in medical billing fraud, increasing health care costs for governments, organizations, and individuals.^a</p>
Loss of personal privacy, embarrassment, or blackmail	Criminal organizations Insiders	<p>Criminal organizations and/or insiders could access data on medical conditions for purposes of blackmail, public embarrassment, or (in celebrity cases) sale to media outlets. For example, in 2008, staff at UCLA Medical Center leaked/sold actress Farrah Fawcett's medical records to tabloid magazines, exposing her medical treatment information^b</p> <p>Verizon reported that private and potentially embarrassing health information could be used to extort money or cause reputational harm to individuals, especially those in sensitive positions. In addition, insiders such as hospital staff may attempt to access medical data on acquaintances or celebrities for purely voyeuristic purposes and thus violate the personal privacy of the affected individuals.</p> <p>Further, sensitive data can be unintentionally compromised when equipment containing unencrypted health information is discarded or misplaced. This information could then be used to facilitate identify theft.</p>
Disruption of health care services	Threat actors	<p>Threat actors may seek to tamper with electronic health IT systems to cause disruptions in the medical community. For example, a threat actor could access and manipulate health records in an attempt to harm patients or disrupt health care operations at a medical facility (for example, by changing patient prescriptions).</p>

Potential adverse impact	Potential threat source	Description
National security impacts	Foreign governments	<p>Security professionals have stated that nation-states could access electronic health information for purposes of espionage. Subject matter experts stated in interviews that foreign governments may seek medical information about U.S. officials to identify health vulnerabilities to gain an advantage in business or diplomatic negotiations.</p> <p>Mandiant reported that a Russia-based threat group collecting intelligence for a sponsor government was deploying software tools to obtain remote access to elements of U.S. critical infrastructure, which includes hospitals and other health care provider organizations.</p> <p>In addition, individuals within foreign governments may seek personal gain from the sale of PII on Americans.</p>

Source: GAO analysis of published subject matter expert reports. | GAO-16-771

^aVerizon, 2015 Protected Health Information Data Breach Report, 29.

^bUCLA Health, UCLA statement on report about Farrah Fawcett's medical records, accessed July 15, 2016, <https://www.uclahealth.org/news/UCLA%20statement%20on%20report%20about%20Farrah%20Fawcetts%20medical%20records>.

HHS Security and Privacy Guidance Does Not Fully Address Important Controls Outlined in Federal Guidance

To encourage covered entities and business associates to implement effective security and privacy protections, HHS established guidance for compliance with the HIPAA requirements regarding the security and privacy of protected health information. However, HHS investigations, industry stakeholders, and HHS's own reviews have shown that organizations have struggled to select appropriate security and privacy controls. For critical infrastructure sectors, such as health care, NIST has published the Cybersecurity Framework to assist organizations in selecting and implementing appropriate controls. However, the guidance published by HHS does not address all of the elements in the NIST guidance. HHS officials said they intended their guidance to be minimally prescriptive to allow flexible implementation by a wide variety of covered entities. However, until these entities address all the elements of the NIST Cybersecurity Framework, their EHR systems and data are likely to remain unnecessarily exposed to security threats.

HHS Developed Security and Privacy Risk Assessment Guidance for Covered Entities

HHS recognizes that performing a comprehensive risk assessment is essential for organizations to understand their environment and to select appropriate security and privacy controls. Under the Security Rule promulgated by HHS, a key element for compliance with HIPAA requirements is completing a security risk assessment.¹⁹ HHS guidance states that conducting such an assessment serves as the foundation for an organization's security and privacy program as it represents a comprehensive determination of the risks that are common to the organization's core functions, processes, segments, common infrastructure, and information systems. A comprehensive risk assessment reduces the risk of a HIPAA violation and increases assurance that health information is protected appropriately.

According to OCR, an effective risk assessment includes analysis of the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that an organization creates, receives, maintains, or transmits. Security risk assessments are intended to be the basis for a wide variety of risk-based decisions and activities by organizations through all phases of designing, developing, implementing, and maintaining information security controls. OCR identifies such assessments as the first step in implementing safeguards and a cornerstone of effective HIPAA compliance.

Because security risk assessments are central to the implementation of effective security controls, OCR, in consultation with NIST, developed two sets of guidance to help organizations of different sizes perform risk assessments. According to OCR officials, the NIST HIPAA Security Rule (HSR) Toolkit²⁰ guidance was issued in 2010 and is meant to assist larger covered entities and their business associates in conducting security risk assessments. The stated purpose of the HSR Toolkit is to help covered entities and their business associates better understand the requirements of the HIPAA Security and Privacy Rules, implement those requirements, and assess those implementations in their operational environment.

¹⁹As used in this report, "HIPAA requirements" refer to the requirements of the Privacy and Security Rules, the regulations that implement HIPAA. Security risk assessments, referred to as a "risk analysis" in the regulation, are required under the Security Rule. 45 C.F.R. §§164.308(a)(1)(ii)(A).

²⁰The *NIST HIPAA Security Rule Toolkit* and materials can be found at this site: <https://scap.nist.gov/HIPAA/>.

In response to feedback that the HSR Toolkit was difficult for smaller entities to use, OCR issued additional guidance in coordination with the Office of the National Coordinator for Health Information Technology (ONC) in 2015. This guidance, referred to as the Security Risk Assessment Tool,²¹ is designed to provide smaller²² covered entities and business associates step-by-step guidance in conducting their assessments.

Both guidance documents address the implementation specifications identified in the HIPAA Security Rule and cover basic security practices, security failures, risk management, and personnel issues. The tools are organized as a series of questions addressing various security categories. Basic security practice questions include defining and managing access, backups, recoveries, and physical security. Risk management questions address periodic reviews and evaluations. Lastly, personnel issue questions address access to information as well as the on-boarding and release of staff.

Covered Entities and Business Associates Have Been Challenged to Comply with the HIPAA Security and Privacy Rules

OCR investigations, industry stakeholders, and HHS's own audits have shown that covered entities and their business associates face challenges in implementing the Security and Privacy Rules. Specifically, HHS data from 2015 show that performing risk assessments and developing risk management plans, which document how identified risks are to be addressed, are among the most challenging aspects of the rules for covered entities to implement. OCR investigations where corrective actions were required showed that approximately 23.9 percent²³ of complaints and breach reports received by HHS result in investigations that involve questions about how organizations have conducted risk

²¹The ONC security risk assessment guidance and materials can be found at this site: <https://www.healthit.gov/providers-professionals/security-risk-assessment-tool>.

²²HHS defines a smaller covered entity or business associate as practices with 1 to 10 health care providers. This includes providers such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies that transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

²³The 95% confidence interval for this estimate is (20.0, 27.8).

analyses and approximately 22.3 percent²⁴ involve how organizations developed risk management plans.

Further, stakeholders from the private sector have expressed concerns that risk management programs under the HHS guidance are difficult because requirements are not clearly defined. One stakeholder from a private sector organization who works on HIPAA compliance and assessment stated that it was difficult for organizations to know whether they had adequately addressed all the requirements.

OCR identified incomplete risk assessments as an area of concern during its pilot audit program. Under the HITECH Act, HHS was required to conduct periodic audits to ascertain whether covered entities and business associates are in compliance with the HIPAA Security and Privacy Rules. In response, OCR developed and implemented a pilot program that it used to conduct 115 audits of covered entities from 2012 to 2013. According to OCR officials, one trend identified during the pilot program was a failure to complete risk assessments at many of the covered entities that were audited. OCR officials noted that a failure to complete a comprehensive risk assessment can put an organization at a higher risk for failing to meet other HIPAA security and privacy requirements, which could result in a breach of ePHI.

HHS Security Guidance Does Not Fully Align with the NIST Cybersecurity Framework

The Security Rule requires covered entities and their business associates to perform risk analyses and create risk management plans. To provide guidance on assessing risks to ePHI, HHS developed the Security Rule Toolkit and Security Risk Assessment guidance. To supplement this guidance and provide organizations assistance in developing risk management plans that address identified risks, HHS published seven documents called the HIPAA Security Information Series.²⁵ Additionally, HHS has published several pieces of threat-specific guidance to assist

²⁴The 95% confidence interval for this estimate is (18.6, 25.9).

²⁵The *HIPAA Security Information Series* and other risk-specific guidance can be found at this site: <http://www.hhs.gov/hipaa/for-professionals/security/guidance/>.

covered entities in developing controls to address specific risks, such as the risks to mobile devices.²⁶

Similarly, NIST has published the Cybersecurity Framework to provide organizations in critical infrastructure sectors, including health care, guidance on designing an effective information security program, including both assessing risks and implementing controls to mitigate them. NIST's Cybersecurity Framework includes a core set of cybersecurity activities common to all critical infrastructure sectors that form a baseline of topics for critical infrastructure organizations to consider as they tailor specific implementations of security controls to meet their identified risks. The framework core is divided into five broad security functions (Identify, Protect, Detect, Respond, and Recover), which in turn are divided into 22 more specific categories²⁷ and 98 subcategories. The 98 subcategories generally correspond to security controls cited in NIST's guidance on security and privacy controls for federal information systems and organizations.

While adherence to the Cybersecurity Framework is voluntary, its core set of security controls represents a consensus of topics to consider when developing information security programs. It was developed by NIST with extensive collaboration among private and public sector stakeholders.²⁸ In February 2016, OCR acknowledged the importance of the framework by publishing the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework,²⁹ which maps the Security Rule's administrative, physical,

²⁶HHS guidance on securing mobile devices can be found at:

<https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security>.

²⁷The categories are: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Processes, Planning, Communications (Respond), Analysis, Mitigation, Improvements (Respond), Recovery Planning, Improvements (Recover), Communications (Recover).

²⁸For an analysis of the development of the framework, see GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, [GAO-16-152](#) (Washington, D.C.: Dec. 17, 2015).

²⁹The *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework* can be found at this site: <http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/>.

and technical controls to relevant subcategories in the framework. According to officials from HHS's Office of the Coordinator for Health Information Technology, this crosswalk was intended to show how organizations' existing HIPAA compliance efforts fit into the NIST guidance.

However, while the crosswalk demonstrated that the major elements of the Security Rule correspond to elements of the NIST Cybersecurity Framework, HHS guidance does not address many of the specific security control elements included in the Cybersecurity Framework. For example, of the 98 framework subcategories, the HSR Toolkit fully addresses only 19. Many of the specific controls detailed within the framework's 98 subcategories are not addressed in either the HHS security assessment guidance or in its other risk management guidance.³⁰ The HIPAA Security Information Series, which is intended to provide additional guidance on remediating risks, outlines a high-level approach to choosing and implementing controls and does not specifically address the Cybersecurity Framework controls or how covered entities and business associates should tailor them to meet their specific needs.

The Cybersecurity Framework subcategories that were not fully addressed include a wide range of security controls. For example, the guidance on risk assessments addresses controls from risk assessment subcategories, such as the need to develop and perform risk assessments, installing software updates, and receiving security alerts. However, it does not address controls in other risk assessment subcategories, such as penetration testing and developing risk responses. Penetration testing ensures that controls are operating as intended by testing to identify vulnerabilities that could be exploited. If security controls are not operating as intended, covered entities may be leaving their systems vulnerable to threats.

HHS officials stated that the HSR Toolkit and the Security Risk Assessment guidance were designed specifically for the risk analysis portion of the overall risk management process and thus were not intended to assist organizations in the selection and tailoring of specific

³⁰We considered a subcategory of the Cybersecurity Framework to be "fully addressed" if all of the controls that the framework references were addressed and "not addressed" if none of the controls that the framework references were addressed.

security controls to meet their needs. However, gaps in the overall set of guidance could lead to incomplete risk assessments and risk management plans as well as inconsistent implementation of security controls. Without addressing all major elements of the Cybersecurity Framework, the guidance may not be helping guide these entities as effectively as possible to comprehensively consider potential risks to the security and privacy of electronic health information. As a result, systems containing such information may remain unnecessarily vulnerable to breaches and other security and privacy threats.

HHS Oversight Actions Did Not Always Ensure the Security and Privacy Rules Were Implemented

To enforce the Security and Privacy Rules, HIPAA grants HHS investigatory powers and the ability to impose civil money penalties on covered entities. The Secretary of HHS delegated these responsibilities to OCR, which is charged with implementing and enforcing the HIPAA rules. As part of its oversight of the implementation of the Security, Breach Notification, and Privacy Rules by covered entities and business associates, OCR has established an enforcement program to review the high volume of complaints that are submitted each year. However, the office does not always ensure that identified issues are corrected and does not always issue appropriate guidance for cases resolved informally. Further, while the office has developed an audit function as an additional oversight function, as required under the HITECH Act, it is not yet fully operational and its effectiveness is not yet known. The office also has not demonstrated the effectiveness of its enforcement program over time or fully communicated or coordinated its enforcement results with the Centers for Medicare & Medicaid Services (CMS). Until HHS addresses these issues, it is likely missing opportunities to ensure compliance and to demonstrate the full effectiveness of its oversight program.

HHS Has Established a Program for Investigating Potential Violations of the HIPAA Security and Privacy Rules

Through OCR, HHS investigates potential violations of the HIPAA Security, Breach Notification, and Privacy Rules. These investigations may be initiated in several ways. For example, the office has established a system for individuals to submit complaints about potential data breaches or other potential violations of the HIPAA Security and Privacy Rules, which it may investigate if warranted and based on resource availability. HHS also provides covered entities a reporting system to

notify OCR of data breaches.³¹ The office assesses these cases to determine whether to initiate investigations.³² In addition, OCR can initiate its own investigations based on factors such as media reports, patterns of repeat violations, or referrals from other government organizations, among other instigating events.

OCR receives thousands of individual consumer complaints every year, and the number has been growing. For example, OCR reported receiving 17,779 complaints regarding the potential violations of HIPAA rules in 2014; 12,974 in 2013; and 10,457 in 2012. To address the high volume of cases that it receives, OCR has implemented a triage process where a central intake unit reviews all complaints as they are submitted and decides whether to (1) forward the complaint to a regional office for further review and potential investigation, (2) provide “technical assistance” in lieu of an investigation, or (3) decline to investigate.

Of the many complaints it receives, OCR opens investigations of relatively few.³³ Analysis of OCR case files shows that a variety of factors limit the number of investigations. Reasons OCR may decline to investigate a complaint include a lack of jurisdiction, a lack of consent from an individual to disclose information to the entity being investigated, allegations that would not constitute a violation of the Security and Privacy Rules, or covered entities no longer being in business. In some cases, instead of opening an investigation, the office may provide technical assistance intended to clarify the responsibilities of covered entities or how to implement specific aspects of the Security and Privacy Rules.

³¹Covered entities are required by 45 C.F.R. § 164.408 to notify HHS of potential breaches of unsecured PHI.

³²OCR automatically begins investigations on all breaches affecting 500 or more individuals and initiates investigations on breaches of fewer than 500 individuals at its discretion.

³³OCR reported receiving 17,779 complaints in 2014; 12,974 in 2013; and 10,457 in 2012. For 2014, the office reported that 89 percent of the complaints submitted were closed either on intake after review or after providing technical assistance. Of the remaining 11 percent, 4 percent had no violation found after investigation and 7 percent resulted in corrective action.

According to OCR officials, if the office conducts a complaint investigation, it has several options for reaching a resolution. It may conclude that no violation has occurred or that corrective actions have already been taken that address any identified deficiencies. Some investigations may result in a resolution agreement, which may contain items such as a binding corrective action plan, settlements, or requirements for reporting to HHS on progress. Consistent with the regulation, the office seeks primarily to resolve complaints through informal means and technical assistance and resorts to fines only in cases where the organization will not comply or in cases of willful neglect. In the preamble to the Enforcement Rule, HHS stated that based on its experience this method is effective and that the law does not mandate an adversarial approach.³⁴

OCR Technical Assistance Did Not Always Address Identified Issues

While OCR does not investigate all complaints that are submitted, in many cases it chooses to provide “technical assistance” intended to help covered entities and business associates comply with Security, Breach Notification, and Privacy Rule requirements. According to OCR officials, and consistent with regulation, providing technical assistance is a way to address cases that would otherwise be closed without an investigation. For the 2015 period we reviewed, in most of the cases where technical assistance was provided in lieu of a full investigation the guidance documents provided were relevant to the issue. However, for 12 of the 94 cases we reviewed the technical assistance was not directly applicable to the submitted complaint.

For example, in one case, a complaint was submitted about a covered entity using easily guessed passwords to secure protected health information before e-mailing it to individuals. HHS closed this complaint by sending the covered entity a checklist for securing postal mail and faxes rather than guidance for protecting e-mail. In several other cases complaints were made about ePHI being inappropriately accessible on a covered entity’s website. OCR provided guidance to the entities on password protections for workstations, which was not relevant to the identified website problem.

³⁴45 C.F.R. § 160.304. See also 71 Fed. Reg. 8390, 8394 (Feb. 16, 2006).

According to OCR officials, the reason that technical assistance does not always address identified problems is that OCR has only limited technical assistance guidance on hand, which may not always directly address identified issues, and there is no review process to ensure that it is consistent and relevant. OCR officials stated that resource limitations have prevented them from developing a more comprehensive set of technical guidance or establishing a review process. As a result, some complaints are closed with organizations receiving limited guidance on how to achieve compliance. The unaddressed weaknesses identified in the complaints increase the risk of future HIPAA violations and may result in entities continuing to employ weak security practices that could jeopardize the security and privacy of the electronic health information in their custody.

OCR Did Not Always Ensure That Corrective Actions Were Taken to Address Identified Issues

OCR's letters closing out cases that it investigated did not always include indications that covered entities had implemented or had committed to implement corrective actions or other measures to better adhere to the Security, Breach Notification, and Privacy Rules. Internal control standards state that to ensure identified deficiencies are corrected in a timely manner, oversight bodies should monitor the status of remediation efforts until they are completed.³⁵

During the 2015 period we reviewed, most of the identified actions were addressed before the cases were closed. However, in 13 of the 205 cases we reviewed where corrective actions were identified, such actions were not addressed before closure.

In one case HHS concluded that a covered entity that had suffered a breach had failed to fully address several key elements of the Security and Privacy Rules. Specifically, the entity had not completed a risk assessment or risk management plan, had not trained its staff appropriately, did not have written policies and procedures for securing protected health information, and did not use encryption. Although the entity reported implementing improved encryption and data loss

³⁵GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014) and *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: September 1999). The earlier version of the internal control standards was in effect through September 2015.

prevention software, it had not provided evidence of instituting the required training, establishing the required HIPAA compliance policies, or conducting the required enterprise-wide risk assessment and risk management plan. Nevertheless, HHS closed the investigation with these significant issues outstanding. In its close-out letter, HHS encouraged the entity to revisit its training policies and HIPAA compliance policies and reminded it of its responsibilities to perform a risk assessment and create a new risk management plan.

OCR requires monitoring of corrective actions for up to 3 years in cases where it and an entity under its jurisdiction enter into a settlement agreement. However in other cases, OCR does not generally follow up on investigations where corrective actions are ongoing or where such actions have not yet been fully implemented. HHS officials stated that the covered entities and business associates understand that not addressing identified issues could result in more serious enforcement actions if a repeat issue were identified in future investigations. HHS cited a lack of resources as the reason that it did not follow up with covered entities to ensure that corrective actions were being implemented before closing cases. OCR officials told us that they considered it a better use of resources to open and pursue new investigations rather than tie up resources waiting for covered entities to provide evidence that corrective actions had been taken. According to these officials, follow-up is resource intensive due to the need to constantly reassess an entity's progress and the quality of the actions it takes. Yet, without follow up, OCR cannot determine whether corrective actions have actually been made to address identified problems or whether covered entities have responded to technical assistance with improvements to their electronic health information protections. As a result, security and privacy weaknesses may remain unaddressed.

OCR's Audit Program Is Not Yet Operational, and Its Effectiveness Is Unknown

Under the HITECH Act, HHS is required to conduct periodic audits to ensure that covered entities and business associates are in compliance with the Security and Privacy Rules. In response, OCR developed and implemented a pilot program that it used to conduct 115 audits of covered entities and business partners from 2011 to 2012.

After the pilot program was completed, OCR analyzed the results and used them to make adjustments in its audit protocol, which it finalized in 2016. For example, according to OCR officials, the revised protocol makes the purpose of the audits clearer and provides more specific information about the types of documents and time frames involved in an

audit. OCR has announced that it will begin an initial round of audits in 2016 by selecting and reviewing 224 covered entities and business associates.³⁶ The audits will be a combination of desk audits and on-site reviews. While OCR officials acknowledged that this sample will not represent a statistically projectable population, they stated that they expect the results to highlight security and privacy issues facing covered entities and business associates. For example, the final report from their pilot project identified developing risk analyses and risk management plans as a challenge for many entities.

OCR has not yet determined the proportion of audits that will be desk audits versus site visits but expects the majority to be desk audits due to resource constraints. Desk audits are designed to be less-intensive document reviews that assess whether organizations have produced artifacts such as policies, procedures, and assessments as required under the Security, Breach Notification, and Privacy Rules. For site visits a team of assessors visits an organization for 2 to 5 days and conducts artifact reviews, interviews with organization personnel, and some verification of implementation. According to OCR officials, these reviews may include visual inspection of physical security controls but will not include technical control testing, such as scanning servers for software vulnerabilities.

An important piece of implementing effective internal controls, such as audit programs, is establishing performance measurements for management objectives such as these.³⁷ However, because no audits have yet been completed, it is not known whether OCR's audit program as currently planned will be effective in improving covered entities' adherence to the Security, Breach Notification, and Privacy Rules. OCR officials stated that the audit program's results could be used as a measure of the effectiveness of its overall enforcement program. However, OCR has not yet established benchmarks or performance measures to assess the effectiveness of the audit program when it

³⁶To select entities for review, OCR officials stated that they compiled a database from multiple sources, including several commercially available datasets as well as their own database of organizations reporting breaches of fewer than 500 individuals. OCR plans to maintain a database of approximately 14,000 entities to sample from for its audits.

³⁷[GAO-14-704G](#).

becomes operational. Without such benchmarks or measures it will be difficult to determine whether the audit efforts as designed are effective.

OCR and CMS Do Not Share Results of all Privacy and Security Rules Investigations

While OCR and the Centers for Medicare & Medicaid Services (CMS) coordinate through many joint activities,³⁸ including sharing information about breach reports, OCR and CMS do not share the results of their investigations internally. Sharing information across organizational boundaries can help organizations achieve their goals.³⁹

Specifically, OCR does not notify CMS of investigative cases it has completed in which it has determined that risks assessments were not conducted. A goal of the meaningful use incentive program that CMS administers is to ensure that providers have implemented the requirements that they have attested to, including the completion of risk assessments. Specifically, to receive the incentives, eligible professionals must attest that they have conducted a risk analysis as required by HIPAA. While CMS conducts its own audits of program participants' compliance with requirements for meaningful use incentives, OCR's investigations have at times also reviewed whether covered entities and business associates have conducted risk analyses, and in some cases it has determined that risk assessments were not completed. If those entities were also participating in the meaningful use incentive program, they should be ineligible for financial incentives. Nevertheless, OCR does not notify CMS of these cases that might indicate ineligibility.

Sharing this information could allow CMS to better ensure that recipients of financial incentives under the HITECH Act's meaningful use program have met the requirements for those incentives. In response, OCR stated that CMS currently investigates entities based on its own jurisdiction under meaningful use and other legal authorities and OCR and CMS does not regularly coordinate on investigations. However, without OCR and CMS sharing the results of investigations and audits, the potential is

³⁸OCR provides oversight and enforcement of covered entities' and their business associates' compliance with HIPAA. CMS is responsible for the administration of the Medicare and Medicaid Electronic Health Records Program, which provides financial incentives— estimated to be \$30 billion from 2011 through 2019—to eligible entities to adopt and meaningfully use certified EHR technology.

³⁹[GAO-14-704G](#).

increased for covered entities and business associates who have not fulfilled the requirements to be inappropriately receiving incentive payments.

Conclusions

While the increasing use of EHR systems has the potential to improve health care quality, they can be vulnerable to security lapses that can jeopardize the confidentiality, integrity, and availability of the information they contain. Data breaches experienced by covered entities and their business associates have resulted in tens of millions of individuals having sensitive information compromised.

As required by HIPAA, HHS issued the Security, Breach Notification, and Privacy Rules, as amended by the HITECH Act, and has implemented an oversight program to enforce compliance by covered entities and business associates. However, HHS's guidance does not address how covered entities should tailor their implementations of key security controls identified by the National Institute of Standards and Technology to their specific needs, and thus may not be as effective as it could be.

Although OCR continues to close thousands of cases per year, the closure activities in a significant minority of cases do not provide assurance that identified issues are addressed. When technical assistance is used to close cases, it does not always address the complaint directly or provide meaningful direction to organizations on how to comply with the Security and Privacy Rules. Further, cases that are closed with incomplete corrective actions and no follow-up do not provide assurance that covered entities and their business associates are completing the actions as agreed.

OCR has reported on steps it is taking to improve privacy and security in the health care sector, including taking significant enforcement actions and implementing its audit program. However, without establishing measures for progress in improving security and privacy through its audit program, it will be difficult to determine whether the program as designed is effective. Additionally, OCR does not routinely coordinate with CMS to help ensure that only eligible entities receive meaningful use incentive payments under the HITECH Act's EHR program.

Recommendations for Executive Action

To improve the effectiveness of HHS guidance and oversight of privacy and security for health information we recommend that the Secretary of Health and Human Services take the following actions:

-
- update security guidance for covered entities and business associates to ensure that the guidance addresses implementation of controls described in the NIST Cybersecurity Framework;
 - update technical assistance that is provided to covered entities and business associates to address technical security concerns;
 - revise the current enforcement program to include following up on the implementation of corrective actions;
 - establish performance measures for the OCR audit program; and
 - establish and implement policies and procedures for sharing the results of investigations and audits between OCR and CMS to help ensure that covered entities and business associates are in compliance with HIPAA and the HITECH Act.

Agency Comments and Our Evaluation

We provided a draft copy of this report to HHS for review and comment, and in response the department provided written comments, which are reproduced in appendix II. HHS stated that it concurred with three of the five recommendations in the draft report and would take actions to implement them. The department did not agree or disagree with the remaining two recommendations but stated that it would consider taking actions to implement them as well.

Regarding our third recommendation—that HHS revise the current enforcement program to include following up on the implementation of corrective actions—HHS stated that for settlement agreements, OCR follows up with entities to ensure corrective actions have been taken. We agree that for these cases, follow up does occur and have clarified this in the final report. However, for cases that do not result in a settlement agreement, ensuring that corrective actions have been taken would provide OCR greater assurance that entities have implemented actions to come into compliance with HIPAA requirements. Additionally, for those cases that we identified where corrective actions had not been completed before case closure, we intend to provide HHS with additional requested information.

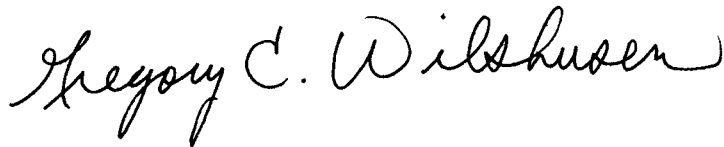
With regard to our fifth recommendation—that HHS improve information sharing between OCR and CMS on organizations that may be in violation of HIPAA requirements—HHS noted that OCR shares information with CMS on breach reports. We note this in the report. However, our recommendation focuses on OCR sharing information about the results of its investigations with CMS, which is not currently done. Sharing this information could allow CMS to better ensure that recipients of financial

incentives under the HITECH Act's meaningful use program have met the requirements for those incentives.

HHS also provided technical comments, which we incorporated as appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Department of Health and Human Services. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staffs have questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244. He can also be reached by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the expected benefits and cyber threats to electronic health information; (2) determine the extent to which the Department of Health and Human Services' (HHS) security and privacy guidance for electronic health records reflect and align with federal guidance; and (3) assess the extent to which HHS oversees compliance with HHS information security and privacy requirements at covered entities.

To address our first objective, we analyzed prior GAO reports that identified benefits of electronic health records and security and privacy threats to data and information systems to identify major risks that can affect systems that collect, maintain, and share electronic health information. We also reviewed independent analyses of the threat landscape affecting electronic health data and systems and interviewed subject matter experts and stakeholders from organizations that collect and analyze data on this subject. We identified these experts and stakeholders through interviews with agency officials and other stakeholders. They were considered subject matter experts and stakeholders based on job titles, organizational affiliation, and publications. Further, we analyzed information reported by HHS on health care data breaches affecting over 500 individuals and interviewed knowledgeable HHS officials about the data. We determined that the data were sufficiently reliable for our purposes by interviewing knowledgeable agency officials and reviewing the data for obvious outliers.

Regarding our second objective, we reviewed relevant information security and privacy laws, including the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act. Additionally, we reviewed the Security, Breach Notification, and Privacy rules issued by HHS. We also reviewed National Institute of Standards and Technology (NIST) standards and guidance, including the Cybersecurity Framework and Special Publication 800-53, Security and Privacy Controls for Federal Information Systems, to identify baseline security and privacy controls that are recommended for consideration when conducting security risk assessments. We compared these controls to those cited in HHS's security risk assessment guidance to identify potential gaps in the guidance. We also obtained key documents from a representative sample of Security, Breach Notification, and Privacy Rules investigations conducted by HHS's Office of Civil Rights (OCR) that were closed between January 1, 2015, and December 10, 2015. Specifically, we obtained and analyzed key documents, such as notification letters and closure letters, associated with 205 cases that OCR determined required a corrective action and 94 cases where OCR

provided technical assistance in lieu of investigation. Estimates based on a probability sample are subject to sampling error. Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our particular sample's results as a 95 percent confidence interval (e.g., plus or minus 10 percentage points). This is the interval that would contain the actual population value for 95 percent of the samples we could have drawn. We determined that these data were sufficiently reliable for our purposes by examining the data for outliers and interviewing knowledgeable officials about any discrepancies we identified. We also interviewed knowledgeable HHS officials to understand the purpose and structure of the HHS guidance.

To address our third objective, we analyzed actions OCR took to close the representative sample of investigations that we used for the second objective. We analyzed the circumstances under which OCR directed that a corrective action be taken, provided technical assistance on complying with the Security and Privacy Rules, or closed cases without taking any action. We analyzed and compared OCR's actions with its stated mission of enforcing compliance with the Security and Privacy Rules and helping to oversee standards for the security and privacy of protected health information. We also interviewed knowledgeable OCR and CMS officials about their enforcement role and oversight activities.

We conducted this performance audit from June 2015 to August 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

AUG 10 2016

Gregory C. Wilshusen
Director of Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Wilshusen:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, *"Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight"* (GAO-16-771).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

A handwritten signature in black ink that reads "Jim R. Esquea".

Jim R. Esquea
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: ELECTRONIC HEALTH INFORMATION: HHS NEEDS TO STRENGTHEN SECURITY AND PRIVACY GUIDANCE AND OVERSIGHT (GAO-16-771)

The U.S. Department of Health and Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation

To improve the effectiveness of its guidance and oversight of privacy and security for health information, we recommend that the Secretary of Health and Human Services update security guidance for covered entities and business associates to ensure that the guidance addresses implementation of controls described in the NIST Cybersecurity Framework.

HHS Response

HHS concurs with the recommendation for the Office for Civil Rights (OCR) to update its security guidance for HIPAA covered entities and their business associates to ensure that the guidance more fully addresses implementation of controls described in the NIST Cybersecurity Framework. The Framework was developed by NIST to apply to all sectors of the United States economy and describes a specific approach to understanding and responding to cybersecurity issues, which includes administrative, technical, and physical safeguards in addition to risk assessment. We appreciate the comments from GAO and from industry stakeholders provided in the report that: OCR's current guidance does not address all of the security control elements in the Framework; risk management under the HIPAA Security Rule is difficult, because the requirements may not be clearly defined; and OCR's risk assessment guidance is not intended to cover risk management activities.

OCR's website houses many helpful guidance documents for HIPAA covered entities and business associates to comply with the requirements of the HIPAA Security Rule, which include technology-neutral guidance on risk assessment, mobile device security, and NIST guidance, among others, that are flexible and scalable for use by the many different entities that HIPAA regulates. For example, OCR's risk assessment guidance was developed with our partners at NIST and the Office of the National Coordinator for Health Information Technology (ONC) to help HIPAA covered entities and business associates comply with the requirement of the HIPAA Security Rule at 45 C.F.R. § 164.308(a)(1)(ii)(A) that entities conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the electronic protected health information (ePHI) in their enterprises. Additionally, as pointed out in the Report, OCR, ONC, and NIST have already developed a map of all applicable provisions of the HIPAA Security Rule to the Framework, as a result of requests by HIPAA covered entities and their business associates to provide more information on how to understand the Framework from a HIPAA perspective. However, OCR will work to provide additional guidance on the requirements of the HIPAA Security Rule, to the extent feasible, given OCR's resource constraints and other priorities. For example, OCR can develop additional guidance addressing provisions at 45 C.F.R. § 164.308(a)(1)(ii)(B), that require entities to implement security measures (administrative, technical, and physical safeguards) to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level. Any guidance that OCR develops must incorporate the flexible and scalable nature of the HIPAA Security Rule's technology-neutral requirements, particularly with regard to the extreme diversity among HIPAA covered entities and

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: ELECTRONIC HEALTH INFORMATION: HHS NEEDS TO STRENGTHEN SECURITY AND PRIVACY GUIDANCE AND OVERSIGHT (GAO-16-771)

their business associates, so that covered entities and business associates can develop and implement safeguards that work best for their enterprises.

Recommendation

To improve the effectiveness of its guidance and oversight of privacy and security for health information we recommend that the Secretary of Health and Human Services update technical assistance that is provided to covered entities and business associates to address technical security concerns.

HHS Response

HHS concurs with the recommendation for OCR to provide technical assistance materials to HIPAA covered entities and their business associates that are more applicable to allegations in complaints filed against them. As a result of GAO's helpful review in this matter, OCR plans to update its technical assistance materials to provide such guidance to covered entities and business associates and refer them to additional guidance on OCR's website, which contains many resources for covered entities and business associate to use to come into compliance with the HIPAA Rules, including frequently-asked questions, videos, technical guidance documents, and links to helpful resources from other federal government partners, including ONC and NIST. In this effort, we appreciate GAO's willingness to share additional information about the 12 (of 94) cases it identified where the technical assistance did not directly apply to the allegations in the complaint.

Recommendation

To improve the effectiveness of its guidance and oversight of privacy and security for health information we recommend that the Secretary of Health and Human Services revise the current enforcement program to include following up on the implementation of corrective actions.

HHS Response

HHS appreciates GAO's recommendation for OCR to revise the current enforcement program to include additional contact with and requests for additional information from HIPAA covered entities and their business associates after the conclusion of investigations. OCR already requires two or three year monitoring as part of corrective actions plans in settlement agreements resolving cases that highlight ongoing compliance issues in the health care industry, systemic or egregious conduct, or other important considerations under the HIPAA Rules, as detailed on our website. OCR will consider how best to implement this recommendation in other cases, given the number of complaint investigations, compliance reviews, and breach compliance reviews that OCR currently undertakes, the increasing number of complaints and referrals OCR receives each year, and the audits that OCR is now performing, taking into account the number of investigators and other OCR resources necessary for such requests for information and reviews of such additional information submitted pursuant to such requests. Further, OCR is sensitive to the burdens on HIPAA covered entities and business associates that investigatory document requests from OCR place on such entities, and must consider how best to implement this recommendation without creating unwarranted burdens on such entities once an investigation is closed. In considering this issue, OCR would appreciate additional information about the 13 (of 205) investigated cases that GAO identified where specific corrective actions may not have been fully addressed before closure.

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: ELECTRONIC HEALTH INFORMATION: HHS NEEDS TO STRENGTHEN SECURITY AND PRIVACY GUIDANCE AND OVERSIGHT (GAO-16-771)

Recommendation

To improve the effectiveness of its guidance and oversight of privacy and security for health information we recommend that the Secretary of Health and Human Services establish performance measures for the OCR audit program.

HHS Response

HHS concurs with this recommendation. OCR initiated Phase 2 of its audit program, and intends to use the results of Phase 2 to ensure that our permanent audit program reflects lessons-learned and effective practices. To develop the measures recommended by GAO, OCR will evaluate the results of Phase 2, as they unfold. As OCR completes Phase 2 and continues to implement the audit program required by HITECH, we will develop measures to evaluate the efficacy of the audits and the overall program.

Recommendation

To improve the effectiveness of its guidance and oversight of privacy and security for health information we recommend that the Secretary of Health and Human Services establish and implement policies and procedures for sharing the results of investigations and audits between OCR and CMS to help ensure that covered entities and business associates are in compliance with HIPAA and the HITECH Act.

HHS Response

Within HHS, OCR already shares information about breach reports that involve cybersecurity incidents that OCR receives with the Centers for Medicare and Medicaid Services (CMS) and other HHS agencies. OCR and CMS are happy to consider coordinating on information-sharing about investigations and audits that implicate CMS's Electronic Health Record Incentive Program.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact named above, John de Ferrari (assistant director), Thomas Johnson (Analyst in Charge), Carl Barden, Andrea Harvey, Wilfred Holloway, Lee McCracken, Monica Perez-Nelson, Justin Palk, and Paige Teigen made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.