United States Government Accountability Office

Report to Congressional Requesters

March 2016

HEALTHCARE.GOV

Actions Needed to Enhance Information Security and Privacy Controls

Accessible Version

GAO-16-265

GAO Highlights

Highlights of GAO-16-265, a report to congressional requesters

March 2016

HEALTHCARE.GOV

Actions Needed to Enhance Information Security and Privacy Controls

Why GAO Did This Study

The Patient Protection and Affordable Care Act required the establishment of health insurance marketplaces in each state to allow consumers to compare, select, and purchase health insurance plans. States establishing their own marketplaces are responsible for securing the supporting information systems to protect sensitive personal information they contain. CMS is responsible for overseeing states' efforts, as well as securing federal systems to which marketplaces connect, including its data hub.

GAO was asked to review security issues related to the data hub, and CMS oversight of state-based marketplaces. Its objectives were to (1) describe security and privacy incidents reported for Healthcare.gov and related systems, (2) assess the effectiveness of security controls for the data hub, and (3) assess CMS oversight of state-based marketplaces and the security of selected state-based marketplaces. GAO reviewed incident data, analyzed networks and controls, reviewed policies and procedures, and interviewed CMS and marketplace officials. This is a public version of a limited official use only report that GAO issued in March 2016. Sensitive information on technical issues has been omitted from this version.

What GAO Recommends

GAO is recommending that CMS define procedures for overseeing the security of state-based marketplaces and require continuous monitoring of state marketplace security controls. HHS concurred with GAO's recommendations.

View GAO-16-265. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The Centers for Medicare & Medicaid Services (CMS) reported 316 security-related incidents, between October 2013 and March 2015, affecting Healthcare.gov—the web portal for the federal health insurance marketplace—and its supporting systems. According to GAO's review of CMS records for this period, the majority of these incidents involved such things as electronic probing of CMS systems by potential attackers, which did not lead to compromise of any systems, or the physical or electronic mailing of sensitive information to an incorrect recipient. None of the incidents included evidence that an outside attacker had successfully compromised sensitive data, such as personally identifiable information.

Consistent with federal guidance, CMS has taken steps to protect the security and privacy of data processed and maintained by the systems and connections supporting Healthcare.gov, including the Federal Data Services Hub (data hub). The data hub is a portal for exchanging information between the federal marketplace and CMS's external partners. To protect these systems, CMS assigned responsibilities to appropriate officials and documented information security policies and procedures.

However, GAO identified weaknesses in technical controls protecting the data flowing through the data hub. These included

- insufficiently restricted administrator privileges for data hub systems,
- inconsistent application of security patches, and
- insecure configuration of an administrative network.

GAO also identified additional weaknesses in technical controls that could place sensitive information at risk of unauthorized disclosure, modification, or loss. In a separate report, with limited distribution, GAO recommended 27 actions to mitigate the identified weaknesses.

In addition, while CMS has taken steps to oversee the security and privacy of data processed and maintained by state-based marketplaces, improvements are needed. For example, CMS assigned roles and responsibilities to various oversight entities, met regularly with state officials, and developed a reporting tool to monitor performance. However, it has not defined specific oversight procedures, such as the timing for when each activity should occur, or what follow-up corrective actions should be performed if deficiencies are identified. Further, CMS does not require sufficiently frequent monitoring of the effectiveness of security controls for state-based marketplaces, only requiring testing once every 3 years.

GAO identified significant weaknesses in the controls at three selected state-based marketplaces. These included insufficient encryption and inadequately configured firewalls, among others. In September 2015, GAO reported these results to the three states, which generally agreed and have plans in place to address the weaknesses. Without well-defined oversight procedures and more frequent monitoring of security controls, CMS has less assurance that state-based marketplaces are adequately protected against risks to the sensitive data they collect, process, and maintain.

Contents

Table

Figures

Abbreviations

CCIIO	Center for Consumer Information and Insurance Oversight
CHIP	Children's Health Insurance Program
CMCS	Center for Medicaid and CHIP Services
CMS	Centers for Medicare & Medicaid Services
data hub	Federal Data Services Hub
FISMA	Federal Information Security Modernization Act of 2014
HHS	Department of Health and Human Services
IRS	Internal Revenue Service
IT	information technology
MARS-E	Minimum Acceptable Risk Standards for Exchanges
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OTS	Office of Technology Solutions

PII	personally identifiable information
PPACA	Patient Protection and Affordable Care Act
SMART	State Based Marketplace Annual Reporting Tool
URL	uniform resource locator

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 23, 2016

Congressional Requesters

The Patient Protection and Affordable Care Act (PPACA),[1] signed into law on March 23, 2010, includes provisions to reform aspects of the private health insurance market and expand the availability and affordability of health care coverage. It required the establishment of health insurance exchanges, now commonly referred to as "marketplaces,"[2] in each state[3] by January 1, 2014. These marketplaces are required to allow consumers and small employers to compare, select, and purchase health insurance offered by participating private issuers of qualified health plans.[4]

The Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) is responsible for overseeing the establishment and operation of these marketplaces, including creating a federally facilitated marketplace in states not establishing their own. States choosing to implement their own marketplaces are responsible for securing the information systems that support the marketplace and their connections to the federal marketplace and for protecting the data collected and processed by the marketplace.

Given the high degree of congressional interest in the development and launch of the marketplaces, GAO has conducted a body of work in this area in order to assist Congress with its oversight responsibilities, of which this is the final report. This report examines the privacy and security issues related to the implementation of the Federal Services Data Hub (data hub)—a portal for exchanging information between the federal

[1]Pub. L. No. 111-148, §§ 1311(b), 1321(c), 124 Stat. 119, 173, 186 (Mar. 23, 2010) (hereafter, "PPACA"), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-52, 124 Stat. 1029 (Mar. 30, 2010). PPACA requires the establishment of health insurance exchanges, now known as marketplaces.

[2]In this report, we use the term "marketplace."

[3]In this report, the term "state" includes the District of Columbia.

[4]PPACA requires the insurance plans offered under an exchange, known as qualified health plans, to provide a package of essential health benefits—including coverage for specific service categories, such as ambulatory care, prescription drugs, and hospitalization.

marketplace and CMS's external partners—and CMS's oversight of the state-based marketplaces. Our specific objectives were to (1) describe the extent to which security and privacy incidents were reported for Healthcare.gov or key supporting systems; (2) assess the effectiveness of the controls implemented by CMS to protect the data hub and the information it transmits; and (3) assess the effectiveness of CMS's oversight of key program elements and controls implemented by state-based marketplaces and the effectiveness of those elements at selected state-based marketplaces to protect the information they contain.

This is a public version of a limited official use only report we issued in March 2016. Sensitive information, such as detailed descriptions of information security weaknesses, has been omitted. Nevertheless, it addresses the same objectives and scope as the limited official use only report. Also, the overall methodology used for both reports is the same.

To address our first objective, we reviewed and analyzed data on information security and privacy incidents reported by CMS affecting Healthcare.gov and its supporting systems. Specifically, we reviewed a list of reported incidents and the information in CMS records associated with each incident, such as the incident reports and documentation of actions taken to mitigate the incidents. We analyzed this information to identify relevant statistics on the reported incidents.

To address our second objective, we analyzed the overall network control environment, identified interconnectivity and control points, and reviewed controls for the network and servers supporting the data hub. Specifically, we reviewed controls over the data hub and its supporting software, as well as the operating systems, network, and computing infrastructure provided by the contractor. In order to evaluate CMS's controls over its information systems supporting Healthcare.gov, we used our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; National Institute of Standards and Technology (NIST) standards and guidelines; and CMS policies, procedures, practices, and standards. We performed our work at CMS contractor facilities in Columbia, Maryland, and Chantilly, Virginia.

To address our third objective, we selected three states for review by concentrating on states that received a high amount of PPACA grant funding through 2014, while ensuring a mix of both population size and contractors used. To assess the effectiveness of the three selected states' key management controls, we compared their documented

policies, procedures, and practices to the provisions and requirements contained in CMS security and privacy standards for state-based marketplaces. To evaluate the technical controls implemented for their marketplaces, we analyzed the overall network control environment, identified control points, and reviewed controls for the supporting network and servers and compared these controls to those specified in our *Federal Information System Controls Audit Manual*, NIST guidance, and CMS guidance for state-based marketplaces. Lastly, to determine the effectiveness of CMS oversight of the states' program elements and controls, we reviewed and analyzed CMS policies and procedures regarding oversight of the state-based marketplaces and compared them to federal guidance on security controls testing and GAO's *Standards for Internal Control in the Federal Government*. We also obtained and reviewed oversight-related documentation that CMS provided to the three selected states.

We conducted this performance audit from December 2014 to March 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. A full description of our objectives, scope, and methodology can be found in appendix I.

Background

PPACA directed each state to establish and operate a state-based health insurance marketplace by January 1, 2014.[5] These marketplaces were intended to provide a seamless, single point-of-access for individuals to enroll in private health plans, apply for income-based financial assistance established under the law, and, as applicable, obtain an eligibility determination for other health coverage programs, such as Medicaid or the Children's Health Insurance Program (CHIP).[6]

[5]PPACA, § 1311(b)(1), 124 Stat. at 173.

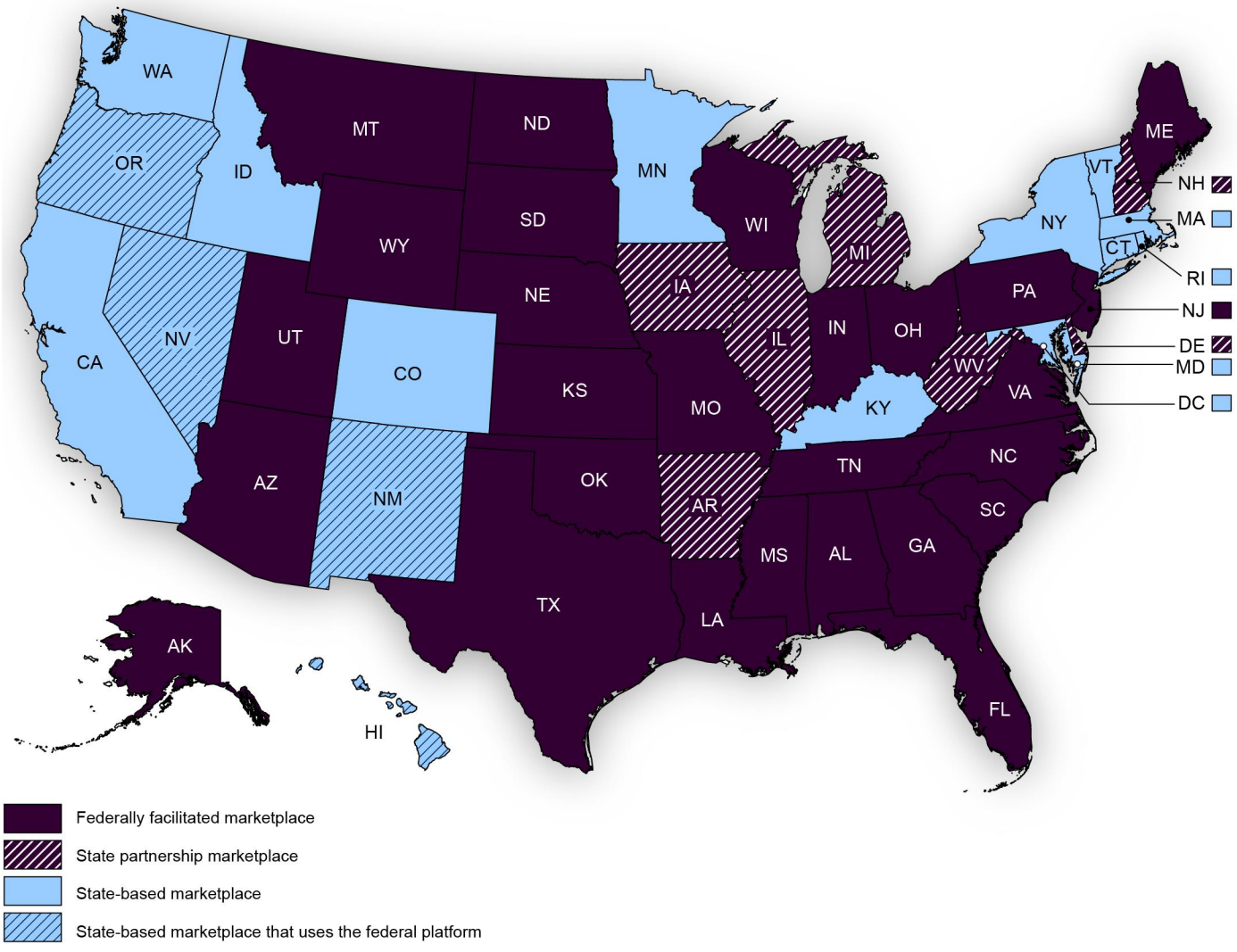
[6]Medicaid is a joint federal-state program that finances health care coverage for certain low-income individuals. CHIP is a federal-state program that provides health care coverage to children 19 years of age and younger living in low-income families whose incomes exceed the eligibility requirements for Medicaid.

In states electing not to establish and operate a marketplace, PPACA required the federal government to establish and operate a marketplace in that state, referred to as a federally facilitated marketplace. Thus, the federal government's role with respect to a marketplace for any given state—in particular whether it established a marketplace or oversees a state-based marketplace—was dependent on a state decision. For plan year 2016,[7] 13 states had a state-based marketplace, 4 had a state-based marketplace using the federal marketplace platform, 27 had a federally facilitated marketplace, and 7 had a state partnership marketplace.[8] Figure 1 shows the states and the types of marketplaces they use.

[7]Open enrollment period for plan year 2016 was the third enrollment period for the state marketplaces, which began on November 1, 2015, and ended on January 31, 2016.

[8]HHS specified options for states to partner with HHS when HHS establishes and operates a marketplace. Under this model, states may assist HHS in carrying out certain functions, such as plan management and consumer assistance. In addition, a state that operates its own marketplace can request that CMS perform eligibility and enrollment functions using federal IT systems. We refer to this as a state-based marketplace using the federal platform.

Figure 1: Type of Health Insurance Marketplace Used by States for Plan Year 2016

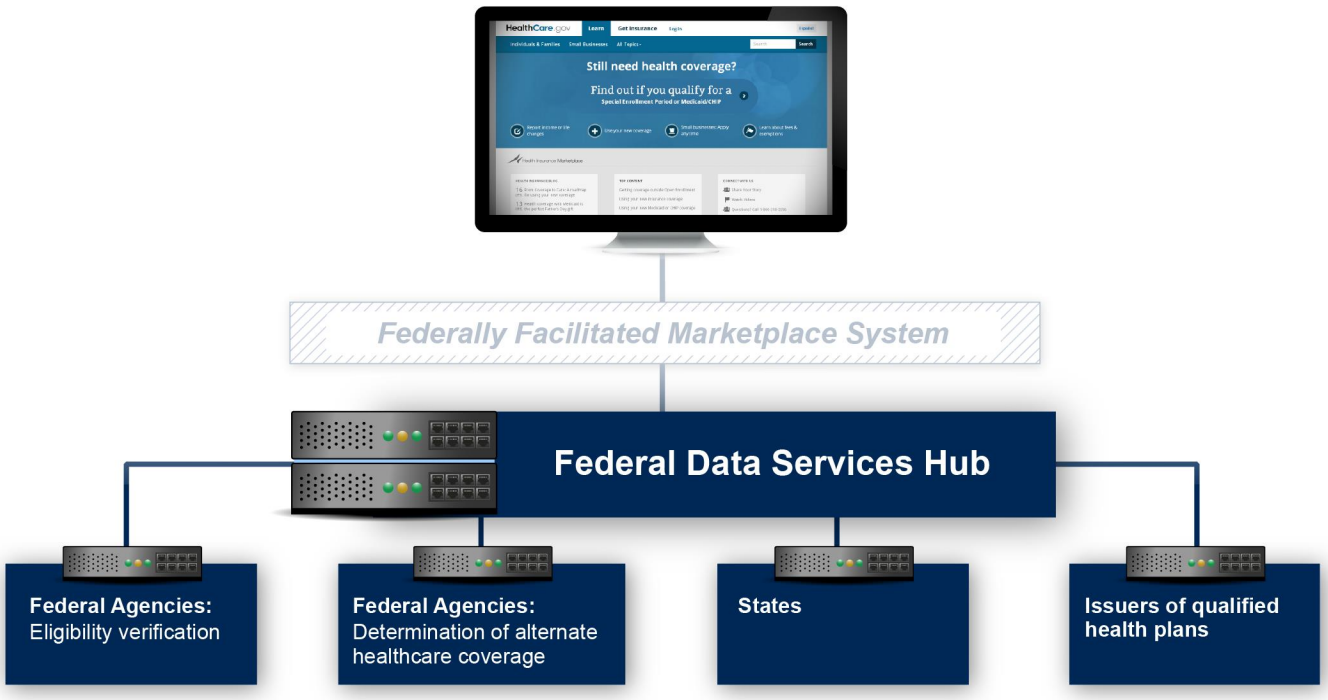


Sources: GAO analysis of Centers for Medicare & Medicaid Services data; Map Resources (map). | GAO-16-265

CMS and State-Based Marketplaces Exchange Data with Many Interconnected Systems and External Partners to Facilitate Enrollment

PPACA requires that CMS and the states establish automated systems to facilitate the enrollment of eligible individuals in appropriate health care coverage. Many systems and entities exchange information to carry out this requirement. The CMS Center for Consumer Information and Insurance Oversight (CCIIO) has overall responsibility for the federal systems supporting Healthcare.gov and for overseeing state-based marketplaces, which vary in the extent to which they exchange information with CMS. Other entities also connect to the network of systems that support enrollment in Healthcare.gov. Figure 2 shows the major entities that exchange data in support of marketplace enrollment and how they are connected.

Figure 2: Overview of Healthcare.gov and Its Supporting Systems



Source: GAO analysis of Centers for Medicare & Medicaid Services data. | GAO-16-265

Regardless of whether a state established and operated its own marketplace or used the federally facilitated marketplace, PPACA and HHS regulations and guidance require every marketplace to have capabilities that enable them to carry out four key functions, among others:

- **Eligibility and enrollment.** The marketplace must enable individuals to assess and determine their eligibility for enrollment in health care coverage. In addition, the marketplace must provide individuals the ability to obtain an eligibility determination for other federal health care coverage programs, such as Medicaid and CHIP. Once eligibility is determined, individuals must be able to apply for and enroll in applicable coverage options.

- **Plan management.** The marketplace is to provide a suite of services for state agencies and health plan issuers to facilitate activities such as submitting, monitoring, and renewing qualified health plans.

- **Financial management.** The marketplace is to facilitate payments of advanced premium tax credits to health plan issuers and also provide additional services such as payment calculation for risk adjustment analysis and cost-sharing reductions for individual enrollments.

- **Consumer assistance.** The marketplace must be designed to provide support to consumers in completing an application, obtaining eligibility determinations, comparing coverage options, and enrolling in health care coverage.

Federal Data Services Hub

The data hub is a CMS system that acts as a single portal for exchanging information between the federally facilitated marketplace and CMS's external partners, including other federal agencies, state-based marketplaces, other state agencies, other CMS systems, and issuers of qualified health plans. The data hub was designed as a "private cloud" service[9] supporting the following primary functions:

- **Real-time eligibility queries.** The federally facilitated marketplace, state-based marketplaces, and Medicaid/CHIP agencies transmit queries to various external entities, including other federal agencies, state agencies, and commercial verification services, to verify information provided by applicants, such as immigration and citizenship data, income data, individual coverage data, and incarceration data.

[9]Although exact definitions vary, cloud computing can, at a high level, be described as a form of computing where users have access to scalable, on-demand IT capabilities that are provided through Internet-based technologies. A private cloud is operated solely for a single organization and the technologies may be on or off the premises.

- **Transfer of application and taxpayer information.** The federally facilitated marketplace or a state-based marketplace transfers application information to state Medicaid/CHIP agencies. Conversely, state agencies also use the data hub to transfer application information to the federally facilitated marketplace. In addition, the Internal Revenue Service (IRS) transmits taxpayer information to the federally facilitated marketplace or a state-based marketplace to support the verification of household income and family size when determining eligibility for advance payments of the premium tax credit and cost-sharing reductions.[10]

- **Exchange and monitoring of enrollment information with issuers of qualified health plans.** The federally facilitated marketplace sends enrollment information to appropriate issuers of qualified health plans, which respond with confirmation messages back to CMS when they have effectuated enrollment. State-based marketplaces also send enrollment confirmations, which CMS uses to administer the advance premium tax credit and cost-sharing reductions and to track overall marketplace enrollment. Further, CMS, issuers of qualified health plans, and state-based marketplaces exchange enrollment information on a monthly basis to reconcile enrollment records.

- **Submission of health plan applications.** Issuers of qualified health plans submit "bids" for health plan offerings for validation by CMS.

Connections between external entities and the data hub are made through an Internet protocol that establishes an encrypted system-to-system web browser connection. Encryption of the data transfer between the two entities is designed to meet NIST standards, including Federal

[10]PPACA offers insurance affordability programs including the advance premium tax credit and cost-sharing reductions. The advance premium tax credit is available on an advance basis, and advance payments of the premium tax credit are reconciled on a tax filer's tax return. The credit is generally available to eligible tax filers and their dependents that are (1) enrolled in a qualified health plan through a marketplace, (2) meet income requirements and (3) not eligible for other health insurance coverage that meets certain standards. Cost sharing generally refers to costs that an individual must pay when using services that are covered under the health plan that the person is enrolled in. Common forms of cost sharing include copayments and deductibles.

Information Processing Standard 140-2.[11] This type of connection is intended to ensure that only authorized systems can access the data being exchanged, thus safeguarding against cyber attacks attempting to intercept the data.

The data hub is designed to not retain any of the data that it transmits in permanent storage devices, such as hard disks. According to CMS officials, data are stored only momentarily in the data hub's active memory. The entities that transmit the data are responsible for maintaining copies of their transmissions in case the data need to be re-transmitted. As a result, CMS does not consider the data hub to be a repository of personally identifiable information.[12]

State-Based Marketplaces

State-based marketplaces generally perform the same functions that the federally facilitated marketplace performs for states that do not maintain their own marketplace. However, in certain cases, known as state partnership marketplaces, states may elect to perform one or both of the plan management and consumer assistance functions while the federally facilitated marketplace performs the rest. The specific functions performed by each partner vary from state to state. Figure 3 shows what functions are performed by each type of marketplace.

[11]Agencies are required to encrypt agency data, where appropriate, using NIST-certified cryptographic modules. FIPS 140-2 specifies the security requirements for a cryptographic module used within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md.: May 2001).

[12]In terms of the Privacy Act of 1974, CMS has determined that the data hub is not a system of records subject to the act's provisions.

Figure 3: Functions Performed by the Various Types of Marketplaces

Source: GAO analysis of Centers for Medicare & Medicaid Services data. | GAO-16-265

Regardless of whether a state operates its own marketplace, most states need to connect their state Medicaid and CHIP agencies to either their state-based marketplace or the federally facilitated marketplace to exchange data about enrollment in these programs. Such data exchanges are generally routed through the CMS data hub. In addition, states may need to connect with the IRS (also through the data hub) in order to verify an applicant's income and family size for the purpose of determining eligibility for or the amount of the advance payment of the

premium tax credit and cost-sharing reductions. Finally, state-based marketplaces are to send enrollment confirmations to the federally facilitated marketplace so that CMS can administer advance payments of the premium tax credit and cost-sharing payments and track overall marketplace enrollment.

Laws and Regulations Set Requirements for Ensuring the Security and Privacy of Personally Identifiable Information

Federal laws and guidance specify requirements for protecting federal systems and data. This includes systems used or operated by a contractor or other organization on behalf of a federal agency. The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support operations and assets of the agency, including those provided or managed by another agency, contractor, or another organization on behalf of an agency.[13]

FISMA assigns certain responsibilities to NIST, which is tasked with developing, for systems other than national security systems, standards and guidelines that must include, at a minimum, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

Accordingly, NIST has developed a risk management framework of standards and guidelines for agencies to follow in developing information security programs. Relevant publications include:

- Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*,[14]

[13]The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014 and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[14]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values from among the security categories that the agency identifies for each type of information resident on those information systems.

- Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*,[15] specifies minimum security requirements for federal agency information and information systems and a risk-based process for selecting the security controls necessary to satisfy these minimum security requirements.

- Federal Information Processing Standard 140-2, *Security Requirements for Cryptographic Modules*,[16] requires agencies to encrypt agency data, where appropriate, using NIST-certified cryptographic modules. This standard specifies the security requirements for a cryptographic module used within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments.

- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*,[17] provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The guidance includes privacy controls to be used in conjunction with the specified security controls to achieve comprehensive security and privacy protection.

[15]NIST, *Minimum Security Requirements for Federal Information and Information Systems,* FIPS Publication 200 (Gaithersburg, Md.: March 2006).

[16]NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md.: May 2001).

[17]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4 (Gaithersburg, Md.: April 2013).

- NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*,[18] explains how to apply a risk management framework to federal information systems, including security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

- NIST Special Publication 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (draft)*,[19] recommends steps to help develop a more defensible and survivable IT infrastructure—including the component products, systems, and services that compose the infrastructure. While agencies are not yet required to follow these draft guidelines, they establish a benchmark for effectively coordinating security efforts across complex interconnected systems, such as those that support Healthcare.gov and state-based marketplaces.

While agencies are required to use a risk-based approach to ensure that all of their IT systems and information are appropriately secured, they also must adopt specific measures to protect personally identifiable information (PII)[20] and must establish programs to protect the privacy of individuals whose PII they collect and maintain. Agencies that collect or maintain health information also must comply with additional

[18]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37 Revision 1 (Gaithersburg, Md.: February 2010).

[19]NIST, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*, SP 800-160, draft (Gaithersburg, Md.: May 2014).

[20]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

requirements. In addition to FISMA, major laws and regulations[21] establishing requirements for information security and privacy in the federal government include the following:

- **The Privacy Act of 1974**[22] places limitations on agencies' collection, access, use, and disclosure of personal information maintained in systems of records. The act defines a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another individual identifier. It defines a "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or other individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system of records notice in the *Federal Register* that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and contest its content.[23]

- **The E-Government Act of 2002**[24] strives to enhance protection for personal information in government information systems by requiring that agencies conduct, where applicable, a privacy impact assessment for each system. This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to Office of Management and Budget (OMB)

[21]Regulations also establish security and privacy requirements that are applicable to the marketplaces or Healthcare.gov-related contracts. For example, in March 2012, CMS issued a final rule regarding implementation of the exchanges (marketplaces) under PPACA and it promulgated a regulation regarding privacy and security standards that marketplaces must establish and follow. See 77 Fed. Reg. 18310, 18444 (March 27, 2012), 45 C.F.R. § 155.260. To ensure that federal contractor-operated systems meet federal information security and privacy requirements, the Federal Acquisition Regulation requires that agency acquisition planning for IT comply with the information technology security requirements in FISMA and addresses application of the Privacy Act to contractors. 48 C.F.R. § 7.103(w), and Subpart 24.1.

[22]5 U.S.C. 552a.

[23]Under the Privacy Act, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[24]Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (Dec. 17, 2002).

guidance,[25] a privacy impact assessment is an analysis of how information is handled to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. Agencies must conduct a privacy impact assessment before developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form or before initiating any new data collections involving identifiable information that will be collected, maintained, or disseminated using IT if the same questions or reporting requirements are imposed on 10 or more people.

- **The Health Insurance Portability and Accountability Act of 1996**[26] establishes national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers, and provides for the establishment of privacy and security standards for handling health information. The act calls for the Secretary of HHS to adopt standards for the electronic exchange, privacy, and security of health information, which were codified in the Security and Privacy Rules.[27] The Security Rule specifies a series of administrative, technical, and physical security practices for "covered entities"[28] and their business associates to implement to ensure the confidentiality of electronic health information. The Privacy Rule reflects basic privacy principles for ensuring the protection of personal health information,

[25]OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

[26]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9). Additional privacy and security protections, and amendments to the HIPAA Privacy and Security Rules, were established by the Health Information Technology for Economic and Clinical Health Act, Pub. 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).

[27]The Health Insurance Portability and Accountability Act of 1996 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).

[28]"Covered 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.

such as limiting uses and disclosures to intended purposes, notification of privacy practices, allowing individuals to access their protected health information, securing information from improper use or disclosure, and allowing individuals to request changes to inaccurate or incomplete information. The Privacy Rule establishes a category of health information, called "protected health information," which may be used or disclosed to other parties by "covered entities" 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 protected health information to accomplish the intended purpose.

HHS Has Established Responsibilities for Ensuring the Security and Privacy of Health Insurance Marketplaces

CMS's CCIIO has overall responsibility for developing and implementing policies and rules governing state-based marketplaces, overseeing the implementation and operations of state-based marketplaces, and administering federally facilitated marketplaces for states that elect not to establish their own.

State-based marketplaces and the federal government must share data and otherwise integrate IT systems for the implementation and operation of the marketplaces. According to federal regulations, state-based marketplaces are responsible for protecting and ensuring the confidentiality, integrity, and availability of marketplace enrollment information, and must also establish and implement certain privacy and security standards. CMS oversees state-based marketplaces and compliance with those standards. Additionally, federal statutes, guidance, and standards require the federal government to protect its IT systems and the information contained within these systems.

As part of its oversight responsibilities, CMS developed a suite of documents—known as the Minimum Acceptable Risk Standards for Exchanges (MARS-E)—that addresses security and privacy standards for the state-based marketplaces. The documents define a risk-based security and privacy framework for state-based marketplaces and their contractors to use in the design and implementation of their IT systems and provide guidance regarding the minimum level of security controls that must be implemented to protect information and information systems. The MARS-E is designed to facilitate marketplaces' compliance with FISMA, the Health Insurance Portability and Accountability Act of 1996, and the Privacy Act of 1974, among other relevant laws.

Prior GAO Reports Highlighted Concerns Regarding the Implementation of the Health Insurance Marketplaces

Over the past 2 years, we have issued a number of reports highlighting challenges that CMS has faced in implementing and operating the health insurance marketplaces' IT systems. In September 2014, we reported that while CMS had taken steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, weaknesses remained in both the processes used for managing information security and privacy as well as the technical implementation of IT security controls.[29] Specifically, we noted that Healthcare.gov and the related systems had been deployed despite incomplete security plans and privacy documentation, incomplete security tests, and the lack of an alternate processing site to avoid major service disruptions.

We recommended that CMS implement 6 management controls and 22 information security controls to help ensure that the systems and information related to Healthcare.gov are protected. The management recommendations were aimed at ensuring system security plans were complete, privacy risks were analyzed and documented, computer matching agreements were developed with the Office of Personnel Management and the Peace Corps, a comprehensive security assessment of the federally facilitated marketplace was performed, the planned alternate processing site made operational in a timely fashion, and detailed security roles and responsibilities for contractors were established. HHS concurred fully or partially concurred with our information security program-related recommendations and all 22 of the recommendations to improve the effectiveness of its information security controls. As of December 2015, CMS had taken steps to address all 6 information security program-related recommendations and was in the process of addressing the security control-related recommendations.

In March 2015, we reported that several problems with the initial development and deployment of Healthcare.gov and its supporting systems had led to consumers encountering widespread performance issues when trying to create accounts and enroll in health plans.[30] We

[29]GAO, *Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls,* GAO-14-730 (Washington, D.C.: Sept. 16, 2014).

[30]GAO, *Healthcare.gov: CMS Has Taken Steps to Address Problems, but Needs to Further Implement Systems Development Best Practices*, GAO-15-238 (Washington, D.C.: Mar. 4, 2015).

noted, for example, that CMS had not adequately conducted capacity planning, adequately corrected software coding errors, or implemented all planned functionality. In addition, the agency did not consistently apply recognized best practices for system development, which contributed to the problems with the initial launch of Healthcare.gov and its supporting systems. In this regard, weaknesses existed in the application of requirements, testing, and oversight practices. Further, we noted that HHS had not provided adequate oversight of the Healthcare.gov initiative through its Office of the Chief Information Officer.

We made recommendations aimed at improving requirements management, system testing processes, and oversight of development activities for systems supporting Healthcare.gov. HHS concurred with all of our recommendations and subsequently took or planned steps to address the weaknesses, including instituting a process to ensure functional and technical requirements are approved, developing and implementing a unified standard set of approved system testing documents and policies, and providing oversight for Healthcare.gov and its supporting systems through the department-wide investment review board.

In September 2015, we reported that CMS established a framework for oversight of IT projects within state-based marketplaces, but the oversight was not always effectively executed.[31] For example, CMS tasked various offices with responsibilities for overseeing states' marketplace IT projects, but the agency did not always clearly document, define, or communicate its oversight roles and responsibilities to states as called for by best practices for project management. In addition, CMS did not involve all relevant senior executives in decisions to approve federal funding for states' IT marketplace projects. Lastly, CMS established a process that required the testing of state marketplace systems to determine whether they were ready to be made operational, but the systems were not always fully tested, increasing the risk that they would not operate as intended.

We recommended that CMS define and communicate its oversight roles and responsibilities, ensure senior executives are involved in funding decisions for state IT projects, and ensure that states complete testing of

[31]GAO, *State Health Insurance Marketplaces: CMS Should Improve Oversight of State Information Technology Projects*, GAO-15-527 (Washington, D.C.: Sept. 16, 2015).

their systems before they are put into operation. HHS concurred with all of our recommendations and stated it had taken various actions that were focused on improving its oversight and accountability for states' marketplace efforts.

Most recently, in February 2016, we reported that CMS should take actions to strengthen enrollment controls and manage fraud risk. We noted, for example, CMS does not, according to agency officials, track or analyze aggregate outcomes of data hub eligibility and enrollment queries—either the extent to which a responding agency delivers information responsive to a request, or whether an agency reports that information was not available. In addition, CMS did not have an effective process for resolving inconsistencies for individual applicants for the federal Health Insurance Marketplace. Lastly, CMS approved subsidized coverage for 11 of 12 fictitious GAO phone or online applicants for 2014 and the applicants obtained a total of about $30,000 in annual advance premium tax credits, plus eligibility for lower costs at time of service.

We made 8 recommendations aimed at strengthening enrollment controls and managing fraud risk, including that CMS consider analyzing outcomes of the verification system, take steps to resolve inconsistencies, and conduct a risk assessment of the potential for fraud in Marketplace applications. HHS concurred with all of GAO's recommendations.

Healthcare.gov and Key Supporting Systems Have Experienced Information Security Incidents

NIST defines an information security incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. A security incident can occur under many circumstances and for many reasons. It can be inadvertent, such as from the loss of an electronic device, or deliberate, such as from the theft of a device, or a cyber-based attack by a malicious individual or group, agency insider, foreign nation, terrorist, or other adversary. Protecting federal systems and the information on them is essential because the loss or unauthorized disclosure or alteration of the information can lead to serious consequences and can result in substantial harm to individuals and the federal government.

FISMA requires the establishment of a federal information security incident center to, among other things, provide timely technical assistance to agencies regarding cyber incidents. The United States Computer Emergency Readiness Team (US-CERT), established in 2003, is the federal information security incident center that fulfills the FISMA mandate. US-CERT consults with agencies on cyber incidents, provides technical information about threats and incidents, compiles the

information, and publishes it on its website, https://www.us-cert.gov/. US-CERT also issues guidelines for agencies to use when reporting incidents. For the time period under our review, US-CERT defined seven categories of incidents for federal agencies to use in reporting incidents, and CMS added two categories of its own, which are described below in table 1.

Table 1: United States Computer Emergency Readiness Team (US-CERT) and Centers for Medicare & Medicaid Services (CMS) Information Security Incident Categories

Category	Name	Description
CAT 0	Exercise/Network Defense Testing	Used during state, federal, national, and international exercises and approved activity testing of internal/external network defenses or responses.
CAT 1	Unauthorized Access	An individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
CAT 2	Denial of Service	An attack that successfully prevents or impairs the normal authorized functionality of a network, system, or application by exhausting resources. Includes being the victim or participating in the denial of service.
CAT 3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.
CAT 4	Inappropriate Usage	A person violates acceptable computing use policies.
CAT 5	Probes and Reconnaissance Scans	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	Unconfirmed incident that is potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
CAT 7[a]	Other	Cases where the incident may fall outside the other defined categories.
CAT 8[a]	Lost, Stolen, Damaged Equipment	Incidents involving lost equipment such as mobile devices, laptops, and thumb drives.

Sources: US-CERT and CMS documentation. | GAO-16-265

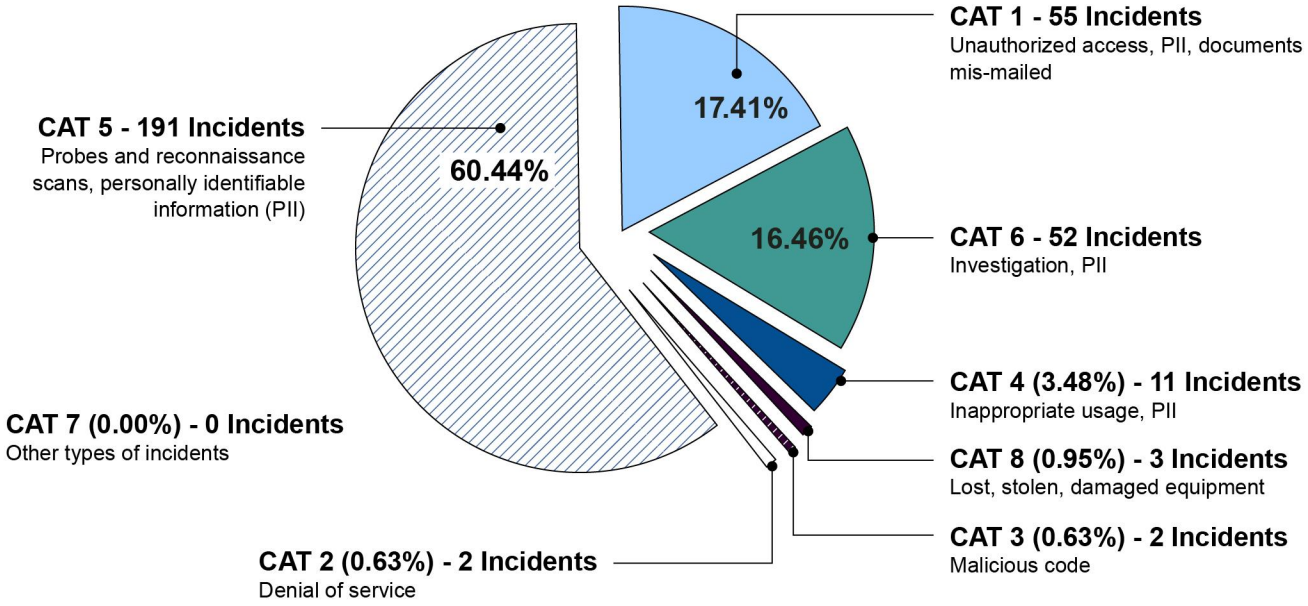
[a]This is a CMS-defined category not found in US-CERT guidance.

Between October 6, 2013, and March 8, 2015, CMS reported 316 incidents[32] affecting Healthcare.gov or key supporting systems.[33] These included—among others—incidents which involved PII and attempts by attackers to compromise part of the Healthcare.gov system. None of the incidents described in the data included any evidence that an attacker had compromised sensitive data, including PII, from Healthcare.gov. Figure 4 shows the 316 reported incidents grouped according to the US-CERT and CMS-defined incident categories.

[32]CMS defines a security incident as a reportable event that meets one or more of the following criteria: (1) the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system processing information on behalf of CMS. It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put CMS data at risk of unauthorized access, use, disclosure, modification, or destruction; (2) an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; and (3) a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

[33]Healthcare.gov and key supporting systems include the Healthcare.gov website, the Enterprise Identity Management System, the Federally Facilitated Marketplace System, and the Federal Data Services Hub.

Figure 4: Healthcare.gov and Key Supporting Systems Reported Security Incidents by United States Computer Emergency Readiness Team and Centers for Medicare & Medicaid Services Incident Categories

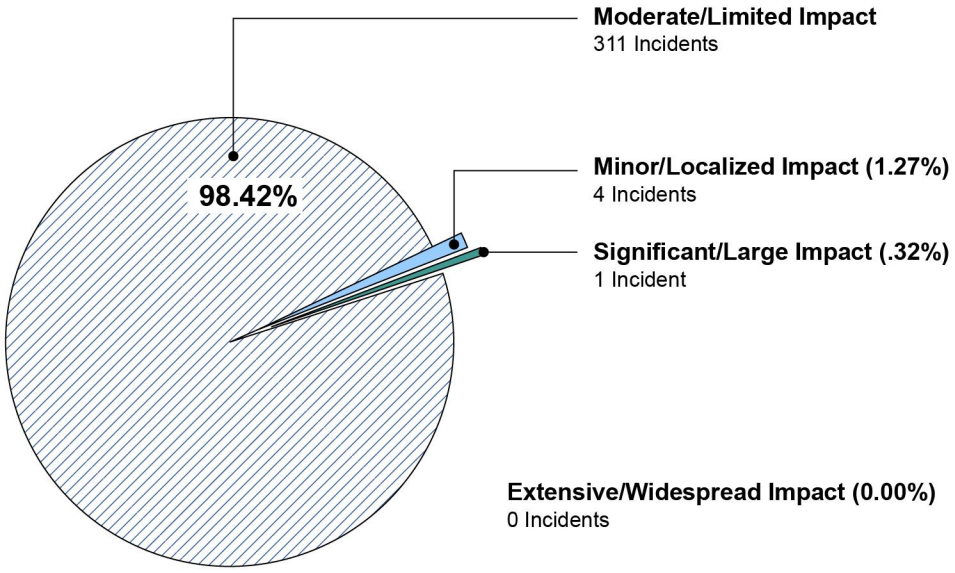


Source: GAO Analysis of Centers for Medicare & Medicaid Services data. | GAO-16-265

CAT 1 unauthorized access incidents made up 17 percent of the incidents logged during the time period under review. Of those, only one incident—which CMS publicly disclosed last year—involved a confirmed instance of an attacker gaining access to a Healthcare.gov-related server. In that incident, the attacker installed malware on a test server that held no PII. The rest of the CAT 1 incidents involved occurrences such as PII being disclosed because of physical mail being sent to an incorrect recipient or unencrypted PII being transmitted via e-mail to a limited number of individuals.

CMS also assessed incidents' impact, categorizing incidents as having an impact of "Extensive/Widespread," "Significant/Large," "Moderate/Limited," or "Minor/Localized." More than 98 percent of the reported incidents were assessed as "Moderate/Limited" impact, and the remainder, less than 2 percent, as "Minor/Localized" impact. See figure 5 for a breakdown of incidents by CMS-assigned level of impact.

Figure 5: Healthcare.gov and Key Supporting Systems Reported Security Incidents by Level of Impact



Source: GAO Analysis of Centers for Medicare & Medicaid Services data. | GAO-16-265

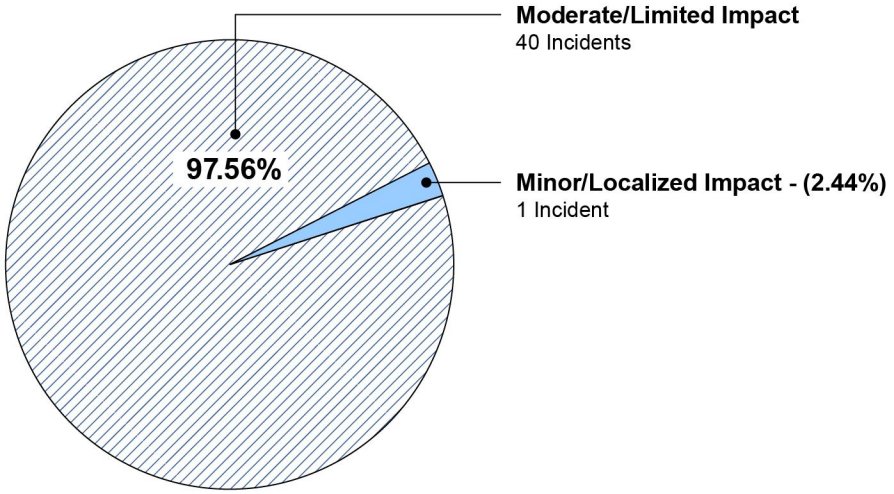
CMS did not classify any of the incidents we reviewed as having "Extensive/Widespread" impact, and classified only one incident as having "Significant/Large" impact. In that incident, a list of CMS employee account IDs, including passwords that had not yet been assigned to employees and phone numbers, was transmitted to CMS staff via an unencrypted e-mail message. In order to mitigate the incident, CMS created new passwords for the affected employees and advised the employees to log on and change their passwords.

A privacy incident generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive information, including PII.[34] According to CMS, 41 of the 316 incidents were reported to involve PII either not being secured properly or being exposed to an unauthorized individual, as

[34]CMS defines a privacy incident as a security incident that involves PII or protected health information where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII or protected health information in usable form, whether physical or electronic.

opposed to other security issues affecting Healthcare.gov and key supporting systems. Of the 41 PII incidents in the CMS data, the agency classified 40 as being of "Moderate/Limited" impact, and one as being of "Minor/Localized" impact. The number of individuals affected by these incidents was not fully documented. While CMS, as of October 2014, began including an estimate of the number of affected individuals in incident reports, several of the reports we reviewed were from earlier incidents and did not contain estimates of the number of affected individuals. See figure 6 for a breakdown of the privacy incidents by CMS-assigned level of impact.

Figure 6: Healthcare.gov and Key Supporting System Reported Privacy Incidents by Level of Impact



Source: GAO Analysis of Centers for Medicare & Medicaid Services data. | GAO-16-265

As noted above, none of these incidents were the result of an attacker compromising data, but were rather the result of errors such as information being sent to the incorrect recipient, PII being transmitted in an unencrypted format, or system configuration errors causing PII to be recorded to system logs or displayed in places it should not have been.

Information Security Weaknesses Associated with the Federal Data Services Hub Place Healthcare.gov Data at Risk

A basic management objective for any organization is to protect the confidentiality, integrity, and availability of the information and systems that support its critical operations and assets. Organizations accomplish this by designing and implementing access and other controls that are intended to protect information and systems from unauthorized disclosure, modification, and loss. Specific controls include, among other things, those related to identification and authentication of users, authorization restrictions, and configuration management. As required by FISMA, NIST has issued guidance for agencies on how to select and implement controls over their information systems. Additionally, in June 2015, OMB directed agencies to take steps to strengthen their controls in the areas of scanning and monitoring for attackers, patching vulnerabilities in a timely manner, limiting the use of administrative accounts, and requiring the use of two-factor authentication,[35] especially for administrators.[36]

As we previously reported, CMS took steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, including the data hub.[37] The steps included developing required security program policies and procedures, establishing interconnection security agreements with its federal and commercial partners, and instituting required privacy protections. For example, it assigned overall responsibility for securing the agency's information and systems to appropriate officials, including the agency Chief Information Officer and Chief Information Security Officer, and designated information system security officers to assist in certifying information systems of particular CMS components. Additionally, CMS documented information security policies and procedures to safeguard

[35]Authentication systems typically rely on one or more of the following factors: something you know (for example, a password); something you have (for example, an ID badge or a cryptographic key); and something you are (for example, a fingerprint or other biometric data). Two-factor authentication refers to the use of more than one of these factors. The strength of authentication systems is largely determined by the number of factors it uses. Implementations that use two factors are considered to be stronger than those that use only one factor, while systems that incorporate all three factors are stronger than systems that incorporate only two.

[36]OMB, *Fact Sheet: Enhancing and Strengthening the Federal Government's Cybersecurity*, (Washington, D.C.: June 12, 2015).

[37]GAO-14-730.

the agency's information and systems and to reduce the risk of and minimize the effects of security incidents.

While CMS has taken steps to secure the data hub, we identified weaknesses in the technical controls protecting the data flowing through the system. Specifically, CMS did not effectively implement or securely configure key security tools and devices to sufficiently protect the users and information on the data hub system from threats to confidentiality, integrity, and availability. For example:

- CMS did not appropriately restrict the use of administrative privileges for data hub systems. NIST Special Publication 800-53 recommends that agencies follow the concept of "least privilege," giving users and administrators only the privileges and access necessary to perform their assigned duties. OMB has also instructed agencies to tighten policies and procedures for privileged users, including limiting the functions privileged users can perform with their administrative accounts. However, CMS did not consistently restrict administrator accounts to perform only the functions necessary to perform their assigned duties. CMS officials stated they are working to further restrict administrative privileges and are reviewing accounts to ensure permissions and roles are appropriate. By not enforcing least privilege, CMS faces an increased risk that a malicious insider or an attacker using a compromised administrator account could access sensitive data flowing through the data hub.

- CMS did not consistently implement patches for several data hub systems. NIST Special Publication 800-53 recommends that organizations test and install newly released security patches, service packs, and hot fixes, and OMB has instructed agencies to patch critical vulnerabilities without delay. However, CMS did not consistently apply patches to critical systems or applications supporting the data hub in a timely manner. CMS officials stated they are reviewing the patch histories on all servers and are directing staff to bring them up-to-date or provide a business rationale for not applying specific patches. By not keeping current with security patches, CMS faces an increased risk that servers supporting the data hub could be compromised through exploitation of known vulnerabilities.

- CMS did not securely configure the data hub's administrative network. NIST Special Publication 800-53 recommends how such a network should be configured. CMS officials stated that they are reviewing the network's configurations to identify a plan for remediation. Without

adhering to NIST recommendations, CMS may face an increased risk of unauthorized access to the data hub network.

In addition to the above weaknesses, we identified other security weaknesses in controls related to boundary protection, identification and authentication, authorization, encryption, audit and monitoring, and software updates that limit the effectiveness of the security controls on the data hub and unnecessarily place sensitive information at risk of unauthorized disclosure, modification, or exfiltration. According to CMS officials, in response to the identified weaknesses, they have formed a task force, comprised of the Deputy Chief Information Security Officer, system maintainers and administrators, database administrators, and security personnel, to work with the stakeholders responsible for the data hub applications and the underlying platform and infrastructure. The same officials stated that meetings will be held on at least a weekly basis to monitor milestone dates, discuss activities, and identify potential barriers to resolution of any given weakness. The control weaknesses we identified during this review are described in greater detail in a separate report with limited distribution.

CMS Has Not Fully Implemented Security and Privacy Oversight of State-Based Marketplaces, Three of Which Had Significant Weaknesses

CMS has taken various actions to oversee the security and privacy controls implemented at the state-based marketplaces, including assigning roles and responsibilities for oversight entities, conducting regular meetings with state officials to discuss pending issues, and establishing a new reporting tool to monitor marketplace performance. However, CMS has not fully documented procedures that define its oversight responsibilities. Further, while CMS has set requirements for annual testing of a subset of security controls implemented within the state-based marketplaces, it does not require continuous monitoring or annual comprehensive testing. Until CMS documents its oversight procedures and requires continuous monitoring of security controls, it does not have reasonable assurance that the states are promptly identifying and remediating weaknesses and therefore faces a higher risk that attackers could compromise the confidentiality, integrity, and availability of the data contained in state-based marketplaces. The need for better assurance that controls are working was highlighted by the results of the reviews we conducted of security and privacy controls at three state-based marketplaces. For those three marketplaces, we identified significant weaknesses that placed the data they contained at risk of compromise.

CMS Has Established Policies to Oversee the Effectiveness of Security and Privacy Controls but Has Not Defined Specific Procedures, Time Frames, or Follow-up Actions

Effective organizational policies and procedures define key management activities in detail, establish time frames for their completion, and specify follow-up actions that must be taken to correct deficiencies. According to GAO's *Standards for Internal Control in the Federal Government*,[38] an organization's policies should identify internal control responsibilities and each unit's responsibility for designing and implementing those controls. Moreover, each policy should specify the appropriate level of detail to allow management to effectively monitor the control activities and define day-to-day procedures, which may include the timing of when an activity is to occur and any follow-up corrective actions to be performed if deficiencies are identified.

While CMS has developed policies for overseeing security and privacy controls at the state-based marketplaces, it has not defined specific oversight procedures, the timing for when each activity should occur, or what follow-up corrective actions should be performed if deficiencies are identified.

CMS has assigned roles and responsibilities for oversight entities, conducted regular meetings with state officials to discuss pending issues, and established a new reporting tool to monitor marketplace performance. For example, as we reported in September 2015,[39] CMS outlined oversight roles and responsibilities. Three key offices—CCIIO, Office of Technology Solutions (OTS), and Center for Medicaid and CHIP Services (CMCS)—were identified as having responsibility for overseeing states' efforts in establishing the marketplaces. Their primary roles and duties included the following:

- CCIIO led the marketplace implementation, and within that office, State Officers were assigned to be accountable for day-to-day communications with state marketplace officials.
- OTS was responsible for systems integration and software development efforts to ensure that the functions of the marketplaces were carried out. A primary participant within OTS was the IT project

[38]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[39]GAO-15-527.

manager, who was the individual responsible for monitoring, among other things, state-based marketplaces' IT development activities.

- CMCS was the office responsible for coordinating and approving implementation of Medicaid activities related to the health insurance marketplaces. The office carried out these responsibilities in conjunction with CCIIO.

While CMS outlined general oversight roles, it did not define or document the specific day-to-day activities of these offices and staff that are responsible for the oversight. For example, according to CCIIO officials, the state officers conduct oversight through weekly meetings with state-based marketplace officials. The same officials stated that the meetings do not have a defined agenda or procedures, but that identified control weaknesses or other security issues are discussed. Further, there are no documented procedures that outline the specific responsibilities of the IT project manager, who was the individual responsible for monitoring state-based marketplaces' IT development activities.

In 2015, CMS began using a new reporting tool to monitor state performance. The State Based Marketplace Annual Reporting Tool (SMART) is intended to collect information to be used as the basis for evaluating a state-based marketplace's compliance with regulations and CMS standards. Information collected through SMART includes performance metrics, summaries from independent programmatic audits, and an attestation to the submission of the most recent required security and privacy documentation.[40] The first submissions from the states were due on April 1, 2015. According to CMS officials, they received the submissions and, as of December 2015, were still reviewing them.

While SMART is intended to collect information on compliance with regulations and CMS standards, including security and privacy controls, CMS has not defined specific follow-up procedures or time frames, including identifying corrective actions to be performed if deficiencies are identified. CMS officials stated SMART is a reporting mechanism used to provide a comprehensive picture of state-based marketplaces and that

[40]The required security and privacy documentation includes: a system security plan, interconnection security agreement, computer matching agreement, information exchange agreement, privacy impact assessment, security assessment report, plan of action & milestones, annual security attestation, and change reports.

CMS does not use it to identify corrective actions to be performed if deficiencies are identified. However, until CMS defines and documents its specific day-to-day procedures, the timing of when control activities are to occur, and what follow-up corrective actions are to be performed if deficiencies are identified, the agency does not have reasonable assurance that it is providing effective oversight of security and privacy at state-based marketplaces.

CMS Requires Testing of State-Based Marketplaces Only Every Three Years

FISMA requires that an agency develop, document, and implement an agency-wide information security program. The program should provide security for the information and information systems that support the operations of the agency, including those provided or managed by a contractor or other source. As part of the information security program, the agency should require periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. FISMA requires this testing to be comprehensive, including testing of management, operational, and technical controls of every information system identified in the inventory.

Further, in November 2013 OMB issued guidance to federal agencies on managing information security risk on a continuous basis, which includes the requirement to continually monitor the security controls in information systems and the environments in which they operate.[41] OMB noted that managing information risk on a continuous basis allows agencies to maintain awareness of information security vulnerabilities and threats to support risk management decisions and improve the effectiveness of safeguards and countermeasures. Rather than enforcing a static, point-in-time reauthorization process, agencies were encouraged by OMB to conduct ongoing authorizations of their information systems and the environments in which they operated, including common controls, through the implementation of their risk management programs.

Although CMS has set requirements for periodic testing of the security controls at the state-based marketplaces, it requires neither continuous monitoring nor comprehensive annual testing. Any state seeking to gain an “authority to connect” to the data hub is required to submit

[41]OMB, *Enhancing the Security of Federal Information and Information Systems*, M-14-03 (Washington, D.C.: Nov. 18, 2013).

documentation that it has properly secured its planned connection.[42] The standard "authority to connect" to the data hub is issued for a 3-year period. Following the approval of the initial "authority to connect," every state is required to conduct reviews of the documentation on a yearly basis, submit quarterly plan of action and milestone reports, and re-sign the interconnection security agreement every 3 years or whenever a significant change has occurred to the interconnected systems. As part of the signed agreement, each state must specify the security controls it has implemented and attest that the state IT system is designed, managed, and operated in compliance with CMS standards. According to the MARS-E, all security controls are required to be assessed over a 3-year period and to meet this requirement a subset is to be tested each year so that all security controls are tested during a 3-year period. However, according to CMS officials, during the time of our review, the states were not required to submit evidence that they had tested subsets of controls each year.

CMS officials stated that they monitor the effectiveness of security controls on an ongoing basis by reviewing documents that contain information on reported weaknesses. The same officials stated that they perform quarterly reviews of state marketplaces' plan of action and milestone reports, and changes to the system boundaries, hardware, software, and data centers. These officials added that if serious deficiencies are noted in their review, such as a large number of open high or moderate findings, or findings that have been open for a long time, they have the ability to terminate a state's connection to the data hub if the deficiencies are not remediated or sufficient progress is not made in a timely manner. However, according to CMS officials, they have not yet terminated any state's connection to the data hub because states have remediated deficiencies to their satisfaction in a timely manner.

[42]The documentation required by CMS included: (1) a system security plan describing the design of the system and the process for identifying and mitigating security risks, (2) a report documenting an assessment of the security risks for the system conducted either internally or through a third party, (3) a plan of action and milestones and corrective action plan for mitigating any risks identified by the security risk assessment, (4) a signed information exchange agreement documenting roles and responsibilities for protecting data, and (5) an interconnection security agreement specifying the interconnection arrangements and responsibilities for all parties, the security controls implemented by the state, the technical and operational security requirements that the state follows, and attesting that the state IT system is designed, managed, and operated in compliance with the CMS standards.

Numerous significant security weaknesses have been identified in state-based marketplaces. For example, in the second quarter of fiscal year 2015, the 14 states[43] that maintained their own state-based marketplaces reported a total of 27 high open findings, 288 moderate open findings, and 259 low open findings from their own internal assessments. One state reported 20 of the 27 high open findings during that time period.

According to CMS officials, while they do not require comprehensive annual testing or continuous monitoring of security controls, they perform annual reviews of the system security plans for the state-based marketplaces and require the states to submit new security assessments anytime they make significant changes to the systems. CMS officials also stated that they monitor various state-generated documents on a weekly, monthly, or yearly basis depending on when the reports are being required. States are advised to include any new assessment, audit, or weakness discovered during normal day-to-day operations in those documents. However, for the plan of action and milestones reports and state-based marketplaces we reviewed, the CMS oversight process has not resulted in timely identification and mitigation of security weaknesses. Without more frequently monitoring of the full set of security controls in the state-based marketplaces and the environments in which they operate, CMS does not have reasonable assurance that the states are promptly identifying and remediating weaknesses and therefore faces a higher risk that attackers could compromise the confidentiality, integrity, and availability of the data contained in state-based marketplaces.

Security and Privacy Weaknesses Place Selected State-Based Marketplaces' Data at Risk

The need for better assurance that security and privacy controls are working properly was highlighted by the results of our reviews of technical controls at three state-based marketplaces, which identified significant weaknesses in those systems. In September 2015, we reported on our reviews of three state-based marketplaces that assessed the effectiveness of key program elements and controls implemented to protect the information they contain.[44] We identified weaknesses in key

[43]For plan year 2015, Hawaii operated and maintained a state-based marketplace. However in plan year 2016, Hawaii now operates a state-based marketplace using the federal platform.

[44]We selected the three states by concentrating on states who received a high amount of PPACA grant funding through 2014, while ensuring a mix of both population size (i.e., large, medium, and small) and contractors used to ensure we reviewed a variety of approaches to system development and operation.

elements of each state's information security and privacy controls, such as security management, privacy policies and procedures, security awareness training, background checks, contingency planning, incident response, and configuration management. Further, we identified security weaknesses in technical controls related to access controls, cryptography, and configuration management that limit the effectiveness of the security controls on the systems. For example:

- One state did not encrypt connections to the authentication servers supporting its system. The MARS-E requires passwords to be encrypted when they are being transmitted across the network. However, the authentication servers we reviewed were configured to accept unencrypted connections. As a result, an attacker on the network could observe the unencrypted transmission to gather usernames and password hashes, which could then be used to compromise those accounts.

- One state did not filter uniform resource locator (URL) requests from the Internet through a web application firewall to prevent hostile requests from reaching the marketplace website. NIST Special Publication 800-53 requires the enforcement of access controls through the use of firewalls. However, the state did not fully configure its filtering to block hostile URL requests from the Internet. As a result, hostile URL requests could potentially scan and exploit vulnerabilities of the portal and potentially gain access to remaining systems and databases of the marketplace.

- One state did not enforce the use of high-level encryption on its Windows servers. NIST Special Publication 800-53 and MARS-E require that if an agency uses encryption, it must use, at a minimum, a Federal Information Processing Standards 140-2–compliant cryptographic module. However, the state did not configure its Windows Active Directory and Domain Name System servers to require the use of Federal Information Processing Standards–compliant algorithms. As a result, the servers may employ weak encryption for protecting authentication and communication, increasing the risk that an attacker could compromise the confidentiality or integrity of the system.

For each of the security and privacy weaknesses we identified, we also identified potential activities to mitigate those weaknesses. In total, we identified 24 potential mitigation activities to address weaknesses in the three states' security and privacy programs and 66 potential mitigation activities to improve the effectiveness of their information security

controls. The results of our work were reported separately in "limited official use only" correspondences.[45] The three states generally agreed with the potential mitigation activities and have plans to address them.

Conclusions

Healthcare.gov and its key supporting systems have experienced information security incidents which involved both PII not being secured properly and attempts by attackers to compromise the Healthcare.gov system. However, for the incidents we reviewed, we did not find evidence that an outside attacker with malicious intent had compromised sensitive data.

Although CMS continues to make progress in correcting or mitigating previously reported weaknesses within Healthcare.gov and its key supporting systems, the information security weaknesses found in the data hub will likely continue to jeopardize the confidentiality, integrity, and availability of Healthcare.gov. The information that is transferred through the data hub will likely remain vulnerable until the agency addresses weaknesses pertaining to boundary protection, identification and authentication, authorization, encryption, audit and monitoring, software updates, and configuration management.

While CMS has taken steps to ensure that the information processed and maintained by stated-based marketplaces is protected from unauthorized access or misuse, it lacks a documented oversight program to ensure that each state is implementing security and privacy controls properly. Given the significant number of control weaknesses found during our review of selected states, CMS not requiring continuous monitoring of security controls at the state level may pose unnecessary and increased security risks to the data hub and other Healthcare.gov systems.

Recommendations for Executive Action

To improve the oversight of privacy and security controls over the state-based marketplaces, we recommend that the Secretary of Health and Human Services direct the Administrator of the Centers for Medicare & Medicaid Services to take the following three actions:

[45]GAO, *Information Security: GAO Review of State-Based Marketplace Security and Privacy – 1*, GAO15-804RSU (Washington, D.C.: Sept. 22, 2015); *Information Security: GAO Review of State-Based Marketplace Security and Privacy – 2*, GAO15-805RSU (Washington, D.C.: Sept. 22, 2015); and *Information Security: GAO Review of State-Based Marketplace Security and Privacy – 3*, GAO15-806RSU (Washington, D.C.: Sept. 22, 2015).

- define procedures for overseeing state-based marketplaces, to include day-to-day activities of the relevant offices and staff;
- develop and document procedures for reviewing the SMART tool, including specific follow-up timelines and identifying corrective actions to be performed if deficiencies are identified; and
- require continuous monitoring of the privacy and security controls over state-based marketplaces and the environments in which those systems operate to more quickly identify and remediate vulnerabilities.

In a separate report with limited distribution, we are also making 27 recommendations to resolve technical information security weaknesses within the data hub related to boundary protection, identification and authentication, authorization, encryption, audit and monitoring, and software updates.

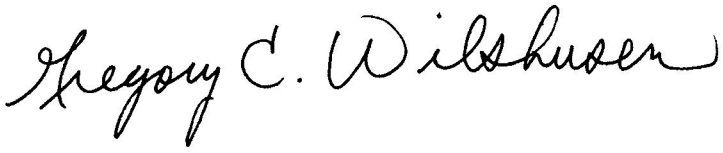
Agency Comments and Our Evaluation

We sent draft copies of this report to the Department of Health and Human Services (HHS) and received written comments in return. These comments are reprinted in appendix II. HHS concurred with all of GAO's recommendations. Further, it also provided information regarding specific actions the agency has taken or plans on taking to address these recommendations. We also received technical comments from HHS, which have been incorporated into the final report as appropriate.

In its written comments, HHS noted that the department and its federal partners comply with relevant laws and use processes, controls, and standards to secure consumer data maintained within Healthcare.gov and its supporting systems. Further, it described the process it uses to mitigate information security risks associated with the data hub, manage security incidents, and oversee the security and privacy of data transmitted by the state-based marketplaces.

We are sending copies of this report to the Department of Health and Human Services. In addition, the report is 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 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov and barkakatin@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

Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering

List of Congressional Requesters

The Honorable Orrin Hatch
Chairman
The Honorable Ron Wyden
Ranking Member
Committee on Finance
United States Senate

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

The Honorable Ron Johnson
Chairman
The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate

The Honorable Claire McCaskill
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Jason Chaffetz
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Kevin Brady
Chairman
The Honorable Sander M. Levin
Ranking Member
Committee on Ways and Means
House of Representatives

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

The Honorable Joseph R. Pitts
Chairman
Subcommittee on Health
Committee on Energy and Commerce
House of Representatives

The Honorable Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Mark Meadows
Chairman
Subcommittee on Government Operations
Committee on Oversight and Government Reform
House of Representatives

The Honorable Jim Jordan
Chairman
Subcommittee on Health Care, Benefits, and Administrative Rules
Committee on Oversight and Government Reform
House of Representatives

The Honorable William Hurd
Chairman
Subcommittee on Information Technology
Committee on Oversight and Government Reform
House of Representatives

The Honorable Mike Coffman
Chairman
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
House of Representatives

Honorable Charles Boustany, Jr.
Chairman
Subcommittee on Tax Policy
Committee on Ways and Means
House of Representatives

The Honorable Peter Roskam
Chairman
The Honorable John Lewis
Ranking Member
Subcommittee on Oversight
Committee on Ways and Means
House of Representatives

The Honorable Michael Bennet
United States Senate

The Honorable Richard Blumenthal
United States Senate

The Honorable Robert P. Casey, Jr.
United States Senate

The Honorable Al Franken
United States Senate

The Honorable Tim Kaine
United States Senate

The Honorable Amy Klobuchar
United States Senate

The Honorable Joe Manchin III
United States Senate

The Honorable Jeffrey A. Merkley
United States Senate

The Honorable Bill Nelson
United States Senate

The Honorable Jeanne Shaheen
United States Senate

The Honorable Jon Tester
United States Senate

The Honorable John Thune
United States Senate

The Honorable Mark R. Warner
United States Senate

The Honorable Ron Barber
House of Representatives

The Honorable Tulsi Gabbard
House of Representatives

The Honorable Duncan Hunter
House of Representatives

The Honorable Darrell Issa
House of Representatives

The Honorable Mike Kelly
House of Representatives

The Honorable Ann McLane Kuster
House of Representatives

The Honorable Daniel W. Lipinski
House of Representatives

The Honorable Patrick E. Murphy
House of Representatives

The Honorable Scott Peters
House of Representatives

The Honorable Kyrsten Sinema
House of Representatives

The Honorable Filemon Vela
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the extent to which security and privacy incidents were reported for Healthcare.gov or key supporting systems; (2) assess the effectiveness of the controls implemented by the Centers for Medicare & Medicaid Services (CMS) to protect the Federal Data Services Hub (data hub) and the information it transmits; (3) assess the effectiveness of CMS's oversight of key program elements and controls implemented by state-based marketplaces and the effectiveness of those elements at selected state-based marketplaces to protect the information they contain.

To address our first objective, we reviewed and analyzed data on information security and privacy incidents reported by CMS that occurred between October 6, 2013, and March 8, 2015, affecting Healthcare.gov and its supporting systems. Specifically, we reviewed a list of reported incidents and the information associated with each incident, such as the incident reports and actions taken to mitigate the incidents. We also reviewed the reported impact of each incident. In order to ensure the reliability of the data, we reviewed related documentation, interviewed knowledgeable agency officials, and performed manual data testing for obvious errors. We then analyzed the information to identify statistics on the reported incidents. Lastly, we interviewed knowledgeable officials and reviewed CMS policies and procedures for incident handling.

To address our second objective, we reviewed relevant information security laws and National Institute of Standards and Technology (NIST) standards and guidance to identify federal security and privacy control requirements. Further, we analyzed the overall network control environment, identified interconnectivity and control points, and reviewed controls for the network and servers supporting the data hub. Specifically, we reviewed controls over the data hub and its supporting software, the operating systems, network, and computing infrastructure provided by the supporting platform-as-a-service.

In order to evaluate CMS's controls over its information systems supporting Healthcare.gov, we used our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; Office of Management and Budget (OMB) guidance; NIST standards and guidelines; and CMS policies, procedures, practices, and standards.

Specifically, we

- reviewed network access paths to determine if boundaries had been adequately protected;
- analyzed system access controls to determine whether users had more permissions than necessary to perform their assigned functions;
- observed configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- reviewed software security settings to determine if modifications of sensitive or critical system resources had been monitored and logged; and
- inspected the operating system and application software on key servers and workstations to determine if critical patches had been installed and/or were up-to-date.

We performed our work at CMS contractor facilities in Columbia, Maryland, and Chantilly, Virginia.

To address our third objective, we selected three states by concentrating on states who received a high amount of federal grant funding through 2014, while ensuring a mix of both population size (I.e., large, medium, and small) and contractors used to ensure we reviewed a variety of approaches to system development and operation. To assess the effectiveness of the three selected states' key program elements and management controls, we compared their documented policies, procedures, and practices to the provisions and requirements contained in CMS security and privacy standards for state-based marketplaces. We also reviewed the results of testing of security controls; analyzed system and security documentation, including information exchange agreements; and interviewed state officials.

To determine the effectiveness of the information security controls the three states implemented for information systems supporting their marketplaces, we reviewed risk assessments, security plans, system control assessments, contingency plans, and remedial action plans. To evaluate the technical controls for the marketplaces, we analyzed the overall network control environment, identified control points, and reviewed controls for the supporting network and servers. We compared the aforementioned items to our *Federal Information System Controls Audit Manual*; NIST standards and guidelines; CMS security and privacy guidance for state-based marketplaces; and Center for Internet Security guidance.

To determine the effectiveness of CMS oversight of the states' program elements and controls, we reviewed CMS policies and procedures regarding oversight of the state-based marketplaces and compared them to Federal Information Security Modernization Act of 2014[1] requirements, OMB guidance on security controls testing, and *GAO's Standards for Internal Control in the Federal Government*. We also obtained and reviewed oversight-related information that CMS provided to the three selected states. Lastly, we interviewed officials from the relevant CMS offices that had oversight responsibilities.

We conducted this performance audit from December 2014 to March 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.

[1]The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014 and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

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

MAR 0 9 2016

Gregory C. Wilshusen
Director, 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, *"Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls" (GAO-16-264SU and GAO-16-265).*

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

Sincerely,

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: HEALTHCARE.GOV: ACTIONS NEEDED TO ENHANCE INFORMATION SECURITY AND PRIVACY CONTROLS (GAO-16-265)

The Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report on the security and privacy of the HealthCare.gov systems and State-based Marketplaces (SBM). As the GAO reported, they did not find evidence that an outside attacker had successfully compromised sensitive data, such as personally identifiable information (PII).

The security and privacy of consumer data is a top priority for HHS and other federal and state agencies. HHS and our federal partners comply with relevant laws and use processes, controls, and standards to secure consumer data. As the GAO reported, consistent with federal guidance, HHS has taken steps to protect the security and privacy of data processed and maintained by the systems and connections supporting HealthCare.gov, including the Federal Data Services Hub (Hub). Consumers entrust HHS and states to protect their data, and HHS is committed to continuously improving privacy and security in the HealthCare.gov systems, including the Hub, and in overseeing privacy and security controls for SBMs.

HealthCare.gov uses recent technological advancements, including the Hub, to verify application information efficiently and without undue burden on individuals or families. As part of that effort, HHS created a multi-layered approach to verifying eligibility that protects the integrity of HealthCare.gov. The Hub provides a secure electronic connection between the Marketplaces and existing federal, state, and private databases. These databases verify the eligibility information in each application by matching it against trusted records, maintained by the Social Security Administration (SSA), the Internal Revenue Service (IRS), the Department of Homeland Security (DHS), Equifax, the Department of Veterans Affairs, Medicare, and TRICARE. Additionally, the Peace Corps and the Office of Personnel Management (OPM) use a secure electronic file transfer process to conduct regular transmissions of Peace Corps and OPM data to verify application information about employer-sponsored coverage. The Hub supported tens of millions of data verifications during the first three open enrollment periods.

HHS has taken significant steps and implemented robust security controls to protect the security and privacy of the systems and connections supporting HealthCare.gov, including the Hub. HHS developed these systems consistent with federal statutes, guidelines, and industry standards that help safeguard the security, privacy, and integrity of the systems and the data that flow through them. HealthCare.gov and the Hub have been determined to be compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institute of Standards and Technology (NIST). Marketplace systems are also in compliance with all the relevant privacy and security statutes, including the Privacy Act of 1974.

The Hub and its associated systems have several layers of protection in place to mitigate information security risk, including penetration testing, which happens on an ongoing basis using industry best practices to appropriately safeguard consumers' personal information. As part of the ongoing testing process, and in line with federal and industry standards, any open risk findings are appropriately addressed with risk mitigation strategies and compensating controls. The security of the system is also monitored by sensors and other tools to deter and prevent unauthorized access. HHS conducts continuous monitoring using a 24/7, multi-layer IT professional security team, added penetration

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: HEALTHCARE.GOV: ACTIONS NEEDED TO ENHANCE INFORMATION SECURITY AND PRIVACY CONTROLS (GAO-16-265)

testing, and a change management process that includes ongoing testing and mitigation strategies implemented in real time.

If HHS identifies a potential security incident, it has procedures and processes in place to quickly report the incident and mitigate any issues, in accordance with FISMA requirements and guidelines issued by the United States Computer Emergency Readiness Team (US-CERT). A dedicated operations center handles all HealthCare.gov and Hub incident response actions and has 24/7 monitoring and response capabilities. All potential incidents are investigated within 24 hours of being reported. Most potential incidents reported pose limited threat to the security and privacy of consumer data. As the GAO noted, more than 98 percent of the reported incidents affecting HealthCare.gov were assessed as "Moderate/Limited" impact. None of the incidents included evidence that an attacker had compromised sensitive data, including PII. As part of its continuous monitoring, HHS investigates all incidents to confirm containment, eradication, and remediation are achieved.

In addition to HHS' responsibilities to protect consumer data on the HealthCare.gov systems, HHS also is responsible for overseeing the security and privacy of data transmitted via the Hub by SBMs. The Affordable Care Act provides states with significant flexibility in the design and operation of their Marketplaces to best meet the unique needs of their citizens and their health insurance issuers. As part of HHS' oversight of SBMs, HHS established strong security controls and standards for each SBM to meet in order to connect to the Hub. These controls and standards are based on federal security and privacy guidelines, including FISMA and the Privacy Act.

Prior to connecting to the Hub, each state had to sign a Computer Matching Agreement, an Interconnection Security Agreement and an Information Exchange Agreement, all of which bind the state to rules and operating procedures related to data security and privacy. Each state is required to complete additional documentation, including a privacy impact assessment, a system security plan, an internal or third party risk assessment, and an action plan to address weaknesses and risks. Every state that connects to the Hub adheres to these procedures. To maintain a connection to the Hub, states are required to submit quarterly action plans and conduct an annual security self-assessment of one-third of their security controls. States must also have an independent, third-party security audit of all of their security controls every three years or have one-third of their security controls reviewed via an independent, third-party security audit each year.

HHS assesses states' progress on all new or urgent security findings regularly and receives quarterly updates on all open findings through an action plan. When HHS receives updates, we work with the states to evaluate the findings and determine remediation plans. In the limited cases where HHS may determine a security finding could pose a risk to the Hub, HHS requires the state to comply with additional security requirements, including significantly reducing or mitigating the findings. Failure to comply with the terms required by HHS may result in a state's disconnection from the Hub.

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: HEALTHCARE.GOV: ACTIONS NEEDED TO ENHANCE INFORMATION SECURITY AND PRIVACY CONTROLS (GAO-16-265)

HHS acknowledges that risks exist inherently for every IT system and that as technology progresses, additional safeguards will be needed. Through the enforcement of documented policies and procedures, as well as dedicated information security staff, HHS protects the security and privacy of the systems and interconnections that support HealthCare.gov, including the Hub. Through the enforcement of requirements, such as annual testing and continuous monitoring, HHS provides oversight of SBM privacy and security. HHS is committed to continued oversight and support of states' protection of consumer data. HHS appreciates the GAO's suggestion of controls and processes that could be improved to further reduce or mitigate risk.

GAO Recommendation
Define procedures for overseeing State-based Marketplaces, to include day-to-day activities of the relevant offices and staff.

HHS Response
HHS concurs with this recommendation. HHS already has oversight and monitoring guidance that it regularly shares with states. To enhance HHS' privacy and security oversight and monitoring, HHS will create an overarching oversight process, including identifying appropriate roles and responsibilities for HHS staff.

GAO Recommendation
Develop and document procedures for reviewing the State-based Marketplace Annual Reporting Tool (SMART), including specific follow-up timelines and identifying corrective actions to be performed if deficiencies are identified.

HHS Response
HHS concurs with this recommendation. HHS already has a process in place outside of SMART for states to submit the required documentation relating to privacy and security of their Marketplaces. As part of this outside process, states are required to submit the most recent system security plan, interconnection security agreement, computer matching agreement, information exchange agreement, privacy impact assessment, security assessment report, action plan, and annual security attestation. Upon submission of these documents, HHS works with the states to evaluate risks and determine remediation plans. HHS will update SMART procedures to clarify this distinct process.

GAO Recommendation
Require continuous monitoring of the privacy and security controls over State-based Marketplaces and the environments in which those systems operate to more quickly identify and remediate vulnerabilities.

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: HEALTHCARE.GOV: ACTIONS NEEDED TO ENHANCE INFORMATION SECURITY AND PRIVACY CONTROLS (GAO-16-265)

HHS Response

HHS concurs with this recommendation. HHS requires continuous monitoring as detailed in its Minimum Acceptable Risk Standards for Exchanges (MARS-E). As part of this requirement, states must develop and implement a continuous monitoring program that includes establishing metrics, monitoring and reporting on security controls on an ongoing basis, and developing response actions to address results of analyses. As part of this process, states conduct an annual security self-assessment of one-third of their security controls. States must also have an independent third-party security audit of all of their security controls every three years or have one-third of their security controls reviewed via an independent, third-party security audit each year. States are required to report on continuous monitoring through updates to their action plans, annual security attestations, security impact analyses, and other reporting documents. HHS will, as part of developing an overarching oversight process, include specific oversight procedures to verify states are performing continuous monitoring and reporting the outcomes to HHS. HHS is committed to continued support of states as they work to strengthen their Marketplaces, including enhancements, maintenance, and operations of their IT systems.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov

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

Staff Acknowledgments

In addition to the contacts named above, John de Ferrari, Edward Alexander Jr., Lon Chin, West Coile and Duc Ngo (assistant directors); Christopher Businsky; Mark Canter; Marisol Cruz; Lee McCracken; Monica Perez-Nelson; Justin Palk; Michael Stevens; and Brian Vasquez made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

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

Page 1

DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation

Washington, DC 20201

MAR 09 2016

Gregory C. Wilshusen

Director, 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, "Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls" (GA0-16-264SU and GA0-16-265).

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

Sincerely,

Jim R. Esquea

Assistant Secretary for Legislation

Attachment

Page 2

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: HEALTHCARE.GOV: ACTIONS NEEDED TO ENHANCE INFORMATION SECURITY AND PRIVACY CONTROLS (GA0-16-265)

The Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report on the security and privacy of the HealthCare.gov systems and State-based Marketplaces (SBM). As the GAO reported, they did not find evidence that an outside attacker had successfully compromised sensitive data, such as personally identifiable information (PII).

The security and privacy of consumer data is a top priority for HHS and other federal and state agencies. HHS and our federal partners comply with relevant laws and use processes, controls, and standards to secure consumer data. As the GAO reported, consistent with federal guidance, HHS has taken steps to protect the security and privacy of data processed and maintained by the systems and connections supporting HealthCare.gov, including the Federal Data Services Hub (Hub). Consumers entrust HHS and states to protect their data, and HHS is committed to continuously improving privacy and security in the HealthCare.gov systems, including the Hub, and in overseeing privacy and security controls for SBMs.

HealthCare.gov uses recent technological advancements, including the Hub, to verify application information efficiently and without undue burden on individuals or families. As part of that effort, HHS created a multi-layered approach to verifying eligibility that protects the integrity of HealthCare.gov. The Hub provides a secure electronic connection between the Marketplaces and existing federal, state, and private databases. These databases verify the eligibility information in each application by matching it against trusted records, maintained by the Social Security Administration (SSA), the Internal Revenue Service (IRS), the Department of Homeland Security (DHS), Equifax, the Department of Veterans Affairs, Medicare, and TRICARE. Additionally, the Peace Corps

and the Office of Personnel Management (OPM) use a secure electronic file transfer process to conduct regular transmissions of Peace Corps and OPM data to verify application information about employer-sponsored coverage. The Hub supported tens of millions of data verifications during the first three open enrollment periods.

HHS has taken significant steps and implemented robust security controls to protect the security and privacy of the systems and connections supporting HealthCare.gov, including the Hub. HHS developed these systems consistent with federal statutes, guidelines, and industry standards that help safeguard the security, privacy, and integrity of the systems and the data that flow through them. HealthCare.gov and the Hub have been determined to be compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institute of Standards and Technology (NIST). Marketplace systems are also in compliance with all the relevant privacy and security statutes, including the Privacy Act of 1974.

The Hub and its associated systems have several layers of protection in place to mitigate information security risk, including penetration testing, which happens on an ongoing basis using industry best practices to appropriately safeguard consumers' personal information. As part of the ongoing testing process, and in line with federal and industry standards, any open risk findings are appropriately addressed with risk mitigation strategies and compensating controls. The security of the system is also monitored by sensors and other tools to deter and prevent unauthorized access. HHS conducts continuous monitoring using a 24/7, multi-layer IT professional security team, added penetration

Page 3

testing, and a change management process that includes ongoing testing and mitigation strategies implemented in real time.

If HHS identifies a potential security incident, it has procedures and processes in place to quickly report the incident and mitigate any issues, in accordance with FISMA requirements and guidelines issued by the United States Computer Emergency Readiness Team (US-CERT). A dedicated operations center handles all HealthCare.gov and Hub incident response actions and has 24/7 monitoring and response capabilities. All potential incidents are investigated within 24 hours of being reported. Most potential incidents reported pose limited threat to the security and privacy of consumer data. As the GAO noted, more than 98 percent of the reported incidents affecting HealthCare.gov were assessed as "Moderate/Limited" impact. None of the incidents included evidence that

an attacker had compromised sensitive data, including PII. As part of its continuous monitoring, HHS investigates all incidents to confirm containment, eradication, and remediation are achieved.

In addition to HHS' responsibilities to protect consumer data on the HealthCare.gov systems, HHS also is responsible for overseeing the security and privacy of data transmitted via the Hub by SBMs. The Affordable Care Act provides states with significant flexibility in the design and operation of their Marketplaces to best meet the unique needs of their citizens and their health insurance issuers. As part of HHS' oversight of SBMs, HHS established strong security controls and standards for each SBM to meet in order to connect to the Hub. These controls and standards are based on federal security and privacy guidelines, including FISMA and the Privacy Act.

Prior to connecting to the Hub, each state had to sign a Computer Matching Agreement, an Interconnection Security Agreement and an Information Exchange Agreement, all of which bind the state to rules and operating procedures related to data security and privacy. Each state is required to complete additional documentation, including a privacy impact assessment, a system security plan, an internal or third party risk assessment, and an action plan to address weaknesses and risks. Every state that connects to the Hub adheres to these procedures. To maintain a connection to the Hub, states are required to submit quarterly action plans and conduct an annual security self-assessment of one-third of their security controls. States must also have an independent, third-party security audit of all of their security controls every three years or have one-third of their security controls reviewed via an independent, third-party security audit each year.

HHS assesses states' progress on all new or urgent security findings regularly and receives quarterly updates on all open findings through an action plan. When HHS receives updates, we work with the states to evaluate the findings and determine remediation plans. In the limited cases where HHS may determine a security finding could pose a risk to the Hub, HHS requires the state to comply with additional security requirements, including significantly reducing or mitigating the findings. Failure to comply with the terms required by HHS may result in a state's disconnection from the Hub.

Page 4

HHS acknowledges that risks exist inherently for every IT system and that as technology progresses, additional safeguards will be needed. Through the enforcement of documented policies and procedures, as well as

dedicated information security staff, HHS protects the security and privacy of the systems and interconnections that support HealthCare.gov, including the Hub. Through the enforcement of requirements, such as annual testing and continuous monitoring, HHS provides oversight of SBM privacy and security. HHS is committed to continued oversight and support of states' protection of consumer data. HHS appreciates the GAO's suggestion of controls and processes that could be improved to further reduce or mitigate risk.

GAO Recommendation

Define procedures for overseeing State-based Marketplaces, to include day-to-day activities of the relevant offices and staff.

HHS Response

HHS concurs with this recommendation. HHS already has oversight and monitoring guidance that it regularly shares with states. To enhance HHS' privacy and security oversight and monitoring, HHS will create an overarching oversight process, including identifying appropriate roles and responsibilities for HHS staff.

GAO Recommendation

Develop and document procedures for reviewing the State-based Marketplace Annual Reporting Tool (SMART), including specific follow-up timelines and identifying corrective actions to be performed if deficiencies are identified.

HHS Response

HHS concurs with this recommendation. HHS already has a process in place outside of SMART for states to submit the required documentation relating to privacy and security of their Marketplaces. As part of this outside process, states are required to submit the most recent system security plan, interconnection security agreement, computer matching agreement, information exchange agreement, privacy impact assessment, security assessment report, action plan, and annual security attestation. Upon submission of these documents, HHS works with the states to evaluate risks and determine remediation plans. HHS will update SMART procedures to clarify this distinct process.

GAO Recommendation

Require continuous monitoring of the privacy and security controls over State-based Marketplaces and the environments in which those systems operate to more quickly identify and remediate vulnerabilities.

Page 5

HHS Response

HHS concurs with this recommendation. HHS requires continuous monitoring as detailed in its Minimum Acceptable Risk Standards for Exchanges (MARS-E). As part of this requirement, states must develop and implement a continuous monitoring program that includes establishing metrics, monitoring and reporting on security controls on an ongoing basis, and developing response actions to address results of analyses. As part of this process, states conduct an annual security self-assessment of one-third of their security controls. States must also have an independent third-party security audit of all of their security controls every three years or have one-third of their security controls reviewed via an independent, third-party security audit each year. States are required to report on continuous monitoring through updates to their action plans, annual security attestations, security impact analyses, and other reporting documents. HHS will, as part of developing an overarching oversight process, include specific oversight procedures to verify states are performing continuous monitoring and reporting the outcomes to HHS. HHS is committed to continued support of states as they work to strengthen their Marketplaces, including enhancements, maintenance, and operations of their IT systems.

Data Tables

Accessible Text for Figure 2: Overview of Healthcare.gov and Its Supporting Systems

1. Federally Facilitated Marketplace System
2. Federal Data Services Hub
    a. Federal Agencies: Eligibility verification
    b. Federal Agencies: Determination of alternate healthcare coverage
    c. States
    d. Issuers of qualified health plans

Source: GAO analysis of Centers for Medicare & Medicaid Services data. | GAO-16-265

Data Table for Figure 4: Healthcare.gov and Key Supporting Systems Reported Security Incidents by United States Computer Emergency Readiness Team and Centers for Medicare & Medicaid Services Incident Categories

Category	Incidents
CAT 5	191
CAT 1	55
CAT 6	52
CAT 4	11
CAT 8	3
CAT 3	2
CAT 2	2
CAT 7	0

Data Table for Figure 5: Healthcare.gov and Key Supporting Systems Reported Security Incidents by Level of Impact

Level of Impact	Incidents
Moderate/Limited	311
Minor/Localized	4
Significant/Large	1
Extensive/Widespread	0

Data Table for Figure 6: Healthcare.gov and Key Supporting System Reported Privacy Incidents by Level of Impact

Level of Impact	Incidents
Moderate/Limited	40
Minor/Localized	1