United States Government Accountability Office

GAO

Report to Congressional Committees

June 2012

PRESCRIPTION DRUG DATA

HHS Has Issued Health Privacy and Security Regulations but Needs to Improve Guidance and Oversight

GAO-12-605

June 2012

PRESCRIPTION DRUG DATA

HHS Has Issued Health Privacy and Security Regulations but Needs to Improve Guidance and Oversight

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-605, a report to congressional committees

Why GAO Did This Study

Prescribing medications and filling those prescriptions increasingly relies on the electronic collection of individuals' health information and its exchange among health care providers, pharmacies, and other parties. While this can enhance efficiency and accuracy, it also raises privacy and security concerns. Federal law establishes the authority for the Secretary of HHS to develop standards for protecting individuals' health information (which includes Medicare beneficiaries) and to ensure that covered entities (such as health care providers and pharmacies) and their business associates comply with these requirements.

The Medicare Improvements for Patients and Providers Act of 2008 required GAO to report on prescription drug use data protections. GAO's specific objective for this review was to determine the extent to which HHS has established a framework to ensure the privacy and security of Medicare beneficiaries' protected health information when data on prescription drug use are used for purposes other than direct clinical care. To do this, GAO reviewed HHS policies and other related documentation and interviewed agency officials.

What GAO Recommends

GAO recommends that HHS issue de-identification guidance and establish a plan for a sustained audit capability. HHS generally agreed with both recommendations but disagreed with GAO's assessment of the impacts of the missing guidance and lack of an audit capability. In finalizing its report, GAO qualified these statements as appropriate.

View GAO-12-605. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

While the Department of Health and Human Services (HHS) has established a framework for protecting the privacy and security of Medicare beneficiaries' prescription drug use information when used for purposes other than direct clinical care through its issuance of regulations, outreach, and enforcement activities, it has not issued all required guidance or fully implemented required oversight capabilities. HHS has issued regulations including the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules to safeguard protected health information from unauthorized use and disclosure. Through its Office for Civil Rights (OCR), HHS has undertaken a variety of outreach and educational efforts to inform members of the public and covered entities about the uses of protected health information. Specifically, OCR has made available on its website guidance and other materials informing the public about the uses to which their personal information may be put and the protections afforded to that information by federal laws. It has also made available guidance to covered entities and their business associates that is intended to promote compliance with the HIPAA Privacy and Security Rules.

However, HHS has not issued required implementation guidance to assist entities in de-identifying personal health information including when it is used for purposes other than directly providing clinical care to an individual. This means ensuring that data cannot be linked to a particular individual, either by removing certain unique identifiers or by applying a statistical method to ensure that the risk is very small that an individual could be identified. According to OCR officials, the completion of the guidance, required by statute to be issued by February 2010, was delayed due to competing priorities for resources and internal reviews. Until the guidance is issued, increased risk exists that covered entities are not properly implementing the standards set forth by federal regulations for de-identifying protected health information.

Additionally, in enforcing compliance with the HIPAA Privacy and Security Rules, OCR has established an investigations process for responding to reported violations of the rules. Specifically, the office annually receives thousands of complaints from individuals and notices of data breaches from covered entities, and initiates investigations as appropriate. If it finds that a violation has occurred, the office can require covered entities to take corrective action and pay fines and penalties.

HHS was also required by law to implement periodic compliance audits of covered entities' compliance with HHS privacy and security requirements; however, while it has initiated a pilot program for conducting such audits, it does not have plans for establishing a sustained audit capability. According to OCR officials, the office has completed 20 audits and plans to complete 95 more by the end of December 2012, but it has not established plans for continuing the audit program after the completion of the pilots or for auditing covered entities' business associates. Without a plan for establishing an ongoing audit capability, OCR will have limited assurance that covered entities and business associates are complying with requirements for protecting the privacy and security of individuals' personal health information.

Contents

Abbreviations

CMS	Centers for Medicare & Medicaid Services
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
MIPPA	Medicare Improvements for Patients and Providers Act of 2008
PHI	protected health information
OCR	Office for Civil Rights
OMB	Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 22, 2012

Congressional Committees

The increasing reliance on electronic processes to deliver health care services has the potential both to improve the quality of care received by patients, including Medicare beneficiaries, and reduce costs. In particular, the process of prescribing medications and filling prescriptions increasingly relies upon the electronic transmission of patient information among health care providers, pharmacies, and other entities. This can make the prescription process more efficient and accurate; however, the transmission and sharing of individuals' personal information raises concerns about protecting the privacy and security of that information.

The capacity of organizations that exchange health information to store and manage a large amount of electronic health information also increases the risk that a breach in security could expose the personal health information of numerous individuals. In recent years, a number of entities—including health plans, hospitals, universities and medical centers—have reported the loss or theft of large amounts of sensitive personal information, such as health information. Such compromises can leave personal health information vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure. For example, the Department of Health and Human Services (HHS) reported that more than 5.4 million individuals were affected by a breach of their personal health information in 2010. While information technology can provide the means to protect the privacy of electronically stored and exchanged health information, the increased risk of inappropriate access and disclosure heightens the importance of implementing adequate privacy protections and security mechanisms in health information exchange systems.

The Medicare Improvements for Patients and Providers Act of 2008 (MIPPA) requires us to report, by September 1, 2012, on prescription drug use data protections.[1] As agreed with committee staff, our specific objective for this report was to determine the extent to which HHS has established a framework to ensure the privacy and security of Medicare

[1]Pub. L. No. 110-275, § 132(c), 122 Stat. 2494, 2527-2531 (July 15, 2008).

beneficiaries' protected health information when data on prescription drug use are used for purposes other than their direct clinical care.[2]

To determine the extent to which HHS has established a framework to ensure the privacy and security of protected health information, we identified the department's responsibilities by reviewing and analyzing the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and its implementing regulations, the Privacy and Security Rules; the Health Information Technology for Economic and Clinical Health Act (HITECH Act); and applicable privacy best practices, such as the Fair Information Practices. To obtain information on the efforts of the department's Office for Civil Rights (OCR) in implementing HIPAA's and the HITECH Act's requirements, we reviewed and analyzed documentation related to OCR's public outreach and guidance efforts, enforcement practices, and HHS rulemakings regarding covered entity and business associate responsibilities and compared those documents to statutory requirements. Further, we interviewed officials from the Centers for Medicare and Medicaid Services (CMS), the Office of the National Coordinator for Health Information Technology, and OCR. To determine the uses of prescription drug use data and the risks associated with the uses of prescription drug data for purposes other than direct clinical care, we interviewed representatives from several covered entities and medical associations, and reviewed academic publications.

We conducted this performance audit from August 2011 through June 2012 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. Our objective, scope, and methodology are discussed in more detail in appendix I.

[2]MIPPA also required us to report on aspects of the Electronic Prescribing Program, which we fulfilled in GAO, *Electronic Prescribing: CMS Should Address Inconsistencies in Its Two Incentive Programs That Encourage the Use of Health Information Technology*, GAO-11-159 (Washington, D.C.: Feb. 17, 2011).

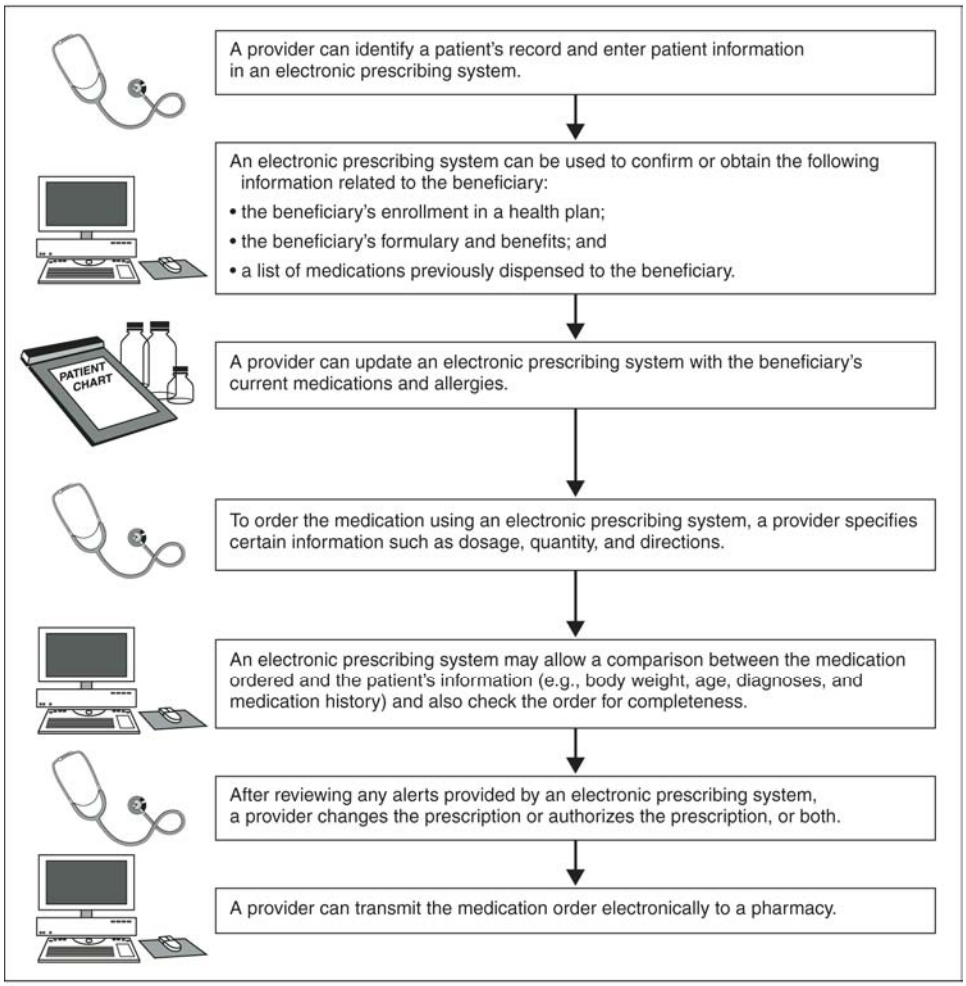
Background

According to HHS, widespread use of health information technology could improve the quality of care received by patients and reduce health care costs. One such technology, electronic prescribing, can be used, for example, to electronically transmit a prescription or prescription-related information between a health care provider and a pharmacy or to provide other technological capabilities, such as alerting a provider to a potential interaction between a drug and the patient's existing medications.

In traditional, or paper-based, prescribing, health care providers that are licensed to issue prescriptions for drugs (e.g., physicians or others licensed by the state) write a prescription, and calling it into or have the patient take that prescription to a dispenser (e.g., pharmacy) to be filled. In contrast, use of an electronic prescribing system consists of a licensed health care provider using a computer or hand-held device to write and transmit a prescription directly to the dispenser. Before doing so, the health care provider can request the beneficiary's eligibility, formulary,[3] benefits, and medication history. Figure 1 illustrates an example of the flow of information during the electronic prescribing process.

[3]A formulary is a list of generic and brand name prescription drugs, grouped by therapeutic class.

Figure 1: Example of Electronic Prescribing Information Flow



Sources: GAO (data); Art Explosion (clip art).

In order to transmit a prescription electronically, multiple entities need to have access to an individual's identifiable health information[4] in an electronic format. Federal laws and regulations dictate the acceptable use and disclosure activities that can be performed with individually identifiable health information, defined as protected health information (PHI).[5] These activities include treatment, payment, health care operations, and—provided certain conditions are met—public health or research purposes. For example, electronic health information can be held by covered entities[6] that perform treatment functions for directly providing clinical care to a patient through electronic prescribing. These covered entities and business associates, such as medical professionals, pharmacies, health information networks, and pharmacy benefit managers, work together to gather and confirm patients' electronic health information for prescribing, such as a beneficiary's eligibility, formulary, benefits, and medication history. To electronically transmit prescription drug data between a health care provider and a pharmacy, an electronic health record[7] can be used to obtain information about the health of an individual or the care provided by a health practitioner.

[4]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.

[5]Protected health information is individually identifiable health information that is transmitted or maintained in any form or medium, and in this report it is used interchangeably with individually identifiable health information.

[6]Covered entities are defined under regulations implementing HIPAA as health plans that provide or pay for the medical care of individuals, health care providers that electronically transmit health information in connection with transactions covered by the regulations, and health care clearinghouses that receive health information from other entities and process or facilitate the processing of that information into standard or nonstandard format for those entities (45 C.F.R. § 160.103).

[7]An electronic health record is a collection of information about the health of an individual or the care provided, including patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports.

In both paper-based and electronic prescribing, information is also provided to the individual's health plan for payment, which would include the identification of the beneficiary, the pharmacy, and the drug cost information. In the case of Medicare beneficiaries' prescription drug data, the information is provided to CMS for Part D payment calculations.[8] Every time a beneficiary fills a prescription under Medicare Part D, a prescription drug plan sponsor must submit a summary record called prescription drug event data to CMS. The prescription drug event data record contains PHI, such as date of birth, the pharmacy that filled the prescription, and the drug dispensed, that enables CMS to make payments to plans. Appendix II provides a summary of the permitted uses and disclosures of PHI.

Prescription Drug Use Information Can Be Used for Purposes Other than Direct Clinical Care

Under certain circumstances, PHI, including prescription drug use information, can be used for purposes not related to directly providing clinical care to an individual. For example, CMS makes Medicare beneficiaries' prescription drug event data available for use in research studies. Release of these elements outside of CMS must be in accordance with its policies and data-sharing procedures. For example, in order to obtain access to this information interested parties must send in an application and submit a user agreement. Table 1 provides other examples of using prescription drug use data for purposes other than directly providing clinical care.

[8]Medicare's Part D provides outpatient prescription drug benefits for Medicare beneficiaries.

Table 1: Examples of Using Prescription Drug Use Information for Purposes Other than Direct Clinical Care

Use	Example
Research	• The American Medical Association created a quarterly newsletter for primary care physicians, called "Therapeutic Insights," that provides treatment guidelines and prescribing data for specific diseases or conditions. Using de-identified prescription drug use information, each newsletter provides a summary analysis of actual treatment practices for specific diseases or conditions (for example, migraines, chronic obstructive pulmonary disease, and Alzheimer's disease).
Healthcare Operations	• Blue Cross Blue Shield of Massachusetts funded and provided prescription drug use data for a study that estimated the quality improvement and savings associated with medication safety alerts as a result of the use of an electronic prescribing system. The study estimated that medication safety alerts prevented an estimated 402 adverse drug events, and resulted in an estimated annual savings of $402,619 due to lower utilization of health care services. • A CVS/Caremark representative noted that the company uses de-identified prescription drug use information to predict future use of prescription drugs to benefit inventory management and delivery services. Further, the representative stated that this type of information can also be useful to retailers, who look at these data for inventory management purposes and to anticipate trends for seasonal treatments (for example, flu shots needed for the winter).
Disclosure for Public Health Activities	• Following Hurricane Katrina, a group of public and private organizations launched ICERx.org (In Case of Emergency Prescription Database), an online resource that provided licensed prescribers and pharmacists caring for disaster victims with secure access to a patient's comprehensive medication history. Information accessible on the website included evacuee prescription history information, including drug name, dosage, quantity, day supply, and the name of the provider who wrote the prescription and the pharmacy that filled it.
Marketing	• An official from Verispan, a company that was considered one of the world's leading providers of information, research and analysis to the pharmaceutical and health care industries, testified that the company advertises the use of de-identified data to identify the prescriptions issued by a prescriber and link them with doctor-identifiable data that then can be used by pharmaceutical companies to directly market to a prescriber.

Source: GAO analysis of entity-provided and publicly available information.

Depending on the nature of the use, the prescription drug use information is used and transmitted in identifiable form or in de-identified format, which involves the removal of PHI (e.g., name, date of birth, and Social Security number) that can be used to identify an individual.

Federal Laws Establish Privacy and Security Protections of Individually Identifiable Health Information Including Prescription Drug Use Information Used for Purposes Other than Direct Clinical Care

Key privacy and security protections associated with individually identifiable health information, including prescription drug information used for purposes other than directly providing clinical care, are established in two federal laws, HIPAA[9] and the HITECH Act.[10]

Recognizing that benefits and efficiencies could be gained by the use of information technology in health care, as well as the importance of protecting the privacy of health information, Congress passed HIPAA in 1996. Under HIPAA, the Secretary of HHS[11] is authorized to promulgate regulations that establish standards to protect the privacy of certain health information and is also required to establish security standards that require covered entities that maintain or transmit health information to maintain reasonable and appropriate safeguards.

HIPAA's Administrative Simplification Provisions[12] provided for the establishment of national privacy and security standards, as well as the establishment of civil money and criminal penalties for HIPAA violations. HHS promulgated regulations implementing the act's provisions through its issuance of the HIPAA rules–the Privacy Rule, the Security Rule, and the Enforcement Rule. The rules cover PHI and require that covered entities only use or disclose the information in a manner permitted by the Privacy Rule, and take certain measures to ensure the confidentiality and integrity of the information and to protect it against reasonably anticipated unauthorized use or disclosure and threats or hazards to its security.

[9]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (codified at 42 U.S.C. §§ 1320d–1320d-8). The HIPAA Privacy and Security Rules were promulgated at 45 C.F.R. Parts 160 and 164.

[10]The HITECH Act was enacted as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act. Pub. L. No. 111-5, Div. A, Tit. XIII, 123 Stat. 115, 226-279 and Div. B, Tit. IV, 123 Stat. 115, 467-496 (Feb. 17, 2009).

[11]HHS is the federal government's principal agency responsible for protecting the health of Americans, including Medicare beneficiaries.

[12]The Administrative Simplification Provisions of HIPAA provided for the establishment of national standards for the electronic transmission of certain health information, such as standards for certain health care transactions conducted electronically and code sets and unique health care identifiers for health care providers and employers.

HIPAA provides authority to the Secretary to enforce these standards.[13] The Enforcement Rule provides rules governing HHS's investigation of compliance by covered entities, both through the investigation of complaints and the conduct of compliance reviews, and also establishes rules governing the process and grounds for establishing the amount of a civil money penalty for a HIPAA violation. The Secretary has delegated administration and enforcement of privacy and security standards to the department's Office for Civil Rights (OCR).

The HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (Recovery Act), is intended to promote the adoption and meaningful use of health information technology to help improve health care delivery and patient care. The act adopts amendments designed to strengthen the privacy and security protections of health information established by HIPAA and also adopts provisions designed to strengthen and expand HIPAA's enforcement provisions.

Table 2 below provides a brief overview of the HITECH Act's key provisions for strengthening HIPAA privacy and security protection requirements.

[13]HIPAA establishes civil money penalties and criminal penalties for violations. 42 U.S.C. §§ 1320d-5-1320d-6. HHS enforces the civil money penalties, while the Department of Justice enforces the criminal penalties. If a complaint is received about a covered entity that describes an action that could be a violation of the criminal provisions of HIPAA, it may be referred to the Department of Justice for investigation.

Table 2: Key HITECH Act Provisions Related to HIPAA Privacy and Security Protection Requirements

Provision area	Description
Civil Money Penalties	Increases the minimum penalty amount for each violation of the HIPAA requirements. These penalties can extend up to $50,000 per violation and up to a maximum amount of $1.5 million for all repeated violations of the same provision in a calendar year.
Breach Notification	Imposes data breach notification requirements to covered entities and business associates for unauthorized uses and disclosures of unsecured PHI.[a]
Business Associate Liability	Requires business associates to comply with certain HIPAA privacy and security protection requirements.
Use and Disclosure of PHI	Prohibits the sale of PHI for purposes such as marketing without a signed authorization from the individual whose PHI is requested.

Source: GAO analysis of the HITECH Act.

[a]The term "unsecured PHI" includes PHI in any form that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through encryption or destruction.

Under the HITECH Act, the Secretary of HHS has significant responsibilities for enhancing existing enforcement efforts, providing public education related to HIPAA protections, and providing for periodic audits to ensure HIPAA compliance.

In implementing the act's requirements, OCR's oversight and enforcement efforts are to be documented and reported annually to Congress. These annual reports provide information regarding complaints of alleged HIPAA violations and the measures taken to resolve the complaints. These reports and other related information are required by the HITECH Act to be made publicly available on HHS's website.

HHS Has a Framework for Protecting Medicare Beneficiaries' Prescription Drug Use Information but Has Not Issued Required Guidance or Implemented Required Oversight Capabilities

In response to requirements set forth in HIPAA and the HITECH Act, HHS, through OCR, has established a framework for protecting the privacy and security of individually identifiable health information, including Medicare beneficiaries' prescription drug use information used for purposes other than directly providing clinical care. This framework includes (1) establishing regulatory requirements, (2) issuing guidance and performing outreach efforts, and (3) conducting enforcement activities to ensure compliance with the rules. However, OCR has not issued required guidance to assist entities in de-identifying individually identifiable health information due to—according to officials—competing priorities for resources and internal and external reviews. Furthermore, although it has recently initiated a pilot audit program, the office has not implemented periodic compliance audits as required by the HITECH Act. Until these requirements are fulfilled, OCR will have limited assurance that covered entities and business associates are complying with HIPAA regulations.

HHS Issued Regulations to Implement Key HIPAA and HITECH Act Requirements for Protecting PHI

The Secretary of HHS issued regulations, such as the HIPAA rules, that implement HIPAA requirements and amendments required by the HITECH Act to govern the privacy and security of individually identifiable health information, known as PHI. These rules establish the required protections and acceptable uses and disclosures of individually identifiable health information, including Medicare beneficiaries' prescription drug use information.

HHS Issued the HIPAA Privacy and Security Rules to Meet HIPAA Requirements

HIPAA provided for the Secretary of HHS to, among other things, (1) issue privacy regulations governing the use and disclosure of PHI and (2) adopt security regulations requiring covered entities to maintain reasonable and appropriate technical, administrative, and physical safeguards to protect the information.

In December 2000, to address the privacy regulation requirement, HHS issued the Privacy Rule.[14] The Privacy Rule regulates covered entities' use and disclosure of PHI. Under the Privacy Rule, a covered entity may not use or disclose an individual's PHI without the individual's written authorization, except in certain circumstances expressly permitted by the

[14]The Secretary of HHS issued the HIPAA Privacy Rule in December 2000, and it was amended in August 2002. The initial compliance date for the HIPAA Privacy Rule was April 2003 for most covered entities.

Privacy Rule. The Privacy Rule reflects basic privacy principles for ensuring the protection of personal health information, as summarized in table 3.

Table 3: Key Privacy Principles in the HIPAA Privacy Rule

Principle	
Uses and disclosures	Limits the circumstances in which an individual's protected health information may be used or disclosed by covered entities and provides for accounting of certain disclosures; requires covered entities to make reasonable efforts to disclose or use only the minimum necessary information to accomplish the intended purpose for the uses, disclosures, or requests, with certain exceptions such as for treatment or as required by law.
Notice	Requires most covered entities to provide a notice of their privacy practices including how protected health information may be used and disclosed.
Access	Establishes individuals' right to review and obtain a copy of their protected health information held in a designated record set.
Security	Requires covered entities to safeguard protected health information from inappropriate use or disclosure.
Amendments	Gives individuals the right to request from covered entities changes to inaccurate or incomplete protected health information held in a designated record set.
Administrative requirements	Requires covered entities to implement a set of administrative requirements, including policies and procedures and workforce training, to ensure compliance with provisions of the Privacy Rule, taking into account their own needs and environment.
Authorization	Requires covered entities to obtain the individual's written authorization for uses and disclosures of protected health information except for certain specified purposes, such as for treatment, payment, and health care operations, or as required by law. Covered entities may choose to obtain an individual's consent to use or disclose protected health information to carry out treatment, payment, or health care operations but are not required to do so.

Source: GAO analysis of the HIPAA Privacy Rule.

The Privacy Rule generally requires that a covered entity make reasonable efforts to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose.[15] Further, the Privacy Rule establishes methods for de-identifying PHI. Under the rule, once identifiers are removed from a data set, it is no longer considered individually identifiable health information and the HIPAA protections no longer apply. De-identification provides a mechanism for reducing the amount of PHI used and disclosed. The Privacy Rule establishes two ways in which PHI can be de-identified. The Safe Harbor Method requires the removal of 18 unique types of identifiers from a data set coupled with

[15]There are exceptions to the "minimum necessary" requirement of the Privacy Rule for certain disclosures for treatment and uses and disclosures required by law.

no actual knowledge that the remaining data could be used to reidentify an individual, either alone or in combination with other information.[16] The expert determination method requires a qualified statistician or other appropriate expert, using generally accepted statistical and scientific principles, to determine that the risk is very small that an individual could be identified from the information when used alone or in combination with other reasonably available information.

In February 2003, to implement HIPAA security requirements for protecting PHI, HHS issued the HIPAA Security Rule.[17] To ensure that reasonable safeguards are in place to protect electronic PHI, including Medicare beneficiaries' health information, from unauthorized access or disclosure, the Security Rule specifies a series of administrative, technical, and physical safeguards for covered entities to implement to ensure the confidentiality, integrity, and availability of electronic PHI. Table 4 summarizes these security safeguards.

[16]The 18 unique types of identifiers are names; all geographic subdivisions smaller than a state (e.g., street address, ZIP code); Social Security numbers; account numbers; device identifiers and serial numbers; biometric identifiers, such as fingerprints and voice prints; telephone numbers; fax numbers; medical record numbers; certificate/license numbers; web uniform resource locators (URLs); full-face photographic images and any comparable images; all dates that are related to an individual (e.g., date of birth, admission); e-mail addresses; health plan beneficiary numbers; vehicle identifiers and serial numbers, including license plate numbers; Internet protocol (IP) address numbers; and any other unique identifying numbers, characteristics, or codes.

[17]45 C.F.R. §§ 164.302-164.318. The initial compliance date for the HIPAA Security Rule was April 2005 for most covered entities.

Table 4: Security Rule Safeguards

Safeguard	Description	Examples
Administrative	Actions, policies, and procedures that manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information.	Security management process Security incident management Security awareness and training Contingency plans
Physical	Measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.	Facility access controls Workstation security Device and media controls
Technical	Technical measures and the policy and procedures for their use that protect the integrity and control access to PHI.	Access controls Audit controls Person or entity authentication

Source: GAO analysis of the HIPAA Security Rule.

The Security Rule, which applies only to PHI in electronic form, states that covered entities have the flexibility to use any security measures that allow them to reasonably and appropriately implement specified standards. Specifically, the rule states that in deciding what security measures are appropriate, the covered entity must take into account elements such as its size, complexity, technical infrastructure, cost of security measures, and the probability and criticality of potential risks to its PHI.

HHS Issued and Amended HIPAA Rules in Response to the HITECH Act

The HITECH Act set additional requirements for the Secretary of HHS and expanded and strengthened certain privacy and security requirements mandated under HIPAA and the HIPAA rules. Specifically, to implement provisions of the HITECH Act, the Secretary was required to (1) issue breach notification regulations to require covered entities and business associates under HIPAA to provide notification to affected individuals and the Secretary concerning the unauthorized use and disclosure of unsecured PHI; (2) establish enforcement provisions for imposing an increased tiered structure for civil money penalties for violations of the Privacy and Security Rules; and (3) extend certain Privacy and Security Rule requirements to business associates of covered entities. Such required activities are intended to strengthen protections for PHI, including Medicare beneficiaries' prescription drug use information.

To implement these provisions of the act, OCR issued two interim final rules[18]—the Breach Notification for Unsecured Protected Health Information Rule,[19] known as the "Breach Notification Rule," and the HITECH Act Enforcement Rule[20]—and has developed a draft rule intended to, among other things, extend the applicability of certain requirements of the Privacy and Security Rules to business associates. OCR issued the Breach Notification for Unsecured Protected Health Information Rule in August 2009. This rule contains detailed requirements for HIPAA-covered entities and business associates to notify affected individuals and the Secretary following the discovery of a breach of unsecured PHI.[21] In addition, in October 2009, OCR issued the HITECH Enforcement Rule, which amends the HIPAA rules to incorporate HITECH Act provisions establishing categories of violations based on increasing levels of culpability and correspondingly increased tier ranges of civil money penalty amounts.

In addition, in July 2010, OCR issued a notice of proposed rulemaking[22] to modify the HIPAA Privacy, Security, and Enforcement Rules to implement other provisions of the HITECH Act. According to the OCR website, the proposed rule is intended to, among other things, make modifications to extend the applicability of certain Privacy and Security Rule requirements to the business associates of covered entities, strengthen limitations on the use or disclosure of PHI for marketing and fundraising and prohibit the sale of PHI, and expand individuals' rights to access their information and obtain restrictions on certain disclosures of protected health information to health plans. According to OCR officials, the proposed rule is currently under review by the Office of Management

[18]An interim final rule is a final rule that has the full force and effect of law; thus, affected parties have an obligation to comply with its requirements. An interim final rule allows stakeholders to submit comments during the public comment period on the areas requested in the interim final rule that the agency will consider before deciding whether to issue a revised final rule or confirm the interim final rule as final.

[19]74 Fed. Reg. 42740 (Aug. 24, 2009).

[20]74 Fed. Reg. 56123 (Oct. 30, 2009).

[21]A breach is generally an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

[22]75 Fed. Reg. 40868 (July 14, 2010).

and Budget (OMB), and OCR officials have not determined an estimated time frame for its issuance.

OCR Provides Guidance and Outreach on the Use of PHI, but Has Not Issued Required De-identification Guidance

The HITECH Act also requires HHS to educate members of the public about how their PHI, which may include Medicare beneficiaries' prescription drug use information, may be used. In addition, the HITECH Act requires HHS to provide guidance for covered entities on implementing HIPAA requirements for de-identifying data—that is, taking steps to ensure the data cannot be linked to a specific individual. Specifically, the act requires HHS to provide information to educate individuals about the potential uses of PHI, the effects of such uses, and the rights of individuals with respect to such uses. In addition—to clarify the de-identification methods established in the HIPAA Privacy Rule—the HITECH Act required OCR to produce guidance by February 2010 on how best to implement the HIPAA Privacy Rule requirements for the de-identification of protected health information.

OCR has undertaken an array of efforts since the rules were issued, as well as to implement the HITECH Act's requirements to promote awareness of the general uses of PHI and the privacy and security protections afforded to the identifiable information. For example, the office has made various types of information resources publicly available.[23] Through its website, the office provides a central hub of resources related to HIPAA regulations, ranging from guidance to consumers on their rights and protections under the HIPAA rules to compliance guidance to covered entities.[24] More specifically, the office has developed resources to guide covered entities and business associates in implementing the provisions of the Privacy and Security Rules, which include, among other things, examples of business associate contract provisions for sharing PHI, answers to commonly asked questions, summaries of the HIPAA rules, and information on regional privacy officers designated to offer

[23]The guidance issued by OCR applies generally to all PHI and the various HIPAA requirements for safeguarding PHI, restricting its use and disclosure, providing individuals their rights with respect to their PHI, and other administrative requirements. As such, the guidance would apply to Medicare beneficiaries' prescription drug use information used for purposes other than direct clinical care.

[24]OCR guidance and educational outreach materials can be found at this site: http://www.hhs.gov/ocr/privacy/.

guidance and education assistance to entities and individuals on rights and responsibilities related to the Privacy and Security Rules.

Table 5 below provides a brief overview of OCR's guidance and education outreach activities in regard to their target audience, purpose, and guidance materials.

Table 5: Overview of OCR's Guidance and Education Outreach Activities

Target audience	Purpose	Guidance materials
General public	To enable the public to be better informed about the uses of PHI and the privacy protections and rights afforded to the public by the HIPAA rules	• Information on individual health information privacy rights • Summaries of the statutory and regulatory protections of PHI • Sharing information with family members and friends • Notices of Privacy Practices • Videos about HIPAA and individual rights available on the OCR YouTube channel
Covered entities/business associates	To promote compliance with the Privacy and Security Rules	• Summaries of the Privacy and Security Rules • Implementation guidance for significant aspects of the HIPAA rules • Presentations related to HIPAA rules • Answers to frequently asked questions • Examples of business associate contract provisions for sharing PHI • Privacy electronic mailing list to inform entities about the release of newly available resources related to health information privacy frequently asked questions, guidance, and technical assistance materials, as well as other announcements

Source: GAO analysis of OCR data.

In another effort to promote awareness, OCR——in conjunction with the Office of the National Coordinator for Health Information Technology[25]—established a Privacy and Security Toolkit to provide guidance on privacy and security practices for covered entities that electronically exchange health information in a network environment. The toolkit was developed to implement the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, also known as

[25]The Office of the National Coordinator for Health Information Technology is a component of the Office of the Secretary of HHS. Its primary focus is on the coordination of nationwide efforts to implement and use health information technology and the electronic exchange of health information.

the Privacy and Security Framework,[26] and includes tools to facilitate the implementation of these practices to protect PHI. Guidance included with the toolkit includes, among other things, security guidelines to assist small health care practices as they become more reliant on health information technology and facts and template examples for developing notices for informing consumers about a company's privacy and security policies in a web-based environment.

Although OCR has initiated these efforts to fulfill its responsibilities to promote awareness of allowable uses and provide guidance for complying with required protections under the HITECH Act, it has yet to publish HITECH Act guidance on implementing HIPAA de-identification methods, which was to be issued by February 2010.[27] OCR officials stated that they have developed a draft of the de-identification guidance, but have not set an estimated issuance date. According to the officials, the draft guidance was developed based on the office's solicitation of best practices and guidelines from multiple venues and forums, including a workshop panel discussion with industry experts in March 2010 that included discussions on best practices and risks associated with de-identifying PHI. The officials stated that guidance will explain and answer questions about de-identification methods as well as clarify guidelines for conducting the expert determination method of de-identification to reduce entities' reliance on the Safe Harbor method.

The issuance of such implementation guidance could provide covered entities—including those that rely on de-identified prescription drug use information for purposes other than directly providing clinical care—with guidelines and leading practices for properly de-identifying PHI in accordance with Privacy Rule requirements. According to OCR officials, competing priorities for resources and internal reviews have delayed the issuance of the guidance. Officials stated that the draft is currently under government wide review. Although officials stated that the guidance will be issued upon completion of the review, no estimated time frame has been set. Until this guidance is issued, increased risk exists that covered

[26]The Privacy and Security Framework is focused on establishing a policy framework for electronic health information exchange that can help guide the nation's adoption of health information technologies and help improve the availability of health information and health care quality.

[27]As previously discussed, de-identification involves the removal of PHI (e.g., name, date of birth, and Social Security number) that can be used to identify an individual.

entities are not properly implementing the standards set by the HIPAA Privacy Rule and that identifiers are not properly removed from PHI.

OCR Conducts Enforcement and Oversight Activities but Has Yet to Implement a Sustained Audit Capability

Federal laws authorize HHS to take steps to ensure that covered entities comply with HIPAA privacy and security requirements targeted toward protecting patient data, including Medicare beneficiaries' prescription drug use information. Specifically, HHS has authority to enforce compliance with the Privacy and Security Rules in response to, among other things, (1) complaints reporting potential privacy and security violations and (2) data breach notifications submitted by covered entities.[28] Furthermore, the HITECH Act increased HHS's oversight responsibilities by requiring the department to perform periodic audits to ensure covered entities and business associates are complying with the Privacy and Security Rules and breach notification standards.[29]

OCR Has Investigated Reported Violations of the Privacy and Security Rules

OCR has developed and implemented an enforcement process that is focused on conducting investigations in response to actions that potentially violate the Privacy and Security Rules. According to OCR officials, the office opens investigations in response to submitted complaints and data breach notifications, as well as conducts compliance reviews based on other reports of potential violations of which the department becomes aware. If necessary, it then requires covered entities to make changes to their privacy and security practices.

[28]The Privacy and Security Rules established the ability for individuals to file complaints with the department if they believed that a covered entity was not complying with a provision of the rules.

[29]Pub. L. No. 111-5, § 13411, 123 Stat. 115, 276.

OCR receives thousands of complaints[30] and breach notifications[31] each year. Officials stated that these complaints and notifications are reviewed to determine if they are eligible for enforcement and require an OCR investigation. According to information provided by OCR, from 2006 to 2010[32] the office has received on average about 8,000 Privacy and Security Rule complaints each year.[33] OCR officials reported that as of February 2012, the office conducted investigations of approximately 24,000 complaints alleging compliance violations of the Privacy or Security Rule, resulting in corrective actions by covered entities in 66 percent of the cases. Corrective actions have included training or sanctioning employees, revising policies and procedures, and mitigating any alleged harm. According to OCR's annual report to Congress on HIPAA Privacy and Security Rule compliance,[34] in instances where an investigation resulted in a determination that a violation of the Privacy or Security Rule occurred, the office first attempted to resolve the case informally by obtaining voluntary compliance through corrective action. Compliance issues investigated most often include impermissible uses and disclosures of PHI and lack of safeguards for or patient access to PHI.

As of May 2012, OCR investigations have resulted in the issuance of a resolution agreement in eight cases. According to OCR officials, a

[30]Complaints present an eligible case for enforcement by OCR if they meet certain criteria: (1) the alleged action must have taken place after April 13, 2003, for a Privacy Rule complaint, and after April 19, 2005, for a Security Rule complaint; (2) the complaint must be filed against an entity that is required by law to comply with the Privacy and Security Rules; (3) a complaint must allege an activity that, if proven true, would violate the Privacy or Security Rule; and (4) complaints must be filed within 180 days of when the person knew or should have known about the alleged violation (OCR may waive this time limit if it determines that there was "good cause" for not submitting the complaint within 180 days).

[31]Data breach notification investigations, according to OCR officials, are initiated for every breach affecting 500 or more individuals; for breaches affecting under 500 individuals, notifications are provided to the regional investigation offices which determine if the breach warrants an investigation.

[32]OCR has received Privacy Rule complaints since April 14, 2003, and Security Rule complaints since October 2009.

[33]The majority of complaints received by OCR were related to potential violations of the Privacy Rule.

[34]U.S. Department of Health and Human Services Office for Civil Rights, "Annual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance For Calendar Years 2009 and 2010," Washington, D.C.: Aug. 11, 2011.

resolution agreement is a formal agreement between OCR and the investigated entity and is used to settle investigations with more serious outcomes. A resolution agreement is a contract signed by HHS and a covered entity in which the covered entity agrees to perform corrective actions (e.g., staff training), submit progress reports to HHS (generally for a period of 3 years), and—in some cases—pay a monetary fine. The eight resolution agreements entered into with the investigated entities all included a payment of a resolution amount, and the development or revision of policies and procedures. In six of these cases further submission of compliance reports or compliance monitoring was required for 2 to 3 years. For example, in response to complaints that several patients' electronic PHI was viewed without permission by university health system employees, OCR initiated an investigation which revealed that unauthorized employees repeatedly looked at the electronic PHI for numerous patients. The university health system agreed to settle potential violations of the Privacy and Security Rules by committing to a corrective action plan and paying approximately $865,000.

When a covered entity does not cooperate with an OCR investigation or take action to resolve a violation, the office also has the authority to impose a civil money penalty. OCR can levy civil money penalties for failure to comply with the requirements of the Privacy Rule, Security Rule, and Breach Notification Rule. For each violation, the maximum penalty amount in four separate categories[35] is $50,000. For multiple violations of an identical provision in a calendar year, the maximum penalty in each category is $1.5 million. As of May 2012, OCR had issued one civil money penalty for noncompliance in the amount of $4.3 million. Since February 2010, pursuant to the HITECH Act, OCR has received and used the money from settlement amounts and civil money penalties for enforcement of the HIPAA rules.

OCR Has Not Developed a Sustained Audit Capability to Evaluate Compliance with Privacy and Security Requirements

In June 2011, OCR initiated efforts to conduct pilot audits of 150 covered entities by the end of December 2012. The office contracted for a private firm to identify the population of covered entities from which to select audit candidates. Additionally, the office contracted with a private audit firm to develop the initial audit procedures for covered entities. These procedures—which OCR documentation asserts are to be in accordance

[35]The four categories of culpability for purposes of imposing civil money penalties are (1) did not know, (2) reasonable cause, (3) willful neglect—corrected, and (4) willful neglect—not corrected.

with generally accepted government auditing standards[36]—are composed of the requirements from the Privacy, Security and Breach Notification Rules, which include protections afforded to prescription drug use information and uses of it for purposes other than directly providing clinical care. In January 2012, OCR officials stated that the target for audits to complete was revised to 115.

According to OCR documentation, during the pilot each audit is conducted based on the following steps:

1. An audit is initiated with the selected covered entity being informed by OCR of its selection and asked to provide documentation of its privacy, security, and breach notification compliance efforts to the contracted auditors.

2. Contracted auditors use the audit procedures developed to assess the compliance activities of the covered entity. According to officials and documentation provided, these procedures correspond to the requirements of the Privacy, Security, and Breach Notification Rules. In this pilot phase, every audit will include a documentation review and site visit.

3. Contracted auditors will provide the audited covered entity the draft findings within 30 days after conclusion of the field work.

4. Audited entities will have 10 days to provide the audit contractor with comments and outline corrective actions planned or taken.

5. Contracted auditors will develop a final audit report to submit to OCR within 30 days of receipt of the comments. The final report will describe how the audit was conducted, what the findings were, and what actions the covered entity is taking in response to those findings as well as describe any best practices of the entity.

According to OCR officials, an initial set of 20 pilot audits was completed by March 2012. Officials stated that these initial audits resulted in the identification of both privacy and security issues at covered entities, such

[36]Audits that are conducted in accordance with generally accepted government auditing standards can provide an independent, objective, nonpartisan assessment of individual entities' compliance with the relevant federal laws and regulations.

as potential impermissible uses and disclosures and not appropriately conducting reviews of audit logs and other reports monitoring activity on information systems. OCR officials stated that the remaining 95 pilot audits, 25 of which were initiated in April 2012, will be completed by the end of December 2012.

However, OCR has yet to establish plans for (1) continuing the audit program once the audit pilot finishes in December 2012 and (2) auditing business associates for privacy and security compliance. According to OCR officials, the dedicated Recovery Act funding for the office's audit effort will expire at the end of December 2012 and officials stated that they have not yet finalized a decision on the future of the program, including the manner in which an audit process will need to be designed to address compliance by business associates.[37] OCR officials stated that the office plans to award a contract in 2012 for a review of the pilot program, including a sample of audits completed during the pilot. OCR officials anticipate that this review will help determine how the office can fully implement an audit function.

Implementing a sustained audit program could allow OCR to help covered entities and business associates identify and mitigate risks and vulnerabilities that may not be identified through OCR's current reactive processes. Furthermore, inclusion of business associates in such a program is important because, according to OCR data, more than 20 percent of data breaches affecting over 500 individuals that were reported to OCR involved business associates. Without a plan for deploying a sustained audit capability on an ongoing basis, OCR will lack the ability to ensure that covered entities and business associates are complying with HIPAA regulations, including properly de-identifying PHI when data on prescription drug use are used for purposes other than directly providing clinical care.

Conclusions

Through its issuance of regulations, outreach, and enforcement activities, HHS has established a framework for protecting the privacy and security of Medicare beneficiaries' prescription drug use information when used

[37]According to OCR officials, business associate compliance was not an element of the pilot program because changes to the regulations to implement the HITECH Act amendments extending liability for compliance to business associates would not be in effect during the period of the audit pilot program.

for purposes other than directly providing clinical care. It has also promoted public awareness on the uses and disclosures of PHI through its education and outreach activities. Further, OCR has established and implemented a process to enforce provisions of the HIPAA Privacy and Security Rules through investigations. However, it has not issued required implementation guidance to assist entities in de-identifying PHI. By not issuing the guidance, increased risk exists that covered entities are not properly implementing the standards set by the HIPAA Privacy Rule and that PHI is not properly stripped of all identifiers that would identify an individual. In addition, OCR has not fully established a capability to proactively monitor covered entities' compliance through the use of periodic audits as required by the HITECH Act. Specifically, OCR has yet to establish plans for a sustained audit capability upon completion of its pilot program at the end calendar year 2012 and has yet to determine how to include auditing business associates. Without a plan for deploying a sustained audit capability on an ongoing basis, OCR will have limited assurance that covered entities and business associates are complying with HIPAA regulations, including whether Medicare beneficiaries' prescription drug use information, when used for purposes other than directly providing clinical care, is being appropriately safeguarded from compromise.

Recommendations for Executive Action

To improve the department's guidance and oversight efforts for ensuring the privacy and security of protected health information, including Medicare beneficiaries' prescription drug use information, we recommend that the Secretary of HHS direct the Director of the Office for Civil Rights to take the following two actions:

- Issue guidance on properly implementing the HIPAA Privacy Rule requirements for the de-identification of protected health information.
- Establish plans for conducting periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and breach notification standards.

Agency Comments and Our Evaluation

In written comments on a draft of the report, the HHS Assistant Secretary for Legislation agreed with our two recommendations, but provided qualifying comments for both. HHS's comments are reprinted in appendix III.

Regarding our recommendation that OCR issue guidance on properly implementing the HIPAA Privacy Rule requirements for the de-identification of protected health information, the Assistant Secretary stated that while the department agrees that issuing the guidance will be helpful to covered entities, the department does not agree that without the guidance, covered entities will have limited assurance that they are complying with the HIPAA Privacy Rule de-identification standards. The Assistant Secretary noted that covered entities have been operating under these existing de-identification standards for almost 10 years and that OCR has not found that the standards have been the subject of significant or frequent compliance issues by covered entities. The Assistant Secretary noted that OCR's purpose in issuing the de-identification guidance was to provide covered entities with the current options and approaches available for de-identifying health information.

We agree that the existing agency information on the de-identification standards provide a level of assurance that covered entities have the parameters and requirements needed to properly remove identifiers from PHI and have clarified this in our report. However, the HITECH Act requires HHS to issue de-identification implementation guidance that addresses how covered entities should implement the de-identification standards. OCR officials stated that the planned guidance will explain and answer questions about de-identification methods as well as clarify guidelines for conducting the expert determination method of de-identification to reduce entities' reliance on the Safe Harbor method. Such information could assist covered entities in determining how to properly implement the de-identification methods. Until such implementation guidance is issued, increased risk exists that covered entities are not properly adhering to the standards set by the HIPAA Privacy Rule and that PHI is not properly stripped of all identifiers that would identify an individual.

Regarding our recommendation that OCR establish plans for conducting periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and breach notification standards, the Assistant Secretary stated the department did not agree with our report's conclusion that without such a plan, OCR will lack the ability to ensure that covered entities and business associates are complying with the HIPAA rules. Specifically, he stated that our conclusion did not adequately take into account the considerable impact of the thousands of complaint investigations, compliance reviews, and other enforcement activities OCR conducts annually to ensure covered entities are complying with the rules. He noted that although the audit

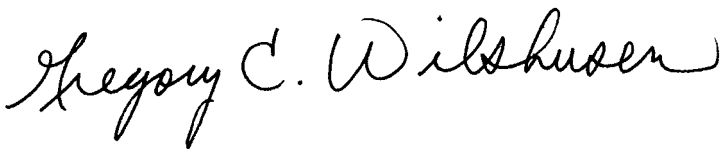
function is a critical compliance tool for identifying vulnerabilities, the importance of the audit function should not be understood to diminish the effectiveness of OCR's other enforcement activities for bringing about and enforcing compliance with the HIPAA rules.

As our report highlighted, OCR has developed and implemented an enforcement process that is focused on responding to actions that potentially violate the Privacy and Security Rules. OCR conducts this reactive process through processing complaints and conducting thousands of investigations each year. An audit program is an important addition to OCR's compliance program as it is a tool to identify vulnerabilities before they cause breaches and other incidents. Without the addition of a proactive process, such as an audit capability, OCR will have limited assurance that covered entities are complying with HIPAA regulations.

HHS also provided technical comments on the report draft, which we addressed in the final report as appropriate.

We will send copies of this report to other interested congressional committees and the Secretary of Health and Human Services. The report will also be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions regarding this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.



Gregory C. Wilshusen
Director
Information Security Issues

List of Committees

The Honorable Max Baucus
Chairman
The Honorable Orrin G. Hatch
Ranking Member
Committee on Finance
United States Senate

The Honorable Tom Harkin
Chairman
The Honorable Michael B. Enzi
Ranking Member
Committee on Health, Education,
Labor & Pensions
United States Senate

The Honorable Fred Upton
Chairman
The Honorable Henry A. Waxman
Ranking Member
Committee on Energy and Commerce
House of Representatives

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

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the extent to which the Department of Health and Human Services (HHS) has established a framework to ensure the privacy and security of Medicare beneficiaries' protected health information (PHI) when data on prescription drug use are used for purposes other than their direct clinical care.

To address our objective, we identified HHS's and its Office for Civil Rights' (OCR) responsibilities for protecting the privacy and security of PHI by reviewing and analyzing the Health Insurance Portability and Accountability Act (HIPAA), including the HIPAA Privacy and Security Rules; the Health Information Technology for Economic and Clinical Health (HITECH) Act; and applicable privacy best practices, such as the Fair Information Practices.

To obtain information on OCR efforts in implementing HIPAA's and the HITECH Act's requirements, we reviewed and analyzed documentation related to the office's public outreach and guidance efforts, enforcement practices, and regulations for covered entity and business associate compliance provided by the office and through the department's website and compared those documents to the office's statutory requirements. To obtain information on the office's enforcement through complaint and breach notice investigations, we interviewed officials, reviewed agency-provided and public information, and analyzed agency documentation. We conducted interviews with OCR officials to discuss the department's approaches and future plans for addressing the protection and enforcement requirements of the HIPAA Privacy and Security Rules that applied to covered entities and business associates. We also analyzed plans and documentation provided by OCR officials that described enforcement and compliance activities for developing an audit mechanism and compared them with requirements for the audit program established in the HITECH Act.

To describe the uses of prescription drug use data for purposes other than directly providing clinical care, we interviewed representatives from several covered entities, business associates, and medical associations, and reviewed the HIPAA Privacy Rule and academic publications.

We conducted this performance audit at the Department of Health and Human Services in Washington, D.C., from August 2011 through June 2012, 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: Key Permissible Uses of Protected Health Information

Permissible use	Description	Example
Treatment	The provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.	A hospital may use protected health information about an individual to provide health care to the individual and may consult with other health care providers about the individual's treatment. A hospital may send a patient's health care instructions to a nursing home to which the patient is transferred.
Payment	The various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.	A hospital emergency department may give a patient's payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its service.
Healthcare Operations	Certain administrative, financial, legal, and quality improvement activities of a covered entity, as defined in the Privacy Rule, that are necessary to run its business and to support the core functions of treatment and payment.	Conducting quality assessment and improvement activities, and case management and care coordination. Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule.
Marketing	With certain exceptions, to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing includes an arrangement between a covered entity and any other entity, whereby the covered entity discloses PHI to the other entity in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. With limited exceptions, such as for face to face communications, the Privacy Rule requires an individual's written authorization before a use or disclosure of his or her PHI can be made for marketing.	Needing an individual's authorization: A health plan sells a list of its members to a company that sells blood glucose monitors, which intends to send the plan's members brochures on the benefits of purchasing and using the monitors. Not needing an individual's authorization: An insurance agent sells a health insurance policy in person to a customer and proceeds to also market a casualty and life insurance policy as well.
Disclosure for Public Health Activities	Covered entities may disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability.	The social services department of a local government might have legal authority to receive reports of child abuse or neglect, in which case the Privacy Rule would permit a covered entity to report such cases to that authority without obtaining individual authorization.
Research	A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. To use or disclose protected health information without authorization by the research participant, a covered entity must obtain either: (1) institutional review board or privacy board waiver of authorization; (2) representations for a preparatory to research activity; (3) representations that the research is on the protected health information of decedents; or (4) a data use agreement[a] with recipient where only a limited data sets[b] is shared.	Approval of a waiver of authorization by an Institutional Review Board or Privacy Board for research, such as for certain records research, when the Board has determined that the use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, and the research could not practicably be conducted without the waiver and without access to the protected health information.

Source: HHS Office for Civil Rights.

[a]A covered entity may always use or disclose for research purposes health information which has been de-identified.

[b]A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual.

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

JUN 7 2012

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

Dear Mr. Wilshusen:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled: "PRESCRIPTION DRUG DATA: HHS Has Issued Health Privacy and Security Regulations but Needs to Improve Guidance and Oversight" (GAO-12-605).

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

Sincerely,

Jim R. Esquea
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "PRESCRIPTION DRUG DATA: HHS HAS ISSUED HEALTH PRIVACY AND SECURITY REGULATIONS BUT NEEDS TO IMPROVE GUIDANCE AND OVERSIGHT" (GAO-12-605)

The Department appreciates the opportunity to review and comment on the draft report. As the draft report indicates, HHS's Office for Civil Rights (OCR) administers the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules, which provide federal privacy and security protections for individuals' identifiable health information and provide individuals with important rights with respect to their health information. OCR, as the enforcement agency, is responsible for ensuring individuals are afforded the rights and protections to which they are entitled under the Rules. To that end, OCR investigates complaints and reports of alleged violations of the Rules and requires health care entities to commit to and implement corrective action where needed to assure compliance. Since the first compliance date in 2003, OCR has conducted investigations into tens of thousands of reports of alleged violations and, through corrective action, has obtained significant results and systemic change that has improved the privacy and security practices of health care entities and the privacy protection of health information for all individuals they serve.

In administering the HIPAA Rules, OCR also conducts extensive outreach and provides guidance to educate both the regulated community about its compliance obligations, as well as health care consumers and the public about their rights. Since 2003, OCR has provided outreach and guidance by publishing on its web site numerous fact sheets and guides, summaries of the HIPAA Rules, hundreds of frequently asked questions, and compliance tools, as well as presented at hundreds of conferences, meetings, and other outreach events. More recently, OCR also has begun to use social media to reach and educate consumers about their rights under the HIPAA Rules. OCR's outreach and guidance development activities are ongoing, particularly as it implements changes to the HIPAA Rules required by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

GAO Report: OCR Provides Guidance and Outreach on the Use of PHI, but Has Not Issued Required De-identification Guidance

The draft GAO report provides that, while OCR has undertaken an array of efforts to provide guidance and outreach, it has yet to publish the guidance required by the HITECH Act on the HIPAA Privacy Rule's de-identification standards. The report concludes that until the guidance is issued, covered entities will have limited assurance they are meeting the HIPAA de-identification standards, and recommends that the Secretary of HHS direct OCR to issue the guidance.

The Department agrees that issuing the De-identification Guidance will provide helpful information for HIPAA covered entities and is committed to publishing the Guidance as soon as possible. The HITECH Act requires that the Department issue the Guidance in consultation with stakeholders and the draft Guidance was developed based on expert input provided to OCR in various forums. As the report indicates, at the current time, the Guidance is undergoing review within the government. More specifically, the draft Guidance has completed review within the

1

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "PRESCRIPTION DRUG DATA: HHS HAS ISSUED HEALTH PRIVACY AND SECURITY REGULATIONS BUT NEEDS TO IMPROVE GUIDANCE AND OVERSIGHT" (GAO-12-605)

Department, and is undergoing review by other agencies with an interest in the subject. The Department expects to issue the guidance as soon as a cleared version is available.

While the Department agrees that issuing the Guidance will be helpful to covered entities, the Department does not agree that without the Guidance, covered entities will have limited assurance they are complying with the HIPAA Privacy Rule de-identification standards. As required by the HITECH Act, the Department is to issue guidance on how best to implement the existing de-identification requirements in the Privacy Rule. Covered entities have been operating under these existing de-identification standards for almost ten years and it has not been OCR's experience in administering the Privacy Rule that the standards have been the subject of significant or frequent compliance issues by covered entities. Further, the Department has previously published answers to questions it has received involving the de-identification standards in its guidance materials for the research community. Accordingly, OCR's purpose in issuing the De-identification Guidance was not to address a particular compliance problem in the regulated community, but rather to provide covered entities with guidance on the current options and approaches available for de-identifying health information.

GAO Report: OCR Conducts Enforcement and Oversight Activities but Has Yet to Implement a Sustained Audit Capability

The draft GAO report provides that while OCR conducts enforcement and oversight activities, it has yet to implement a sustained audit capability and recommends that the Secretary of HHS direct OCR to establish plans for conducting audits to ensure compliance with the HIPAA Rules. The draft report concludes that without a plan for deploying a sustained audit capability on an ongoing basis, OCR will lack the ability to ensure that covered entities and business associates are complying with the HIPAA regulations.

The Department agrees that an audit program will augment OCR's existing HIPAA privacy and security compliance program and is committed to deploying an efficient and effective audit program. The Department also agrees that the audit program could help identify and mitigate risks and vulnerabilities that may not otherwise be identified through OCR's investigations of complaints and breach reports, and compliance reviews. OCR is currently engaged in the necessary first steps towards establishing a sustainable audit capacity and program. OCR has contracted for the development of a comprehensive audit protocol and pilot program, and is in the process of conducting up to 115 audits to be completed by the end of 2012. These pilot audits will test the protocol on a wide range of types and sizes of covered entities. The next step will be to evaluate the effectiveness of the pilot audits, including the protocol and the process that has been developed. As we advised GAO, the outcomes of the evaluation of the pilot audit program will identify requirements needed to fully implement OCR's audit function and will provide other critical information necessary to inform the Department's decision as to how best to establish a sustainable audit program and infrastructure. Once these results are known, the

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "PRESCRIPTION DRUG DATA: HHS HAS ISSUED HEALTH PRIVACY AND SECURITY REGULATIONS BUT NEEDS TO IMPROVE GUIDANCE AND OVERSIGHT" (GAO-12-605)

Department will be able to move forward with the implementation of a sustainable audit program.

The draft GAO report's conclusion that without a plan for a sustained audit program, OCR will lack the ability to ensure that covered entities and business associates are complying with the HIPAA Rules, also does not adequately take into account the considerable impact of the thousands of complaint investigations, compliance reviews, and other enforcement activities OCR conducts annually to ensure covered entities are complying with the Rules. These tools have been the Department's primary enforcement mechanisms for ten years since the initial compliance date of the Privacy Rule and have been effective in bringing about broad and meaningful changes that benefit health care consumers. They will continue to be a central part of OCR's enforcement program, and will become only more effective as OCR leverages the enhanced civil monetary penalty authority created by the HITECH Act. The audit function is a critical compliance tool to identify vulnerabilities before they cause breaches and other incidents and is an important addition to OCR's compliance program The importance of the audit function should not, however, be understood to diminish the effectiveness of OCR's other enforcement activities for bringing about and enforcing compliance with the HIPAA Rules.

3

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact above, John de Ferrari, Assistant Director; Nick Marinos, Assistant Director; Sher`rie Bacon; Marisol Cruz; Wilfred Holloway; Lee McCracken; Monica Perez-Nelson; Matthew Snyder; Daniel Swartz; and Jeffrey Woodward made key contributions to this report.