United States Government Accountability Office

Report to Congressional Requesters

March 2018

# ELECTRONIC HEALTH INFORMATION

# CMS Oversight of Medicare Beneficiary Data Security Needs Improvement

Accessible Version

GAO-18-210

March 2018

# ELECTRONIC HEALTH INFORMATION

## CMS Oversight of Medicare Beneficiary Data Security Needs Improvement

GAO Highlights

Highlights of GAO-18-210, a report to congressional requesters

## Why GAO Did This Study

Recent data breaches have highlighted the importance of ensuring the security of health information, including Medicare beneficiary data. Such data are created, stored, and used by a wide variety of entities, such as health care providers, insurance companies, financial institutions, researchers, and others.

GAO was asked to conduct a study of CMS efforts to protect Medicare beneficiary data accessed by external entities. GAO's objectives were to (1) identify the major external entities that collect, store, and process Medicare fee-for-service beneficiary data; (2) determine whether requirements for the protection of Medicare beneficiary data align with federal guidance; and (3) assess CMS oversight of the implementation of those requirements. GAO analyzed information about how external entities access data, reviewed CMS documentation on who they share data with, compared federal standards with CMS security requirements for external entities, and analyzed results of independent security reviews. GAO also interviewed CMS officials about their oversight activities.

## What GAO Recommends

GAO recommends that CMS develop additional guidance for researchers on implementing security controls required by CMS, consistently track results of independent assessments, and provide oversight of researchers and qualified entities. CMS concurred with GAO's three recommendations and described actions it has planned or taken to address them.

View GAO-18-210. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

## What GAO Found

The Centers for Medicare and Medicaid Services (CMS) shares Medicare beneficiary data with three major types of external entities: (1) Medicare Administrative Contractors (MAC) that perform processing and distribution functions that support the payment of Medicare benefits; (2) research organizations (researchers) that use Medicare beneficiary data to study how health care services are provided to beneficiaries; and (3) qualified public or private entities that use claims data to evaluate the performance of Medicare service providers and equipment suppliers.

CMS has developed requirements for implementing security controls that align with federal guidance for two of the three types of external entities that access Medicare beneficiary data. While CMS has developed guidance for MACs and qualified entities, it has not developed equivalent guidance for researchers. Researchers must adhere to broad governmentwide standards, but are not given guidance on which specific controls to implement. According to CMS, the lack of specific guidance gives the researchers more flexibility to independently assess their security risks and determine which controls are appropriate to implement; however, without providing comprehensive, risk-based security guidance to researchers, CMS increases the risk that external entities possessing agency data may not have applied security controls that meet CMS standards.

Additionally, CMS has established an oversight program for the security of MAC data, but has not established a corresponding program to oversee security implementation by researchers and qualified entities. Without effective oversight measures in place for researchers and qualified entities, CMS cannot fully ensure that the security of Medicare beneficiary data is being adequately protected. Regarding MACs, although they are subject to two types of independent annual assessments, which have regularly identified weaknesses in their implementation of security controls, the weaknesses that have been assessed as low-risk have not been consistently tracked in the CMS finding tracking system. Without more consistent tracking of these low-risk weaknesses, it may be difficult for CMS to determine if all weaknesses are being addressed in a timely manner. Examples of categories of recurring weaknesses that have been identified during annual assessments are listed in the table.

**Table: Key Recurring Categories of Weaknesses Identified in Annual Assessments of Medicare Administrative Contractors**

| Category | Significance |
|---|---|
| Configuration management | Ensures that software updates are timely, appropriate, and do not introduce new security weaknesses. |
| System security plans | Allows assessors to review a system's security strategy and determine whether security has been implemented as intended. |
| System inventories | Ensures that organizations have a complete and up-to-date inventory of hardware and software components as a basis for effective configuration management. |

Source: GAO analysis of annual MAC assessments.

# Contents


Letter 1

Background 3
CMS Shares Medicare Fee-for-Service Beneficiary Data with Three Major Types of External Entities 8
CMS Established Information Security Requirements that Align with Federal Guidance for Some, but Not All, External Entities 18
CMS Has Not Consistently Overseen the Implementation of Security Controls by External Entities 22
Conclusion 30
Recommendations 30
Agency Comments and our Evaluation 31

Appendix I: Objectives, Scope, and Methodology 32

Appendix II: Analysis of CMS Acceptable Risk Safeguards 34

Appendix III: Comments from the Department of Health and Human Services 36

Text of Appendix III: Comments from the Department of Health and Human Services 39

Appendix IV: GAO Contact and Staff Acknowledgments 43


Tables


Table 1: National Institute of Standards and Technology Cybersecurity Framework Functions and Categories 7
Table 2: Shared Systems Used by the MACs to Process Medicare Fee-for-Service Claims 12
Table 3: Key Recurring Categories of Weaknesses Identified in Annual Assessments of MACs 27
Table 4: Extent to Which CMS Addressed NIST Controls in Its Acceptable Risk Safeguards 34


Figures

Figure 1: Medicare Administrative Contractors for Medicare Parts A/B, by State 10
Figure 2: Medicare Administrative Contractors for Durable Medical Equipment by State 11
Figure 3: CMS Sharing of Fee-for-Service Beneficiary Data with External Entities 14

**Abbreviations**

| | |
|---|---|
| ARS | Acceptable Risk Safeguards |
| CCW | Chronic Conditions Warehouse |
| CMS | Centers for Medicare & Medicaid Services |
| DME | Durable Medical Equipment |
| FISMA | Federal Information Security Modernization Act |
| HHS | Department of Health and Human Services |
| MAC | Medicare Administrative Contractor |
| MMA | Medicare Prescription Drug, Improvement, and Modernization Act of 2003 |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PII | personally identifiable information |
| VDCs | virtual data centers |
| VIPS | Viable Information Processing Systems |
| VRDC | Virtual Research Data Center |

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

March 6, 2018

The Honorable Orrin Hatch
Chairman
Committee on Finance
United States Senate

The Honorable Kevin Brady
Chairman
Committee on Ways and Means
House of Representatives

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

Recent data breaches at hospitals, insurance companies, and other entities in the health care industry have highlighted the importance of ensuring the security of health information, including personally identifiable information (PII),[1] about Medicare beneficiaries. The Centers for Medicare & Medicaid Services (CMS) within the Department of Health and Human Services (HHS) is the agency responsible for overseeing the Medicare program, which covers nearly 58 million aged and disabled Americans, who represent approximately 18 percent of the total U.S. population. Federal program spending for Medicare benefits totaled approximately $696 billion for fiscal year 2016.

Medicare beneficiary data are created, stored, and used by a wide variety of entities, such as health care providers, insurance companies, financial institutions, academic researchers, and other federal/state agencies for a wide variety of purposes. These include researching and monitoring the efficacy of health care treatments, payments, and analyzing the cost of health care treatments. The extent of beneficiary data that is collected

[1]Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

and maintained by CMS and its partners makes the data especially useful for these and other purposes. However, the distributed nature of Medicare systems and networks, along with the fact that so many entities external to CMS are connected to them, increases the potential that unauthorized individuals could gain access to these systems and the extensive amount of Medicare beneficiary data they contain.

You requested that we conduct a study of current CMS efforts to protect Medicare fee-for-service beneficiary data.[2] Our objectives were to (1) identify the major entities that collect, store, and process Medicare beneficiary data and that connect with CMS systems and networks; (2) determine whether requirements for the protection of Medicare beneficiary data align with federal guidance; and (3) assess the programs CMS has in place to oversee the implementation of security protections for Medicare beneficiary data.

To address our first objective, we analyzed prior GAO reports and CMS documentation, such as CMS data maps and system documentation. Additionally, we interviewed CMS officials to identify major external entities with which CMS shares Medicare beneficiary data and how those entities access that data. We analyzed the information from CMS to describe the type of Medicare data each major external entity has access to and the purpose for which such access is provided. Further, we analyzed the agency agreement template between CMS and major external entities to describe the processes for managing and monitoring the sharing of beneficiary data.

For our second objective, we reviewed relevant information security and privacy laws and National Institute of Standards and Technology (NIST) standards and guidance to identify federal requirements for implementing security and privacy. We compared the NIST standards and guidance with requirements established by CMS for entities that access Medicare fee-for-service beneficiary data to identify any inconsistencies. Additionally, we analyzed key documentation, such as information security contract clauses for each of the MACs and the standard data use agreement form used for all individuals and organizations that are either qualified entities or researchers, to determine how fully they reflect federal requirements.

[2]Under Medicare fee-for-service, also known as original Medicare, the government pays directly for the health care services that beneficiaries receive. Medicare fee-for-service covers both inpatient and outpatient services.

Regarding our third objective, we analyzed results from information security assessments performed by CMS and conducted interviews with CMS officials responsible for overseeing the security of Medicare fee-for-service beneficiary data provided to external entities. Specifically, we analyzed the information security assessments for contractor systems handling Medicare fee-for-service beneficiary data to determine the nature and extent of reported findings, the disposition of assessment recommendations, and whether assessment results were being addressed in a timely fashion. Appendix I discusses our objectives, scope, and methodology in greater detail.

We conducted this performance audit from October 2016 to January 2018 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.

# Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business, and is especially important for government agencies, where maintaining the public's trust is essential. Concerns about cyber threats to government systems and networks are well-founded, due to the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and advances in the sophistication and effectiveness of cyberattack technology, among other reasons. Without proper safeguards, systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain or manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

We and federal inspectors general have reported extensively on information security deficiencies that place federal agencies at risk of

disruption, fraud, or inappropriate disclosure of sensitive information.[3] Accordingly, since 1997, we have designated federal information security as a government-wide high-risk area.[4] This area was expanded to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

## Federal Law Establishes Security Requirements to Protect Federal Information and Systems

*The Federal Information Security Modernization Act of 2014*[5] (FISMA) is intended to provide a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets as well as the effective oversight of information security risks. FISMA assigns responsibility to the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or on behalf of an agency. The law also delegates to the agency's Chief Information Officer (or comparable official) the authority to ensure compliance with FISMA requirements.

FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency, including those provided or

[3]*Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems,* GAO-16-501 (Washington, D.C.: May 18, 2016), *Financial Audit: Fiscal Years 2016 and 2015 Consolidated Financial Statements of the U.S. Government,* GAO-17-283R (Washington, D.C.: Jan. 12, 2017), and Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report to Congress, FY 2016* (Washington, D.C.: March 2017).

[4]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and recently, GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[5]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 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

managed by another entity. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and procedures; developing plans for providing adequate information security for networks, facilities, and systems; providing security awareness and specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; developing and implementing procedures for detecting, reporting, and responding to security incidents; and ensuring continuity of operations. In addition, FISMA requires agencies to comply with NIST standards.

## Office of Management and Budget Provides Guidance to Agencies on Implementing FISMA

In accordance with FISMA, the Office of Management and Budget (OMB) is responsible for the oversight of agencies' information security policies and practices.[6] OMB establishes requirements for federal information security programs and assigns agency responsibilities to fulfill the requirements of statutes such as FISMA.[7] OMB requires agencies to oversee the implementation of security and privacy controls by contractors that collect, use, process, store, maintain, and disseminate federal information on behalf of a federal agency. For specific technical direction, OMB requires agencies to implement standards and guidelines established by NIST.

## NIST's Framework for Critical Infrastructure Cybersecurity Establishes a Baseline for Protecting Critical Information Assets

NIST has issued a suite of information security standards and guidelines, including *Recommended Security Controls for Federal Information Systems and Organizations*[8] and the *Framework for Improving Critical*

[6]44 U.S.C. § 3553.

[7]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (Washington, D.C.: July 2016).

[8]National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4 (Gaithersburg, Md.: April 2013).

*Infrastructure Cybersecurity*.[9] These documents collectively provide comprehensive guidance on developing and implementing information security programs to agencies and entities that perform work on their behalf.

The framework serves as a baseline for protecting critical information assets. In response to Executive Order 13636,[10] NIST issued the framework in February 2014. It is intended to help organizations apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. The framework outlines a risk-based approach to managing cybersecurity that is composed of three major parts: a framework core, profile, and implementation tiers.

The framework core includes a list of functions, categories, subcategories, and informative references that describe specific cybersecurity activities identified as being in common across all critical infrastructure sectors. Additionally, the framework contains implementation tiers that provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Further, the framework provides guidance on documenting individual organizational profiles that describe how the functions, categories, and subcategories align with the business requirements, risk tolerance, and resources of the organization. According to NIST, the framework core represents a common set of activities for managing cybersecurity risk. The framework also states that, while it is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use subcategories and informative references that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Table 1 lists the five functions and 22 categories of the framework core.

[9]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1 (Gaithersburg, Md.: February 2014).

[10]Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, issued in February 2013, outlines an action plan for improving security for critical cyber infrastructure. This includes, among other things, requirements for NIST to develop a voluntary critical infrastructure cybersecurity framework and performance measures.

**Table 1: National Institute of Standards and Technology Cybersecurity Framework Functions and Categories**

| Function | Category |
|---|---|
| Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. | • Asset management<br>• Business environment<br>• Governance<br>• Risk assessment<br>• Risk management strategy |
| Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. | • Access control<br>• Awareness and Training<br>• Data Security<br>• Information protection processes and procedures<br>• Maintenance<br>• Protective Technology |
| Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. | • Anomalies and events<br>• Security continuous monitoring<br>• Detection processes |
| Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. | • Response planning<br>• Communications<br>• Analysis<br>• Mitigation<br>• Improvements |
| Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. | • Recovery planning<br>• Improvements<br>• Communications |

Source: NIST, Framework for Improving Critical Infrastructure Cybersecurity. | GAO-18-210

Subsequent to the issuance of the *Cybersecurity Framework*, a May 2017 executive order required agencies to use the framework to manage cybersecurity risks.[11] It outlined actions to enhance cybersecurity across federal agencies and critical infrastructure to improve the nation's cyber posture and capabilities against cybersecurity threats to digital and physical security. In addition, the order directed agencies to develop plans to implement the framework within 90 days. The order required agencies to include in their plans:

[11]Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017.

- the status of planning, organizing, and submitting IT budget materials, as directed in the *Fiscal Year 2018 IT Budget Capital Planning Guidance,* that are aligned with the framework,
- the proposed internal management of cybersecurity risk using the updated metrics aligned to the framework,
- a timeline to map existing and planned capabilities with the framework functions, and
- the proposed use of the terminology and concepts in the framework to organize and communicate cybersecurity activities and outcomes.

## CMS Shares Medicare Fee-for-Service Beneficiary Data with Three Major Types of External Entities

CMS shares Medicare beneficiary data with three major types of external entities: (1) Medicare Administrative Contractors (MACs), the contractors that provide the core processing and distribution functions that support the payment of Medicare Part A,[12] Part B,[13] and Durable Medical Equipment (DME)[14] beneficiary claims on behalf of CMS, (2) research organizations (researchers), academic and non-profit entities that use Medicare beneficiary data to assist CMS in monitoring, managing, and improving Medicare programs or the services provided to beneficiaries, and (3) qualified public or private entities that use claims data on behalf of CMS to evaluate the performance of Medicare service providers and equipment suppliers.

[12]Medicare Part A is also known as Hospital Insurance and includes care provided by institutional providers: hospitals, skilled nursing facilities, home health agencies, hospice, comprehensive outpatient rehabilitation facilities, critical access hospitals, rural health clinics, and federally qualified health centers.

[13]Medicare Part B is also known as Supplemental Medical Insurance and includes care provided by physicians and non-physician practitioners, outpatient hospitals, parts of home health and hospice, and durable medical equipment, orthotics, and prosthetics suppliers.

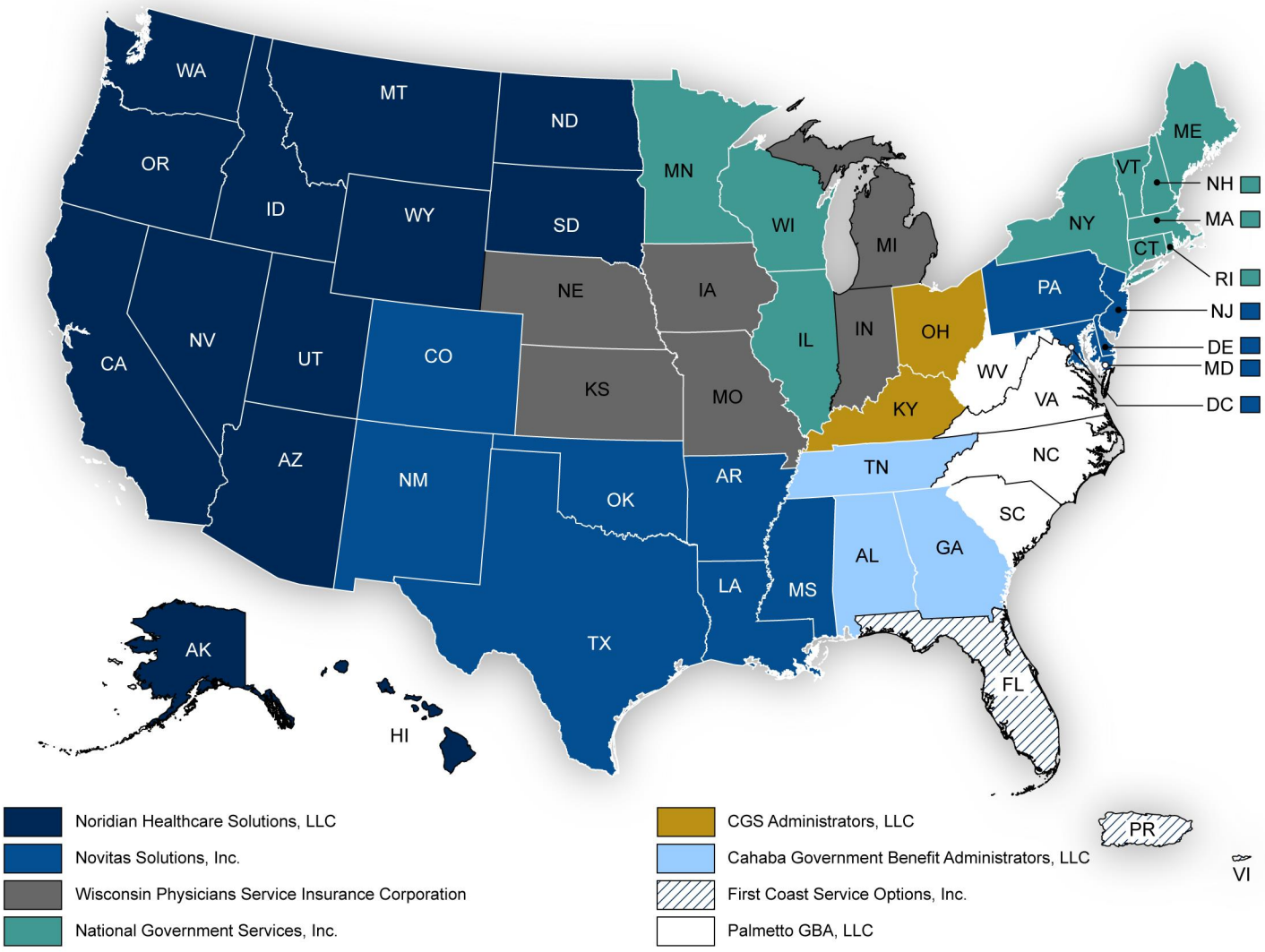
[14]Durable medical equipment is equipment and supplies ordered by a health care provider for everyday and extended use, such as wheelchairs and portable oxygen equipment.

## Medicare Administrative Contractors Access Fee-for-Service Beneficiary Data to Process Claims

MACs process more than 1.2 billion claims for Medicare Fee-for-Service beneficiaries annually. To do so, they interact with more than 1.5 million health care providers enrolled in the Medicare Fee-for-Service program. In addition to claims processing, some of the specific functions that the MACs perform include customer service for beneficiaries and providers, financial and debt management, audit and appeals functions, and medical reviews.

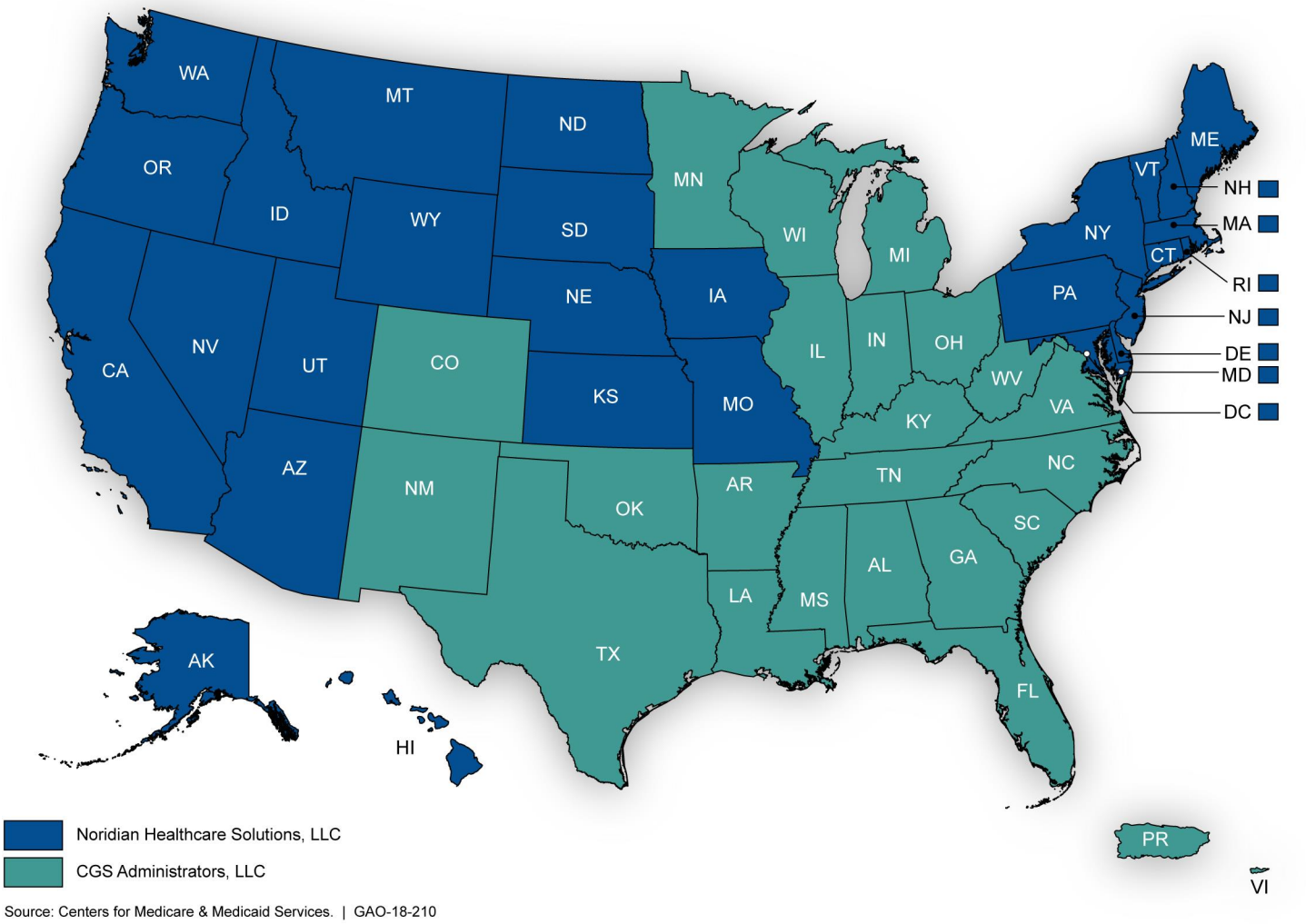
Each MAC contract covers a specific geographic area and a specific type of processing—either (1) Medicare Parts A and B claims or (2) DME claims for beneficiaries. Some MACs may hold multiple contracts and, thus, process multiple types of claims. In total, a network of eight MACs covers 16 multi-state jurisdictions, serving as the primary operational connection between the Medicare Fee-for-Service program and health care providers enrolled in the program. The geographic jurisdictions of the MACs that support Parts A and B and DME beneficiary claims are shown in figures 1 and 2, respectively.

**Figure 1: Medicare Administrative Contractors for Medicare Parts A/B, by State**




Source: Centers for Medicare & Medicaid Services. | GAO-18-210

**Figure 2: Medicare Administrative Contractors for Durable Medical Equipment by State**




Source: Centers for Medicare & Medicaid Services. | GAO-18-210

In order to collect, store, and process information needed to process claims and make benefits payments on behalf of CMS, MACs connect directly to CMS systems. Specifically, MACs connect to CMS's Virtual Data Centers (VDCs) through its CMSNet telecommunications network.[15] MACs process Medicare Fee-for-Service claims, which include

[15]CMSNet is a cloud-based, private government wide area network that is accessible through a secure, virtual private network connection. It is configured to be accessible only to CMS internal employees and contractors. CMSNet interconnects datacenters and systems in over 100 CMS locations across the country.

beneficiaries' PII and protected health information,[16] through the VDCs. The VDCs consists of two large datacenters that are operated and managed by CMS that collectively serve as a platform for Medicare claims processing software systems. MACs use a combination of four CMS systems that operate within the VDCs to process claims. These systems and their functions are described in table 2.

**Table 2: Shared Systems Used by the MACs to Process Medicare Fee-for-Service Claims**

| System name | Function |
|---|---|
| Fiscal Intermediary Shared System | Adjudicate all institutional (Medicare Part A) claims, including claims from hospitals, hospital outpatient departments, home health agencies, skilled nursing facilities, and hospices. |
| Multi-Carrier System | Adjudicate non-institutional (Medicare Part B) claims, including physician/non-physician practitioner claims, laboratory claims, therapy claims, Independent Diagnostic Testing Facility claims, and ambulance claims. |
| Viable Information Processing System (VIPS) Medicare System | Adjudicate durable medical equipment claims and certain prescription drug claims. |
| Common Working File | Approve claims adjudicated through the other three shared systems for payment. The system also stores beneficiary eligibility information, transmits data to a database that collects and maintains billing and utilization data on Medicare beneficiaries, and serves as the repository for beneficiary data received nightly from the Social Security Administration. |

Source: Centers for Medicare & Medicaid Services | GAO-18-210

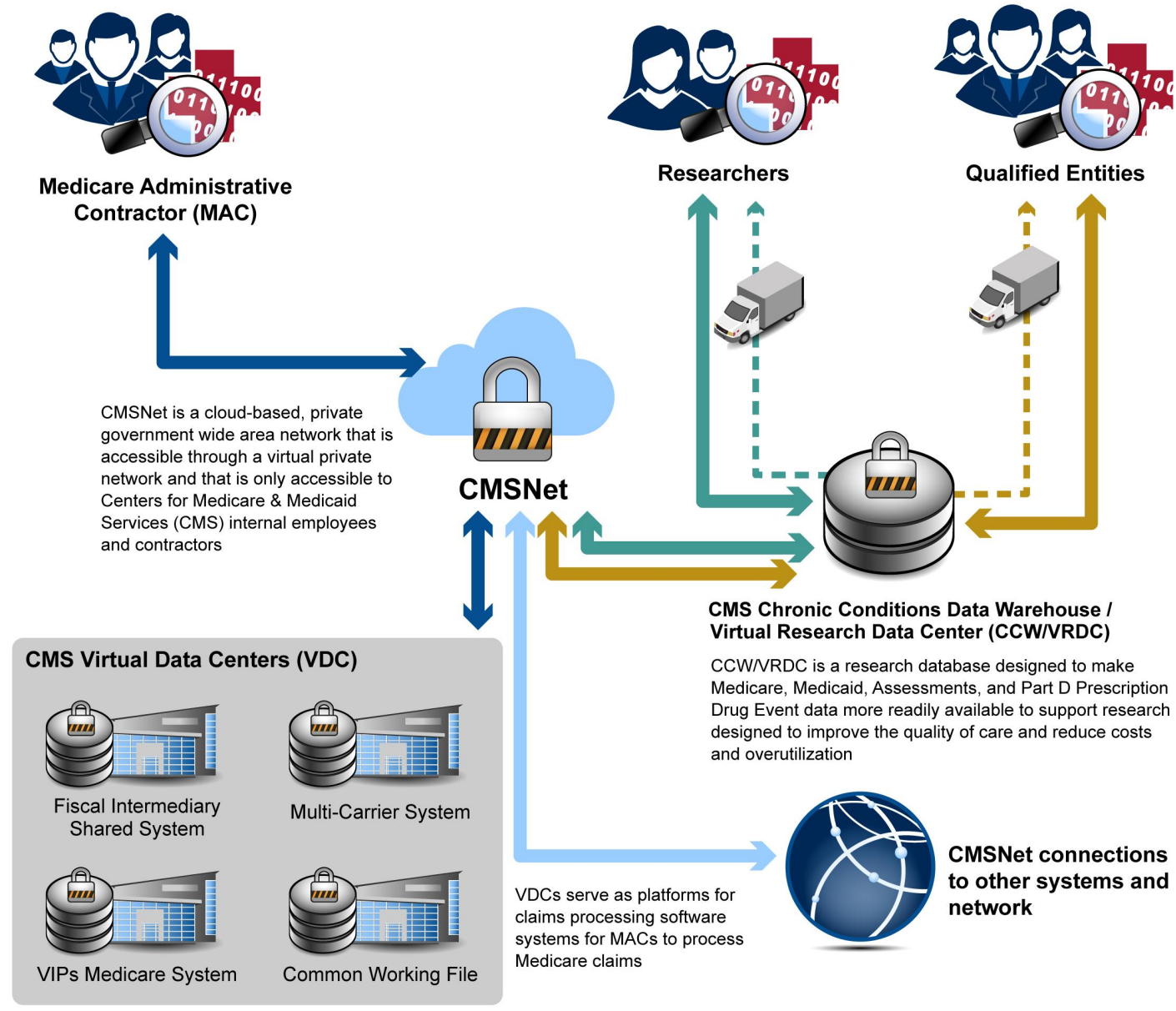
Health care providers submit Medicare fee-for-service claims to the MACs. The claims are reviewed to check if the claim is in a valid format, if the requestor is valid, and whether it is a duplicate. In addition, MACs process claims in the Fiscal Intermediary Shared Systems, Multi-Carrier System, VIPS Medicare System, and Common Working File. Processing

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

includes adjudicating claims, checking whether the services are covered by Medicare, and determining the price that should be paid to the provider for the service.

The links between external entities and CMS systems can take several different paths. Figure 3 shows how these entities are connected to CMS systems in order to obtain and use Medicare beneficiary data.

**Figure 3: CMS Sharing of Fee-for-Service Beneficiary Data with External Entities**




Source: Center for Medicare & Medicaid Services. | GAO-18-210

## Researchers Access Fee-for-Service Beneficiary Data to Assist CMS in Monitoring, Managing, and Improving Medicare Programs and Services

Researchers use Medicare beneficiary data to study how healthcare services are provided to beneficiaries. Examples of research entities include universities and colleges, non-profit research institutes, and policy research organizations. CMS offers researchers a broad range of data on the Medicare program to support research on current and future spending, past and present enrollment, and claims, which can benefit the public through improved delivery of healthcare services. Research performed using this data may also assist CMS in monitoring, managing, and improving Medicare programs and services to beneficiaries.

To obtain Medicare data from CMS, researchers must apply for access to a specific dataset, such as the Carrier file which includes claims for services provided by physicians and other non-institutional providers. In the application, the researcher provides information explaining how the data are to be used and stored, and CMS reviews and approves (or denies) the application. The researcher then enters a data use agreement with CMS for access to specific sets of Medicare beneficiary data, which are to be used only for stated research objectives. The data use agreement specifies which beneficiary data can be accessed, for what purpose, the duration of access, and data protection and confidentiality requirements. Unless the agreement authorizes the release of the data in accordance with CMS policy, it is not to be released by the researcher. As of October 2017, 195 research entities had received Medicare data.

Researchers access Medicare beneficiary data in one of two ways. To gain access from their computers, they connect to CMS's Chronic Conditions Warehouse/Virtual Research Data Center (CCW/VRDC)[17] through a CMS-provided secure network connection. Within the CCW/VRDC, researchers are given access to an individually tailored computing environment containing only copies of the specific sets of beneficiary data they have been authorized to use. Researchers can then

[17]CMS's Chronic Conditions Data Warehouse/Virtual Research Data Center is a research database designed to make Medicare, Medicaid, Assessments, and Part D Prescription Drug Event data more readily available to support research designed to improve the quality of care and reduce costs and overutilization.

conduct their analysis on the data using software tools provided by CMS within this secure environment.

Researchers can also access data by having it shipped to them in encrypted form through the U.S. mail. Once it has been received, researchers decrypt the data and load it into their own information systems for analysis. The data use agreements specify requirements for protecting beneficiary data obtained in this fashion.

## Qualified Entities Access Medicare Fee-for-Service Beneficiary Data to Evaluate the Performance of Service Providers and Equipment Suppliers

Qualified entities use CMS claims data to assess the effectiveness of Medicare service providers and equipment suppliers. The Medicare Data Sharing for Performance Measurement Program, originally established to comply with the *Patient Protection and Affordable Care Act*,[18] requires qualified entities to combine the Medicare data with claims data from sources other than Medicare to produce and publicly disseminate CMS-approved reports on provider and supplier performance with regard to measures of quality, efficiency, effectiveness, and resource use.

Like researchers, after they have been approved to access data by CMS,[19] qualified entities must enter into a data use agreement with CMS. The agreement specifies which beneficiary data can be accessed, for what purpose, the duration of access, and data protection and confidentiality requirements. A separate agreement is required for each qualified entity's activity. The Medicare beneficiary data to be accessed are encrypted and can either be shipped to the qualified entity on an external hard drive or saved within the CCW/VRDC to be accessed

[18]The *Patient Protection and Affordable Care Act* was enacted on March 23, 2010. Effective January 1, 2012, section 10332 of the *Affordable Care Act* amended section 1874 of the *Social Security Act* by adding a new subsection (e) requiring standardized extracts of Medicare claims data under parts A, B, and D be made available to "qualified entities" for the evaluation of the performance of providers of services and suppliers.

[19]The Qualified Entity Certification Program, launched in January 2012, is the certification arm of the Qualified Entity Medicare Data Sharing Program. The purpose of the Qualified Entity Certification Program is to evaluate and certify an entity's ability to serve as a qualified entity. Once certified, qualified entities are eligible to receive standardized extracts of Medicare Parts A and B claims data and Part D prescription drug event data for the purpose of evaluating the performance of providers.

through a Secure File Transfer System connection. Once it has received the electronic files, the qualified entity decrypts the files and analyzes the data on its own system(s).

As of October 2017, ten organizations had received Medicare data as a qualified entity. Each entity is responsible for analyzing and reporting on provider performance for one or more specific geographic area.

# CMS Established Information Security Requirements that Align with Federal Guidance for Some, but Not All, External Entities

CMS has developed requirements for implementing security controls that align with federal guidance for two of the three types of external entities that access Medicare Fee-for-Service data. Specifically, adherence to the requirements, which CMS defined using a risk-based process, is mandatory for MACs and qualified entities. However, CMS does not consider the requirements to be applicable to researchers because they are not CMS contractors. Without providing comprehensive, risk-based requirements for implementing security controls to all external entities that have access to Medicare beneficiary data, CMS increases the risk that external entities possessing CMS data may not have applied security controls that meet CMS standards.

## CMS Requirements for MACs and Qualified Entities Reflect a Risk-Based Assessment and Generally Align with the NIST Cybersecurity Framework

To assist agencies in the selection of appropriate security controls, NIST developed the *Cybersecurity Framework,* which specifies controls that support the core security functions of identifying, detecting, preventing, responding to, and recovering from security incidents.[20] Further, to ensure that controls are selected that achieve the security goals of the organization, NIST recommends that organizations use risk-based methods to tailor the selection of controls within this framework for implementation. According to NIST risk management guidance,[21] the tailoring process includes identifying a baseline of security controls, assigning specific values to organization-defined security control parameters, such as password complexity, and supplementing baselines with additional controls and control enhancements.

[20]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* version 1 (Gaithersburg, Md.: February 2014).

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

Once an agency has assessed security risks and identified appropriate controls to mitigate them, NIST recommends that the agency establish specific requirements for implementing those controls to ensure consistency both internally and externally to the agency. This is important in meeting the requirements of FISMA, which requires that a federal agency's security efforts include information and systems provided or managed by another agency, contractor, or other source. Additionally, the *Cybersecurity Framework* recommends that contracts or other formal agreements abide by NIST guidance to provide a means to ensure privacy and security controls; it also states that contractors are to protect PII in the same manner as their customers.

CMS developed minimum security requirements based on applicable federal guidance, for its own internal systems and for the systems operated by its contractors, such as MACs and qualified entities. These requirements are documented primarily in CMS's *Acceptable Risk Safeguards* (ARS).[22]

CMS designed the ARS as a tailored selection of NIST controls reflecting FISMA requirements as well as the agency's own policies, procedures, and guidance; other federal and non-federal guidance; and industry leading practices.[23] According to the agency, the requirements in the ARS are intended to ensure that systems meet a minimum level of information security and privacy assurance and reflect the agency's information systems security policy. CMS requires all employees, contractors, sub-contractors, and their respective facilities supporting agency business missions and performing work on behalf of the agency to observe this policy.

Because MACs are CMS contractors, the agency requires them to align their security practices with the ARS as well as with broader federal guidance, including NIST's catalog of recommended security controls,[24]

[22]Centers for Medicare and Medicaid Services, *CMS Acceptable Risk Safeguards*, Version 3.0 (Baltimore, MD: Centers for Medicare & Medicaid Services Office of Information Technology, Jan. 31, 2017).

[23]Additional detailed information about optional and required controls is specified in the *CMS Risk Management Handbook* (Baltimore, MD: Centers for Medicare & Medicaid Services Office of Information Technology, Jan. 31, 2017).

[24]National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4 (Gaithersburg, Md.: April 2013).

its minimum security standard for federal information systems,[25] and OMB's guidance on information management.[26] Additionally, as part of the Qualified Entity Certification Program and consistent with NIST guidance, CMS requirements state that systems used by qualified entities to process Medicare beneficiary data have been assessed at a moderate impact level and accordingly are held to the ARS implementation guidance using the minimum controls specified for moderate risk systems.

According to agency officials responsible for developing and maintaining the ARS, CMS used a risk-based process to select security controls to include in the requirements, thus ensuring that the ARS appropriately reflected agency needs and priorities. The process began with a review of baseline control requirements outlined in NIST guidance to ensure that all of those controls were reflected in the requirements. Then, the agency reviewed the rest of the NIST information security controls that were not included in the baseline and determined whether to include them in the ARS as "optional" controls. For example, the officials stated that certain controls appeared to apply primarily to national security systems and would not be needed for CMS applications. In all, the agency decided not to include 13 of the 165 controls specified in the NIST *Cybersecurity Framework,* none of which were designated by NIST as mandatory baseline controls.[27]

By undertaking this process of assessing the risk associated with each of the information security controls, the agency helped to ensure that its ARS reflects security requirements that are necessary and appropriate for its own systems and for systems operated by contractors on its behalf. A complete description of the NIST *Cybersecurity Framework* controls and how the ARS aligns with them can be found in appendix II.

[25]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200 (Gaithersburg, MD: Mar. 2006).

[26]OMB, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, DC: July 2016).

[27]A listing and description of these 13 controls is included in appendix II.

## CMS Does Not Provide Security Guidance for Researchers

While CMS requires MACs and qualified entities to implement security controls consistent with NIST guidance and provides additional guidance to ensure that those controls are consistent with CMS standards, it does not provide supplemental guidance tailored for researchers. Specifically, as part of its data use agreements with researchers, CMS includes a broad requirement to implement security and privacy protections that are consistent with NIST and OMB guidance. However, the agency has not provided risk-based guidance defining the minimum acceptable security controls that researchers should implement to protect Medicare beneficiary data. Nor has CMS provided guidance to researchers on how to select and implement specific security controls.

According to CMS officials who oversee researcher access to CMS data, all researchers are required to prepare data management plans that outline their planned safeguards for protecting Medicare beneficiary data in their custody. In determining what controls to implement, however, they have only broad federal guidance, such as NIST's catalog of controls,[28] to use as a reference. The officials stated that CMS has not developed specific requirements based on an assessment of the risks associated with researcher functions that would define a minimum set of required safeguards. This is in contrast with the MACs and qualified entities, which have specific requirements based on the ARS that they are to implement to adequately protect data received from CMS.

The lack of specific requirements does not affect all data that researchers access on behalf of CMS. In many cases, researchers access and process Medicare beneficiary data on systems operated by CMS and are not responsible for implementing the security controls for those systems. In such cases, the researchers access beneficiary data within a virtualized environment, called the CCW/VRDC, which allows CMS to monitor data retrieval and use.

However, in other cases, CMS provides beneficiary data to researchers on external hard drives or other physical media that are outside of the Chronic Conditions Warehouse. In those cases, researchers receive Medicare beneficiary data that they transfer to and process on their own

[28]NIST SP 800-53.

systems. These systems are secured according to individual researchers' own policies and procedures, which may or may not be consistent with CMS requirements applied to other entities.

CMS requirements tailored specifically for researchers could address topics such as password complexity, patch management, and encryption of sensitive data, all of which otherwise may be implemented inconsistently by different researchers. According to CMS officials responsible for overseeing researcher access to data, CMS does not require researchers to adhere to its *Information Systems Security and Privacy Policy*[29] or to implement the controls specified in the ARS because researchers are not agency contractors. The CMS officials said it was not necessary for the agency to set specific security requirements for entities that do not have a contractual relationship with the agency. Additionally, these officials stated that they believe the lack of specific guidance gives the researchers more flexibility to independently assess their security risks and determine which controls to implement based on that assessment.

However, by not providing guidance to researchers that includes security implementation requirements tailored to CMS-authorized uses of Medicare data, CMS cannot ensure that researchers implement security measures that are commensurate with the sensitivity of the data that is provided to them. As a result, there is an increased risk that sensitive PII and protected health information may be at risk of compromise.

## CMS Has Not Consistently Overseen the Implementation of Security Controls by External Entities

CMS has established a program to oversee the MACs' implementation of security and privacy protections over Medicare beneficiary data, but it does not consistently track low-risk weaknesses in the CMS FISMA Controls Tracking System. MACs are subject to two types of independent annual assessments that regularly identify weaknesses in their implementation of security controls. The assessments have identified several recurring categories of weaknesses; however, the agency does

[29]CMS, *CMS Information Security and Privacy Acceptable Risk Safeguards*, (Baltimore, MD: January 31, 2017).

not track low-risk weaknesses that could be related to these recurring categories. Additionally, CMS has not established a corresponding program for overseeing the implementation of security controls by researchers and qualified entities. Without more consistently tracking identified issues at MACs and establishing effective oversight measures for researchers and qualified entities, CMS cannot fully ensure that the security of Medicare beneficiary data is being adequately protected.

## CMS Has Overseen Independent Assessments at the MACs, but Has Not Consistently Tracked Issues Identified by Those Assessments

Requirements for agencies to oversee the implementation of security protections are established in law and federal guidance. For example, the NIST *Cybersecurity Framework* specifies that organizations should assess security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. The framework states that, as part of the process for conducting security control assessments, organizations should track and monitor weaknesses and develop remedial actions. Further, according to the framework, the security assessment process is intended to provide feedback to organizations that can use the information to make risk-based adjustments to protections for their systems and networks.

In addition, both FISMA and the *Medicare Prescription Drug, Improvement, and Modernization Act* (MMA) of 2003 set specific requirements for CMS oversight of the implementation of information security controls by the MACs. FISMA requires an annual independent evaluation of an agency's information systems, including those provided or managed by contractors, to ensure compliance with NIST requirements. Further, OMB's FISMA guidance specifies regular testing of all security controls with an agency-determined, risk-based subset to be tested annually. The MMA likewise requires the MACs to undergo an independent evaluation of their information security program on an annual basis. Specifically, an independent assessor is to annually test an appropriate subset of a contractor's systems and assess compliance with federal requirements for information security policies, procedures, standards, and guidelines, as defined by OMB.

## MACs Undergo Two Types of Annual Assessments

In order to meet the requirements of the MMA and FISMA, CMS established two separate annual information security assessment processes for the MACs. Specifically, to comply with MMA, CMS has overseen independent annual evaluations of these contractors since the law was enacted in 2003. CMS selected an independent assessor to perform all of the MMA assessments. The assessor first reviews documentation of the implementation of security controls by the contractor and then reviews technical security controls onsite at each MAC. In 2010, CMS expanded the MMA assessments into more technical areas and has included penetration testing as part of the assessments.

In addition, agency officials that oversee the MMA assessments stated that CMS reviews contractor policies and procedures for configuration management twice a year and conducts an on-site review of the implementation of selected technical controls every June. In 2016, the independent assessor performed tests in nine categories of security controls at eight MAC datacenters.[30] In total, these assessments reported 168 weaknesses, of which 53 were categorized as high or moderate risk and 115 were low-risk.

Further, to comply with FISMA requirements that all controls are tested regularly, CMS requires MACs to test one-third of their system security controls annually. CMS determines the control families to be tested in any given year and rotates the selection each year so that all controls are tested by the end of the 3-year testing cycle. For the 2016 FISMA assessment, CMS selected 121 security requirements within 8 control families.[31]

The independent assessor is responsible for assessing the security controls and making recommendations on how to correct weaknesses and address identified vulnerabilities. To determine compliance with CMS

[30]The nine control categories included conducting periodic risk assessments; establishing policies and procedures to reduce risk; defining system security plans; conducting security awareness training; periodically testing security controls; tracking remedial actions; detecting, reporting, and responding to incidents; maintaining plans for continuity of operations; and protecting privacy.

[31]CMS selected the following eight control families: security assessment and authorization, configuration management, media protection, planning, risk assessment, system and communications protection, transparency, and use limitation.

requirements, controls are assessed against the minimum security requirements defined in the CMS ARS.

According to CMS officials from the Medicare Contractor Management Group,[32] the two annual assessment processes together ensure that sufficient testing is being conducted each year. For example, in any given year, the MMA assessments may cover different security controls than the FISMA assessments.[33] In addition, the FISMA assessors may identify outstanding recommendations that were made from the prior year's MMA assessment and provide a status update on progress made to address open recommendations.

## Corrective Actions and Milestones Have Not Always Been Tracked Consistently

Tracking and remediation are key parts of an organization's security program that help to ensure that identified issues are addressed promptly and effectively. CMS requires the MACs to develop corrective action plans to remediate most of the weaknesses identified by the MMA and FISMA assessments. CMS requires that these weaknesses, along with plans of action and milestones for correcting them, be captured and tracked in its CMS FISMA Controls Tracking System, which is an agency-wide system for tracking the remediation of identified weaknesses. The tracking system maintains the certification and accreditation documents for all MAC systems and manages plans of action and milestones, their remediation activities, and completion. CMS monitors the disposition of all issues captured in the CMS FISMA Controls Tracking System, which helps to ensure that the MACs take steps to address weaknesses within required time frames.

[32]The Medicare Contract Management Group, among other responsibilities, coordinates the reviews of MACs, ensures that findings are tracked, and monitors corrective action plans to ensure that they are completed.

[33]The *Medicare Modernization Act* requires testing and an assessment of compliance with FISMA and other information security requirements. The MMA requires the information security program to meet requirements in the following areas: periodic risk assessment, policies and procedures to reduce risk, system security plans, security awareness training, periodic testing of information security controls, remedial actions, incident detection, incident reporting, incident response, and continuity of operations. Additionally, CMS added privacy controls to the areas of testing starting in 2015.

However, because CMS does not routinely track low-risk weaknesses, it may not be ensuring that all weaknesses consistently receive appropriate management attention and timely remediation. Specifically, with regard to the MMA assessments, CMS requires MACs to develop a corrective action plan to remediate only high and medium-risk weaknesses, which are tracked using plans of action and milestones. CMS does not require the tracking of low-risk weaknesses, which are shown in the assessment reports as recommended improvements rather than weaknesses in need of correction. In certain cases, MMA assessments have classified weaknesses as low-risk, and they have not been tracked in the CMS FISMA Controls Tracking System, even though similar weaknesses were classified by other assessments as medium- or high-risk, and were tracked. In contrast to the MMA assessments, CMS requires that MACs track all weaknesses identified in FISMA assessments in the CMS FISMA Controls Tracking System.

Examples of inconsistently classified weaknesses reported in the 2016 MMA assessments include (1) maintaining complete and up-to-date inventories of information system components and (2) ensuring that protections against malicious software are installed and kept up-to-date. Of the six assessments that reported that MACs did not have a complete and accurate listing of systems and devices supporting Medicare claims processing, three classified this weakness as medium-risk and created a plan of action and milestones, while the other three assessed a low-risk level and did not create a plan of action and milestones. Similarly, eight assessments reported that MACs either did not have malicious software protections installed or they were not up-to-date. Of these eight, CMS officials stated that three were classified as medium-risk and were tracked by CMS, while the other five were assigned a low-risk level and not tracked.

The inventory and malicious software protection weaknesses that were tracked inconsistently are related to categories of weaknesses that have posed recurring challenges for the MACs in recent years. Since 2009, both the MMA and FISMA assessments have reported incomplete implementation of several types of high-risk security requirements across all the MACs. The weaknesses identified during these assessments—which generally involved configuration management, system security plans, and system inventories—have yet to be fully resolved. Table 3 describes these key categories of weaknesses.

**Table 3: Key Recurring Categories of Weaknesses Identified in Annual Assessments of MACs**

| Category | Description |
|---|---|
| Configuration management | Configuration management is the process of monitoring and controlling how changes are made to systems and networks, including how configuration settings and baselines are updated. It is essential to ensure that software updates are timely, appropriate, and do not introduce new security weaknesses. |
| System security plans | System security plans contain detailed descriptions of how security controls are intended to be implemented, allowing assessors to effectively review a system's security strategy and determine whether security has been implemented as intended. |
| System inventories | An accurate and complete inventory of each system is critical as a basis for effective configuration management. Without a complete inventory, configuration management activities may be rendered incomplete or ineffective. Consequently, security officials may be unaware that inappropriately configured devices running obsolete versions of software may be connected to the network, posing risks to other systems and information. |

Source: GAO Analysis of annual MAC assessments. | GAO-18-210

According to CMS officials, weaknesses identified in the annual MMA assessments may be ranked at different risk levels because the specific circumstances of each finding can vary. However, documentation of the specific weaknesses identified in the 2016 MMA assessment reports does not make clear why findings that are characterized in similar terms or have the same name may have been assigned different risk levels.

CMS officials who oversee the information security testing at MACs stated that they are aware of the recurring areas of weaknesses identified in the annual assessments and have been taking actions to address them. For example, in 2009, CMS began requiring MACs to submit evidence that their configuration management programs complied with CMS requirements. According to the officials, since this program has been put into place, configuration management processes at the MACs have become more consistent and more thoroughly documented. Nevertheless, the 2016 FISMA assessments concluded that a MAC's system security plan did not include procedures for testing changes made to their production environments, and the MAC was not tracking changes made to the production environments. According to the CMS officials, the fact that recurring issues such as these have not yet been fully resolved may be due to the root causes of the deficiencies not yet being addressed.

Without more consistent tracking of identified issues through plans of action and milestones, it may be difficult for CMS to fully determine the extent to which security weaknesses identified during assessments of the MACs are remediated. Weaknesses that appear to be low-risk may be indicators of more significant underlying issues and, thus, may not be receiving appropriate management attention or prompt remediation, unnecessarily exposing Medicare beneficiary data to security risks.

## CMS Does Not Have Effective Oversight Processes and Procedures for Researchers and Qualified Entities

While CMS has established assessment programs for MACs, the agency has much more limited security oversight mechanisms in place to ensure that qualified entities and researchers with access to Medicare beneficiary data implement appropriate security controls. CMS oversight processes and procedures for qualified entities and researchers consists primarily of reviewing the data protections that researchers and qualified entities describe in the data management plans they submit when requesting access to Medicare beneficiary data.

According to CMS officials who review these plans, they may ask follow-up questions to obtain more information or make recommendations on how to better implement security safeguards in accordance with CMS requirements. However, no further reviews are conducted for any qualified entities or researchers. For example, CMS does not conduct on-site reviews of the implementation of security controls and does not collect or review evidence of whether the controls have been appropriately implemented. Further, it does not conduct or require any independent testing of security controls.

As an additional check for qualified entities, instead of assessing their security controls, CMS assesses their responses to questions relating to 213 moderate-level data security controls from 26 control families set forth in the ARS. However, once the initial document review has been completed, CMS does not perform any in-person or document reviews of security controls that are in place unless the qualified entity reports a major change in its data security environment after initial approval.

According to officials of the Office of Enterprise Data Analytics, which is responsible for overseeing access to Medicare data by researchers and qualified entities, CMS has, in the past, conducted remote and on-site reviews as a pilot project. These reviews examined selected researchers'

security controls, based on factors such as the use of data described in the researchers' data management plans. According to these officials, the pilot project is no longer being conducted because funding for the program has stopped.

The need to ensure that these entities have effectively implemented information security controls is demonstrated by data breaches that these organizations have reported. Of the 195 research entities that CMS has data use agreements with, six have suffered data breaches involving the loss of over 500 records containing PII covered under the *Health Insurance Portability and Accountability Act of 1996*,[34] which they reported to the HHS Office of Civil Rights. These breaches included Internet-based intrusions into researcher systems as well as other IT-related incidents.

According to CMS officials who oversee access to Medicare data for researchers and qualified entities, the data use agreement requires organizations to report any breach of PII or personal health information from the CMS data files to the agency. These officials also stated that the six organizations did not report any breaches to CMS and that they were unaware that the organizations had reported compromises. The officials noted that if the breaches did not involve PII or personal health information from CMS data files provided under a data use agreement, the organizations were not required to report this information to CMS. Further, these officials stated that the agency is currently revising its data management plan to include a requirement for organizations to fully disclose all breaches to the agency, which may impact whether or not to grant access to Medicare data for organizations that were breached.

Given that, in the past, researchers' systems have been successfully attacked, effective implementation of security controls is critical to reducing threats of compromise. However, without more robust oversight processes and procedures, CMS cannot determine whether qualified entities or researchers have implemented security controls appropriately and, thus, cannot ensure that the risks associated with their use of Medicare beneficiary data have been adequately mitigated.

[34]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).

# Conclusion

CMS shares Medicare beneficiary data with external entities primarily for processing Medicare claims, supporting medical research, and evaluating the performance of Medicare service and equipment providers. CMS has set basic requirements for protecting the security of Medicare beneficiary data that it shares with MACs, qualified entities, and researchers. However, CMS has not required the documentation of low-risk weaknesses in the CMS FISMA Controls Tracking system so that CMS can track the MACs' remediation of weaknesses that have been identified in recurring annual assessments. In addition, MACs and qualified entities are given guidance that generally aligns with federal guidance and is based on an assessment of risks specific to CMS to ensure that appropriate controls have been included. However, CMS has not provided guidance to researchers on how to select and implement specific security controls. Until CMS provides more comprehensive, risk-based guidance on implementing security controls to all of its external partners, there is an increased risk that researchers will not fully implement appropriate protections for Medicare beneficiary data.

CMS has developed and implemented an oversight program for the MACs' implementation of security controls based on two types of annual independent assessments, which together help ensure that sufficient testing is being conducted each year. However, CMS has not ensured that the MACs track and remediate identified weaknesses consistently, including weaknesses that have been identified in recurring annual assessments. Further, CMS has not established an oversight program for qualified entities and researchers to assess whether they are implementing security controls as they are required. Without more effective oversight programs in place, CMS lacks full assurance that external entities are appropriately implementing security protections for Medicare beneficiary data.

# Recommendations

We are making three recommendations to the Administrator of the Centers for Medicare and Medicaid Services:

- Develop and distribute guidance for researchers defining minimum security controls and implementation guidance for those controls that is consistent with NIST guidance. (Recommendation 1)

- Develop processes and procedures to ensure that findings from all MAC assessments are classified consistently and tracked appropriately. (Recommendation 2)
- Develop processes and procedures to ensure that qualified entities and researchers have implemented information security controls effectively throughout their agreements with CMS. (Recommendation 3)

## Agency Comments and our Evaluation

We received written comments on a draft of this report from HHS. In the comments (reprinted in appendix III), the department concurred with our three recommendations and discussed actions that the department has planned or taken. If fully and effectively implemented, the intended actions should help HHS to address weaknesses in processes and procedures for ensuring the protection of Medicare beneficiary data used by the department's contractors. The department also provided technical comments, which we have incorporated in the report, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Health and Human Services, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9342 or marinosn@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 IV.

Nick Marinos
Director, Cybersecurity & Information Management Issues

# Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify the major entities that collect, store, and process Medicare beneficiary data and that connect with Centers for Medicare and Medicaid Services (CMS) systems and networks; (2) determine whether requirements for the protection of Medicare beneficiary data align with federal guidance; and (3) assess the programs CMS has in place to oversee the implementation of security protections for Medicare beneficiary data.

To address our first objective, we analyzed prior GAO reports and CMS documentation, such as CMS data maps and system documentation. Additionally, we conducted interviews with agency officials to identify major external entities that access Medicare beneficiary data, including with Medicare Administrative Contractors (MAC) and researchers. We analyzed the information obtained from CMS to describe the type of Medicare data each entity has access to and purposes for which such access is provided. Further, we analyzed agency agreements with external entities to describe external uses for the data CMS collects and distributes.

Regarding our second objective, we analyzed CMS guidance, specifically its *Acceptable Risk Safeguards*[1] (ARS), to determine baseline requirements for the protection of Medicare beneficiary data that have been established by CMS. To assess the completeness of this guidance, we compared the ARS to the National Institute of Standards and Technology's (NIST) *Cybersecurity Framework's* controls included in the "identify," "protect," "detect," and "respond" categories.[2] We did not include the "recover" category because it is more focused on data recovery than on the identification, protection, and detection capabilities necessary to prevent incidents. We compared the controls referenced by NIST to the controls that were documented in the ARS to identify controls

[1]CMS, *CMS Information Security and Privacy Acceptable Risk Safeguards*, (Baltimore, MD: January 31, 2017).

[2]The NIST Cybersecurity Framework core consists of five functions—Identify, Protect, Detect, Respond, and Recover. When considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

that had not been included. We also interviewed CMS officials responsible for developing the ARS to determine the process that the agency uses to select controls.

Additionally, to determine how CMS required external entities to implement security measures, we reviewed formal agreements that were entered into with those organizations. For the MACs, we analyzed contracts to determine CMS security requirements. For researchers and qualified entities, we reviewed the data use agreement templates to determine what requirements CMS specified for selecting and implementing security measures.

To address our third objective, we analyzed system assessments performed by CMS and conducted interviews with CMS officials responsible for overseeing the security of Medicare beneficiary data provided to external entities. Specifically, we analyzed information security assessments to determine the nature and extent of reported findings, the disposition of assessment recommendations, and whether assessment results were being addressed in a timely fashion over the span of time that they have been conducted.

For the MACs, we reviewed assessments performed in accordance with the *Federal Information Security Management Act* and the *Medicare Prescription Drug, Improvement, and Modernization Act of 2003.* For researchers and qualified entities, we obtained information from CMS about ongoing and previously performed assessment programs. Through interviews with relevant CMS officials, we obtained and analyzed information about the findings that were not resolved in a timely fashion and about the constraints that prevented the ongoing assessment of researchers and qualified entities.

We conducted this performance audit from October 2016 to January 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Analysis of CMS Acceptable Risk Safeguards

We compared the Centers for Medicaid and Medicare Services (CMS) *Acceptable Risk Safeguards (*ARS) with the National Institute of Standards and Technology (NIST) *Cybersecurity Framework* to determine the extent to which the ARS aligns with the framework. To do this, we compared the controls noted as informative references by the framework to the controls documented in the ARS. We did not assess the "Recover" category because it is more focused on data recovery than on the identification, protection, and detection capabilities necessary to prevent incidents.

Our analysis showed that the ARS generally aligns with the NIST *Cybersecurity Framework*, addressing most but not all of the controls noted as informative references to the framework. Specifically, of the 165 NIST controls, the ARS reflects 152. There are 13 controls referenced in the framework and NIST guidance that are not also reflected in the ARS. For example, 4 of the 16 controls from the Audit and Accountability family and 3 of the 11 controls from the Identification and Authorization family are not reflected in the ARS. None of the 13 controls were designated by NIST as mandatory baseline controls. Table 4 includes details about the controls that were not addressed in the ARS:

**Table 4: Extent to Which CMS Addressed NIST Controls in Its Acceptable Risk Safeguards**

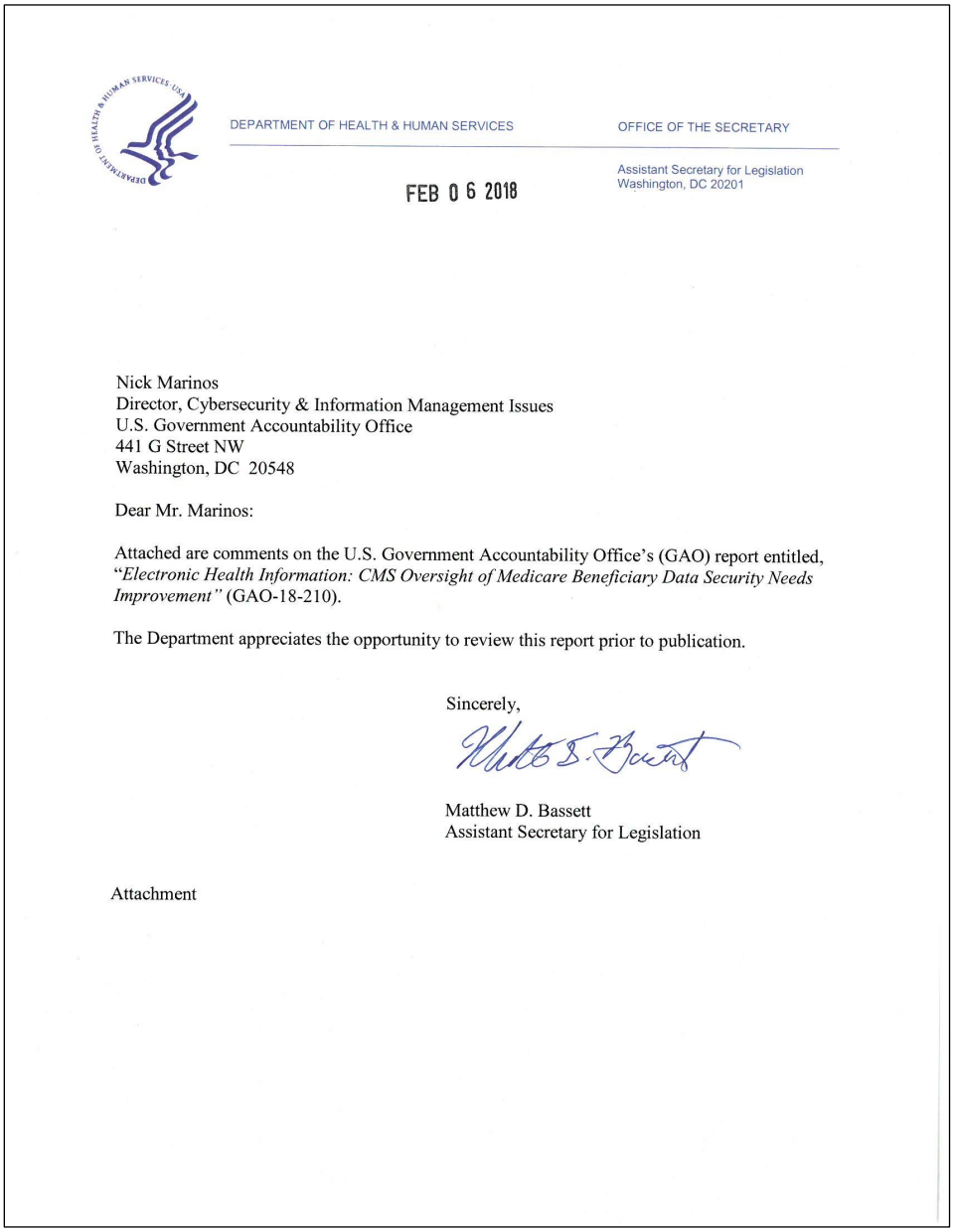
| NIST Control Category | NIST Control Subcategory | Status | GAO Analysis |
|---|---|---|---|
| Identify | Asset management | Partially | CMS addressed most, but not all, of the controls listed under Asset Management. The control not addressed was performing a criticality analysis to identify critical information system components and functions. This control is important to establish better risk management to prioritize supply chain protection. |
| | Business environment | Partially | CMS addressed most, but not all, of the controls listed under business environment. Examples of controls not addressed include the ability to communicate via alternate means and performing a criticality analysis to identify critical information system components and functions. These controls are important to establish communication that would not be compromised in the event of an attack. |
| | Risk assessment | Partially | CMS addressed most, but not all, of controls listed under risk assessment. The control not addressed was performing a criticality analysis to identify critical information system components and functions. This control is important to establish better risk management to prioritize supply chain protection. |

| NIST Control Category | NIST Control Subcategory | Status | GAO Analysis |
|---|---|---|---|
| Protect | Access control | Partially | CMS addressed most, but not all, of the controls listed under access control. Examples of controls not addressed include the ability to provide additional identification and authentication measures under specific circumstances and to provide dynamic authentication for service providers. These controls are important to establish more avenues of identifying individuals or services that receive Medicare Beneficiary Data. |
| | Data Security | Partially | CMS addressed most, but not all, of the controls listed under data security. The control not addressed was performing an analysis to identify ways that an unauthorized entity might access security domains. This is important to know if there are any ways to communicate in the environment the organization might not be aware of in order to address that vulnerability. |
| | Information protection processes and procedures | Fully | CMS addressed all of the requirements for establishing the policies for this family of controls. |
| Detect | Anomalies and events | Fully | CMS addressed all of the requirements for establishing the policies for this family of controls. |
| | Security continuous monitoring | Partially | CMS addressed most, but not all, of the controls listed under security continuous monitoring. Examples of controls not addressed include monitoring information sites for breaches of organization data and establishing a zone in the network environment to test data, such as e-mails, for malware before accessing the data in a production environment. These controls are important in order to become aware of potential breaches and to address malware without risking the live environment. |
| | Detection processes | Fully | CMS addressed all of the requirements for establishing the policies for this family of controls. |
| Respond | Response planning | Fully | CMS addressed all of the requirements for establishing the policies for this family of controls. |
| | Analysis | Fully | CMS addressed all of the requirements for establishing the policies for this family of controls. |
| | Mitigation | Fully | CMS addressed all of the requirements for establishing the policies for this family of controls. |

Legend: ● – Fully implemented. ◐ - Partially implemented.

Source: GAO analysis | GAO-18-210

# Appendix III: 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

FEB 0 6 2018

Nick Marinos
Director, Cybersecurity & Information Management Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Marinos:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement*" (GAO-18-210).

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

Sincerely,

Matthew D. Bassett
Assistant Secretary for Legislation

Attachment

**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – ELECTRONIC HEALTH INFORMATION: CMS OVERSIGHT OF MEDICARE BENEFICIARY DATA SECURITY NEEDS IMPROVEMENT (GAO-18-210)**

The U.S. Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report on Centers for Medicare & Medicaid Services (CMS) oversight of Medicare beneficiary data security. HHS takes its responsibility to protect and secure Medicare beneficiary data seriously.

The Federal Information Security Management Act of 2002 (FISMA) requires each Federal agency to develop, document, and implement an agency-wide information and information system security program that supports the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The Federal Information Security Modernization Act of 2014 amends FISMA 2002, recognizing evolving security concerns by focusing on issues caused by security incidents, by strengthening the use of continuous monitoring, and by increasingly focusing on compliance.

FISMA 2002 and 2014 require the National Institute of Standards and Technology (NIST) to develop security standards and guidance, including minimum requirements for federal systems. NIST also developed an integrated *Risk Management Framework* which brings together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies. HHS utilizes a risk-based approach to implementing NIST standards across the agency through policies and procedures such as the *HHS Information Security and Privacy Policies* and has an enterprise-wide information security and privacy program, known as the HHS Cybersecurity Program, to protect against potential information technology threats and vulnerabilities. In addition, CMS provides guidance to both internal CMS staff and its contractors in the *CMS Information Security Acceptable Risk Safeguards* as to the minimum acceptable level of required security controls that must be implemented by CMS and its contractors to protect information and information systems.

HHS requires information security risk assessments that document the impact of interruptions on business functions and assesses the system's security posture against potential threats. To ensure standardized levels of security, HHS requires all employees, contractors, sub-contractors and their respective facilities to observe this policy. As GAO notes in the report, FISMA requirements are not applicable to researchers and qualified entities because they are not classified as a federal entity or contractor. All findings, risks, and assessments of HHS systems subject to FISMA requirements are tracked through an electronic Governance, Risk and Compliance tool; the CMS FISMA Controls Tracking System is the repository used by CMS to manage the security and privacy requirements of its information systems. This platform provides a common foundation to manage standards, controls, risks, assessments and deficiencies across the CMS IT Enterprise.

In addition to the FISMA process outlined above, Medicare Administrative Contractors (MACs) are subject to requirements outlined in the *Medicare Prescription Drug, Improvement, and Modernization Act* (MMA). The MMA requires MACs to undergo an independent evaluation of their information security program, utilizing standards and guidelines defined by OMB, on an

**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: ELECTRONIC HEALTH INFORMATION: CMS OVERSIGHT OF MEDICARE BENEFICIARY DATA SECURITY NEEDS IMPROVEMENT (GAO-18-210)**

annual basis. In order to meet both FISMA and MMA requirements, HHS has established two separate annual information security cycles for the MACs. Findings and remediation actions for both processes are tracked through completion in the CMS FISMA Controls Tracking System.

GAO's recommendations and HHS' responses are below.

**Recommendation**
The Administrator of CMS should develop and distribute guidance for researchers defining minimum security controls and implementation guidance for those controls that is consistent with NIST guidance.

**HHS Response**
HHS concurs with this recommendation. HHS will consider the impact guidance would have on researchers and after such considerations, evaluate developing and distributing guidance that would define and implement minimum security controls that are consistent with NIST guidance.

**Recommendation**
The Administrator of CMS should develop processes and procedures to ensure that findings from all MAC assessments are classified consistently and tracked appropriately.

**HHS Response**
HHS concurs with this recommendation. CMS classifies all findings from both the FISMA and MMA assessments consistently and tracks them through completion. Prior to this GAO review, HHS implemented a process to review, evaluate and risk rank all findings noted at each MAC. This process was implemented to ensure that each finding is risk ranked as consistently and objectively as possible.

**Recommendation**
The Administrator of CMS should develop processes and procedures to ensure that qualified entities and researchers have implemented information security controls effectively throughout their agreements with CMS.

**HHS Response**
HHS concurs with this recommendation. HHS is considering implementing processes and procedures that would be necessary to ensure that qualified entities and researchers have implemented information security controls during their agreements with CMS. CMS will consider the impact these processes and procedures would have on qualified entities and researchers while developing them.

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

## Page 1

Nick Marinos

Director, Cybersecurity & Information Management Issues

U.S. Government Accountability Office 441 G Street NW

Washington, DC 20548

Dear Mr. Marinos:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, " Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement" (GAO-18-210).

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

Sincerely ,

Matthew D. Bassett

Assistant Secretary for Legislation

Attachment

## Page 2

The U.S. Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report on Centers for Medicare & Medicaid Services (CMS) oversight of Medicare beneficiary data security. HHS takes its responsibility to protect and secure Medicare beneficiary data seriously.

The Federal Information Security Management Act of 2002 (FISMA) requires each Federal agency to develop, document, and implement an agency-wide information and information system security program that supports the operations and assets of the agency, including those provided or managed by another agency, contractor, or

other source. The Federal Information Security Modernization Act of 2014 amends FISMA 2002, recognizing evolving security concerns by focusing on issues caused by security incidents , by strengthening the use of continuous monitoring, and by increasingly focusing on compliance.

FISMA 2002 and 2014 require the National Institute of Standards and Technology (NIST) to develop security standards and guidance, including minimum requirements for federal systems. NIST also developed an integrated Risk Management Framework which brings together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies. HHS utilizes a risk- based approach to implementing NIST standards across the agency through policies and procedures such as the HHS Information Security and Privacy Policies and has an enterprise- wide information security and privacy program, known as the HHS Cybersecurity Program, to protect against potential information technology threats and vulnerabilities. In addition, CMS provides guidance to both internal CMS staff and its contractors in the CMS Information Security Acceptable Risk Safeguards as to the minimum acceptable level of required security controls that must be implemented by CMS and its contractors to protect information and information systems.

HHS requires information security risk assessments that document the impact of interruptions on business functions and assesses the system's security posture against potential threats. To ensure standardized levels of security, HHS requires all employees, contractors, sub-contractors and their respective facilities to observe this policy. As GAO notes in the report, FISMA requirements are not applicable to researchers and qualified entities because they are not

classified as a federal entity or contractor. All findings , risks, and assessments of HHS systems subject to FISMA requirements are tracked through an electronic Governance, Risk and

Compliance tool; the CMS FISMA Controls Tracking System is the repository used by CMS to manage the security and privacy requirements of its information systems. This platform provides a common foundation to manage standards, controls, risks, assessments and deficiencies across the CMS IT Enterprise.

In addition to the FISMA process outlined above, Medicare Administrative Contractors (MACs) are subject to requirements outlined in the Medicare Prescription Drug, Improvement, and Modernization Act (MMA). The MMA requires MACs to undergo an independent evaluation of their information security program, utilizing standards and guidelines defined by OMB, on an

annual basis. In order to meet both FISMA and MMA requirements, HHS has established two separate annual information security cycles for the MACs. Findings and remediation actions for both processes are tracked through completion in the CMS FISMA Controls Tracking System.

GAO's recommendations and HHS' responses are below.

Recommendation

The Administrator of CMS should develop and distribute guidance for researchers defining minimum security controls and implementation guidance for those controls that is consistent with NIST guidance.

HHS Response

HHS concurs with this recommendation. HHS will consider the impact guidance would have on researchers and after such considerations, evaluate developing and distributing guidance that would define and implement minimum security controls that are consistent with NIST guidance.

Recommendation

The Administrator of CMS should develop processes and procedures to ensure that findings from all MAC assessments are classified consistently and tracked appropriately.

HHS Response

HHS concurs with this recommendation. CMS classifies all findings from both the FISMA and MMA assessments consistently and tracks them through completion. Prior to this GAO review, HHS implemented a process to review, evaluate and risk rank all findings noted at each MAC. This process was implemented to ensure that each finding is risk ranked as consistently and objectively as possible.

Recommendation

The Administrator of CMS should develop processes and procedures to ensure that qualified entities and researchers have implemented information security controls effectively throughout their agreements with CMS.

HHS Response

HHS concurs with this recommendation. HHS is considering implementing processes and procedures that would be necessary to ensure that qualified entities and researchers have implemented information security controls during their agreements with CMS. CMS will consider the impact these processes and procedures would have on qualified entities and researchers while developing them.

# Appendix IV: GAO Contact and Staff Acknowledgments

## GAO Contact

Nick Marinos, (202) 512-9342, MarinosN@gao.gov

## Staff Acknowledgments

In addition to the contact named above, John De Ferrari (assistant director); Thomas Johnson (analyst-in-charge); Chris Businsky, Kavita Daitnarayan, Nancy Glover, Charles Hubbard III, Monica Perez-Nelson, and Richard Sayoc made key contributions to this report.

## GAO's Mission

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

## Obtaining Copies of GAO Reports and Testimony

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

### Order by Phone

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

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

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

## Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: https://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

## Public Affairs

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

## Strategic Planning and External Liaison

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