United States Government Accountability Office

GAO

Report to Congressional Committees

June 2009

PRIVACY AND SECURITY

Food and Drug Administration Faces Challenges in Establishing Protections for Its Postmarket Risk Analysis System

GAO

Accountability * Integrity * Reliability

GAO-09-355

June 2009

PRIVACY AND SECURITY

Food and Drug Administration Faces Challenges in Establishing Protections for Its Postmarket Risk Analysis System

GAO Accountability•Integrity•Reliability

Highlights

Highlights of GAO-09-355, a report to congressional committees

Why GAO Did This Study

The Food and Drug Administration (FDA) is responsible for assessing the safety of certain medical products after approval (a process called postmarket risk surveillance). To this end, the Food and Drug Administration Amendments Act of 2007 required that FDA establish a postmarket risk identification and analysis system based on electronic health data. In May 2008, FDA began its Sentinel initiative, intended to fulfill this requirement. Additionally, the Act established a requirement for GAO to review FDA's planned system. GAO's specific objectives were to (1) describe the current status of FDA's implementation of the Sentinel system and (2) identify the key privacy and security challenges associated with FDA's plans for the Sentinel system. To do so, GAO analyzed available system documentation; reviewed key privacy and security laws, guidance, standards, and practices; and obtained and analyzed the views of privacy and security experts.

What GAO Recommends

GAO recommends that the Commissioner of FDA develop a plan, including milestones, for developing the Sentinel system and for addressing privacy and security challenges. In written comments on this report, FDA agreed with GAO's recommendation, but noted concerns with GAO's representation of the program which FDA stated would lead readers to believe that their protected health information was at risk.

View GAO-09-355 or key components.

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

What GAO Found

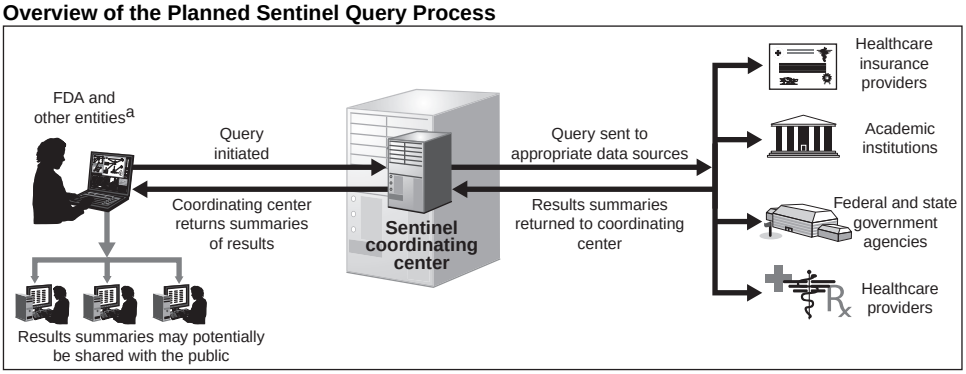
The Sentinel system is still in the early planning stages, with key decisions about development and milestones yet to be made. In planning for Sentinel, FDA has held outreach meetings with stakeholders, established a senior management team to solicit input from agency components; established a working group to share information with federal partners; and sought input from projects involving both public and private sector entities that are meant to refine research approaches and identify challenges and concerns. Although FDA has developed a preliminary design of the Sentinel process for making medical product safety-related queries (see below), key decisions such as developing a governance model for oversight and enforcement of relevant policies, establishing an architecture, and setting privacy and security policies have not yet been made. Further, FDA has not yet developed a plan or set of milestones for when it expects to have these issues addressed.

Because the Sentinel system will rely on sensitive electronic health data, FDA will likely be faced with several significant privacy and security challenges as it continues to develop the Sentinel system including

- ensuring that appropriate legal mechanisms are established to protect privacy and implement security consistently across the Sentinel system;
- defining a clear and specific purpose for the system and ensuring that partners use personal health information only for specified purposes;
- ensuring public involvement and effectively informing the public of the program's planned uses of their personal health information;
- ensuring that de-identified information—data stripped of fields that uniquely identify individuals—is not re-identified;
- establishing adequate security controls to protect the personal health information associated with Sentinel; and
- establishing sufficient oversight and enforcement mechanisms to ensure that privacy and security requirements are consistently implemented.

FDA has yet to develop a plan or set milestones for addressing these challenges.

Overview of the Planned Sentinel Query Process



Source: GAO based on FDA data.

[a] Pharmaceutical companies are potential partners in the system, but may be limited in their capabilities. According to FDA officials, partners in the pharmaceutical industry are not to have access to personal health information but may be provided access to results summaries.

Contents

Abbreviations

CMS	Centers for Medicaid & Medicare Services
eHI	eHealth Initiative
FDA	Food and Drug Administration
FDAAA	Food and Drug Administration Amendments Act of 2007
FISMA	Federal Information Security Management Act of 2002
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
MMA	Medicare Prescription Drug, Improvement, and Modernization Act of 2003
NIST	National Institute of Standards and Technology
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
PIA	privacy impact assessment

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 1, 2009

The Honorable Edward M. Kennedy
Chairman
The Honorable Michael B. Enzi
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate

The Honorable Henry A. Waxman
Chairman
The Honorable John D. Dingell
Chair Emeritus
The Honorable Joe L. Barton
Ranking Member
Committee on Energy and Commerce
House of Representatives

The U.S. Food and Drug Administration (FDA), a component of the Department of Health and Human Services (HHS), has the responsibility to approve medications and certain other medical products for public use and then continue to assess the products' risks and benefits after they have been made available to the public (a process called postmarket risk surveillance). With increased attention to improving the safety and quality of health care, there has been growing interest in leveraging the large amounts of electronic health data being collected on a regular basis to enhance surveillance of postmarket risk.

However, increased analytical use of personal health information raises concerns about the privacy and security of that information. According to the National Research Council, medical information is often the most privacy-sensitive information that individuals provide to others about themselves and protecting the privacy of that information has long been recognized as an essential element in the administration of health care systems. Further, industry groups and professional associations have called for stronger protections for personal health information.

The Food and Drug Administration Amendments Act of 2007 (FDAAA) requires that FDA develop methods for the establishment of a postmarket risk identification and analysis system of electronic health data. In response, FDA announced the start of its Sentinel initiative in May 2008.

The initiative includes planning for the development of an integrated system to analyze electronic health data in order to identify potential risks and assess the safety of medical products after they have been made available to the public.

FDAAA mandated that no later than 18 months after the date of its enactment we (1) evaluate the data privacy, confidentiality, and security issues related to accessing, transmitting, and maintaining data for the FDA Active Postmarket Risk Identification and Analysis System and (2) make recommendations regarding the need for further legislative actions to ensure the privacy, confidentiality, and security of the system or otherwise address privacy, confidentiality, and security issues to ensure the effective operation of the system.

As agreed with your offices, we fulfilled the FDAAA mandate through a briefing provided on March 24, 2009. The specific objectives for our study were to (1) describe the current status of FDA's implementation of the Sentinel system and (2) identify the key privacy and security challenges associated with FDA's plans for the Sentinel system. To address the first objective, we

- analyzed available documentation and plans for system design and development;
- reviewed the statements of work in contracts to assess specific aspects of future Sentinel system development, such as governance structures and data sources;
- reviewed information on current demonstration projects to assess their status and their potential contribution to future Sentinel development; and
- analyzed prior GAO reports to assess prior FDA activities related to postmarket risk evaluation.

To address the second objective, we

- obtained and analyzed the views of privacy and security experts from the World Privacy Forum, the Health Law & Policy Institute, the Health Privacy Project at the Center for Democracy and Technology, and the SANS Institute;
- obtained and analyzed the views of a privacy and information policy consultant;

- obtained and analyzed the views of FDA officials and representatives from related projects;
- analyzed independent studies and previous GAO reports to corroborate challenges identified by experts; and
- analyzed provisions of key privacy and security laws, guidance, standards, and practices with respect to FDA's plans for the Sentinel system and challenges identified by privacy and security experts.

We conducted this performance audit at FDA in the Washington D.C., metropolitan area from May 2008 to May 2009 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.

This report summarizes the information we provided to your staff during our March 24, 2009, briefing, with revisions to reflect information obtained through agency comments. The full briefing, including our objectives, scope, and methodology, can be found in appendix I. In summary, our briefing made the following points:

The Sentinel system is still in the early planning stages, with key decisions about development and milestones yet to be made. FDA has had several outreach meetings with a variety of stakeholders, such as the health care industry and patient and consumer advocacy groups, and has established an FDA senior management team to provide input from various agency components. FDA has also established a working group to share information with federal partners, such as the Department of Veterans Affairs and Department of Defense, and discuss issues related to relevant efforts being carried out by federal agencies, and has sought input from several projects involving both public and private sector entities that are meant to refine research approaches and identify challenges and concerns with launching a large-scale public-private partnership for postmarket surveillance. Because the Sentinel system is still in such an early stage of planning, FDA has yet to make key decisions related to major aspects of program development such as developing a governance model for oversight and enforcement of relevant policies, and establishing an architecture. While FDA has asserted that privacy risks will be reduced because Sentinel participants will not routinely exchange personal health

information, the agency has not yet set policies to ensure the protection of privacy and security. Further, FDA has not yet developed a plan or set milestones for when it expects to have these issues addressed.

In ensuring that the design of the Sentinel system provides adequate privacy and security protections, FDA will likely be faced with several significant challenges. These challenges include

- ensuring that appropriate legal mechanisms are established to protect privacy and implement security consistently across all elements associated with the Sentinel system;
- defining a clear and specific purpose for the system and ensuring that partners with varying interests and business missions use personal health information only for specified purposes;
- ensuring public involvement and effectively informing the public of the program's planned uses of their personal health information and privacy protections that will be applied to it;
- ensuring that de-identified information—data stripped of fields that uniquely identify individuals—is not re-identified and that the use of personal health information in individually identifiable form is minimized and adequately protected;
- establishing adequate security controls to protect the personal health information associated with Sentinel from unauthorized disclosure, modification, and destruction; and
- establishing sufficient oversight and enforcement mechanisms to ensure that privacy and security requirements are consistently implemented across Sentinel's wide range of partners.

FDA has yet to develop a plan or set milestones for addressing these challenges. If these challenges are not adequately addressed, the privacy and security of personal health information could be compromised.

Recommendation for Executive Action

We are not making recommendations for further legislative actions. However, given the significant privacy and security challenges we have identified, we recommend that the Commissioner of FDA develop a plan, including milestones, for developing the Sentinel system and for addressing the privacy and security challenges associated with:

- ensuring consistent application of protections to all Sentinel partners,
- limiting use of personal health information to a clear and specific purpose,
- involving the public in the development of the system and informing the public of the program's planned uses of personal health information and privacy protections,
- using de-identified data,
- establishing adequate security controls, and
- overseeing and enforcing key privacy and security requirements.

Agency Comments and Our Evaluation

In written comments on a draft of this report transmitted by the Acting Assistant Secretary for Legislation at the Department of Health and Human Services, the Acting Commissioner of Food and Drugs stated that protecting the privacy and security of protected health information was of paramount concern to FDA and agreed with our recommendation to develop a plan with milestones for the Sentinel system, noting that this recommendation was consistent with ongoing FDA efforts. The letter is reprinted in appendix II.

In its comments, FDA also raised concerns that the report contained inaccuracies that seriously misrepresent the program and would lead readers to believe that their protected health information was at risk. However, we believe the report accurately characterizes the potential privacy and security risks with the Sentinel program and related analysis. The program is still in its early stages, and while FDA has stated its intention to establish controls for privacy and security, no specific implementation plans have yet been developed. Moreover, FDA officials acknowledged that the concerns raised in our report could be relevant to secondary analysis precipitated by Sentinel. It will be critical that these concerns are fully addressed as FDA moves forward with the Sentinel initiative.

In explaining its position, the agency maintained that transactions that it foresees occurring within the Sentinel program would not pose a risk to protected health information. FDA noted that it envisions developing Sentinel as a distributed network, wherein protected health information would not be exchanged but would remain under the control of its owners and be protected by the controls they already have in place. As

participants in Sentinel, these data owners would separately perform analysis on their own data and share only summaries of their results with other entities. We agree with FDA that its stated intent for conducting basic analysis under Sentinel is designed to minimize risk to privacy, and we believe that this approach, if implemented as FDA envisions it, could reduce privacy concerns. However, we do not believe it is appropriate to focus narrowly on just the transactions that FDA classifies as being within Sentinel, because other related transactions could pose greater risks. Specifically, FDA has acknowledged that there may be a need for secondary analysis based on results obtained through Sentinel, stating that this analysis would occur outside of Sentinel. Such secondary analysis could involve the sharing of protected health information, and many of the concerns raised in our report apply in these circumstances. It will be critical that these concerns are fully addressed as FDA moves forward with the Sentinel initiative.

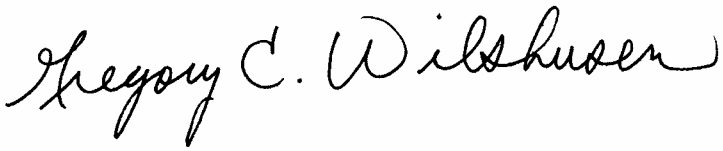
In its comments, FDA also noted that privacy and security are of paramount concern to the agency, and that the agency had engaged with individuals in the privacy and security field to examine privacy and security issues. FDA stated that Sentinel would be subject to the security requirements of the Federal Information Security Management Act of 2002 (FISMA) and would implement policies and procedures to ensure computer security. While FDA's stated commitment to investigating privacy issues and implementing rigorous security controls is important, until specific privacy and security safeguards have been implemented, concerns remain. Further, at this early stage of development, it is important to highlight areas in which potential compromises could occur so that attention can be focused on them. Identifying and assessing such concerns can help better ensure that planning for the system incorporates a comprehensive set of effective privacy and security controls.

Finally, FDA expressed concern that the figure that appears in the Highlights and on page 24 could mislead readers, and it provided an alternate figure with modified labels and alternate illustrations for the elements of the system. We have made adjustments to the labels to address concerns raised by FDA. However, in addition to wording changes, FDA expressed concern that the illustrations in our figure give the impression that Sentinel is a fully automated system that does not include human participation and expertise. We believe the graphic—which portrays individuals, systems, and symbols for institutions—accurately portrays the nature of the Sentinel system, which is expected to include automated systems as well as human and institutional involvement.

In addition, FDA provided technical comments, which we have incorporated as appropriate.

We are sending copies of this report to interested congressional committees and the Commissioner of FDA. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staffs have any questions about 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 III.



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Briefing to Congressional Committees

GAO
Accountability * Integrity * Reliability

Privacy and Security: Food and Drug Administration Faces Challenges in Establishing Protections for Its Postmarket Risk Analysis System

Briefing to Congressional Committees

March 24, 2009

GAO
Accountability * Integrity * Reliability

Contents

2

GAO
Accountability * Integrity * Reliability

Introduction

The Food and Drug Administration (FDA), a component of the Department of Health and Human Services (HHS), has the responsibility to approve medical products for public use and then continue to assess the products' risks and benefits after they have been made available to the public (a process called postmarket risk surveillance). With increased attention to improving the safety and quality of health care, there has been growing interest in leveraging the large amounts of electronic health data being collected on a regular basis to enhance surveillance of postmarket risk.

However, increased analytical use of personal health information[1] raises concerns about the privacy and security of that information. According to the National Research Council, medical information is often the most privacy-sensitive information that patients provide to others about themselves, and protecting the privacy of that information has long been recognized as an essential element in the regulations of health care systems. Further, industry groups and professional associations have called for stronger protections for personal health information.

[1]Personal health information in this briefing refers to information relating to the health or health care of an individual and that identifies, or can be used to identify, the individual.

3

GAO
Accountability * Integrity * Reliability

Introduction

The Food and Drug Administration Amendments Act of 2007 (FDAAA)[2] requires that FDA develop methods for the establishment of a postmarket risk identification and analysis system of electronic health data. In response, FDA announced the start of its Sentinel initiative in May 2008. The initiative includes planning for the development of an integrated system to analyze electronic health data in order to identify potential risks and assess the safety of medical products after they have been made available to the public.

[2]Pub. L. No. 110-85, § 905,121 Stat. 823, 944 (Sept. 27, 2007).

4

GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

FDAAA mandates that no later than 18 months after the date of its enactment we (1) evaluate the data privacy, confidentiality,[3] and security issues related to accessing, transmitting, and maintaining data for the FDA Active Postmarket Risk Identification and Analysis System and (2) make recommendations regarding the need for further legislative actions to ensure the privacy, confidentiality, and security of the system or otherwise address privacy, confidentiality, and security issues to ensure the effective operation of the system.

As agreed with your offices, the objectives for this study were to (1) describe the current status of FDA's implementation of the Sentinel system and (2) identify the key privacy and security challenges associated with FDA's plans for the Sentinel system.

To address the first objective, we

- analyzed available documentation and plans for system design and development;
- reviewed the statements of work in contracts to assess specific aspects of future Sentinel system development, such as governance structures and data sources;
- reviewed information on current demonstration projects to assess their status and their potential contribution to future Sentinel development; and
- analyzed prior GAO reports to assess prior FDA activities related to postmarket risk evaluation.

[3]As confidentiality is a key aspect of information security, it was included under our review of security issues.

5

GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

To address the second objective, we

- obtained and analyzed the views of privacy and security experts on key challenges from the World Privacy Forum, the Health Law & Policy Institute, the Health Privacy Project at the Center for Democracy and Technology, and the SANS Institute;
- obtained and analyzed the views from a privacy and information policy consultant;
- obtained and analyzed the views of FDA officials and representatives from related projects to identify key privacy and security challenges;
- analyzed independent studies and previous GAO reports to corroborate challenges identified by experts; and
- analyzed provisions of key privacy and security laws, guidance, standards, and practices with respect to FDA's plans for the Sentinel system and challenges identified by privacy and security experts.

6

GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

We conducted this performance audit at the Food and Drug Administration in the Washington, D.C., metropolitan area from May 2008 to February 2009, 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.

7

GAO
Accountability * Integrity * Reliability

Results in Brief

The Sentinel system is still in the early planning stages, with key decisions about development and milestones yet to be made. FDA has had several outreach meetings with a variety of stakeholders, such as the health care industry and patient and consumer advocacy groups, and has established an FDA senior management team to provide input from various agency components. FDA has also established a working group to share information with federal partners, such as the Department of Veterans Affairs and Department of Defense, and discuss issues related to relevant efforts being carried out by federal agencies, and it has sought input from several projects involving both public and private sector entities that are meant to refine research approaches and identify challenges and concerns with launching a large-scale public-private partnership for postmarket surveillance. Because the Sentinel system is still in such an early stage of planning, FDA has yet to make key decisions related to major aspects of program development such as developing a governance model for oversight and enforcement of relevant policies, establishing an architecture, and setting privacy and security policies. Further, FDA has not yet developed a plan or set milestones for when it expects to have these issues addressed.

8

GAO
Accountability * Integrity * Reliability

Results in Brief

In designing and developing the Sentinel system, FDA will likely be faced with several significant privacy and security challenges. These challenges include

- ensuring that appropriate legal mechanisms are established to protect privacy and implement security consistently across all elements of the Sentinel system;
- defining a clear and specific purpose for the system and ensuring that partners with varying interests and business missions use personal health information only for specified purposes;
- ensuring public involvement and effectively informing the public of the program's planned uses of their personal health information and privacy protections that will be applied to it;
- ensuring that de-identified information—data stripped of fields that uniquely identify individuals—is not re-identified and that the use of personal health information in individually identifiable form is minimized and adequately protected;
- establishing adequate security controls to protect the personal health information included in Sentinel from unauthorized disclosure, modification, and destruction; and
- establishing sufficient oversight and enforcement mechanisms to ensure that privacy and security requirements are consistently implemented across Sentinel's wide range of partners.

9

GAO
Accountability * Integrity * Reliability

Results in Brief

FDA has yet to develop a plan or set milestones for addressing these challenges. If these challenges are not adequately addressed, the privacy and security of personal health information could be compromised.

We are not making recommendations for further legislative actions. However, given the potential risk to privacy and security, we recommend that the Commissioner of FDA develop a plan, including milestones, for developing the Sentinel system and for addressing the privacy and security challenges associated with ensuring consistent application of protections to all Sentinel partners, limiting use of personal health information to a clear and specific purpose, involving the public in the development of the system, using de-identified data, establishing adequate security controls, and overseeing and enforcing key privacy and security requirements.

In comments on a draft of this briefing provided via e-mail, FDA generally agreed with our recommendation. FDA asserted that privacy and security challenges raised by the use and transfer of personal health information would be largely alleviated by current plans for the Sentinel system—which call for all personal health information to remain with the entities that have custody of it and only analytical results to be shared—but acknowledged that secondary analysis involving personal health information may be necessary and that the privacy challenges we identified would be relevant to such analysis. FDA also noted that its ongoing contracts will help to set achievable milestones.

10

GAO
Accountability * Integrity * Reliability

Background
Postmarket Risk Evaluation

FDA approves medical products for marketing when the agency judges that their known benefits outweigh known risks. After a product has been placed on the market, FDA's practice is to continue to assess its risks and benefits by conducting postmarket evaluation through review of reports of adverse reactions (adverse events) and information from studies of the product, including clinical trials and studies following the use of the product in ongoing medical care (observational studies).

FDA currently relies predominantly on a "passive" form of evaluation to obtain information on adverse events. That is, it is based on data from mandatory reports of adverse drug events submitted by manufacturers, as well as voluntarily submitted information about such events from health care providers and the public. FDA's Adverse Event Reporting System, which captures this information, is the primary means the agency uses to collect information to monitor adverse events. In contrast, Sentinel would present a more "active" system that would enable linking to multiple electronic databases to be queried and analyzed to detect early warning signals of adverse events.

11

GAO
Accountability * Integrity * Reliability

Background
Postmarket Risk Evaluation

According to FDA, active risk evaluation would result in

- utilization of existing electronic databases run by different entities, including private health plans, insurance plans, and government agencies with health care data;
- the possibility of early discovery, or more complete understanding, of adverse events through review of electronic health data, including claims databases;
- the possibility of timelier and more accurate results, based on the rapid review of data on millions of people; and
- the ability to identify important medical product safety questions and develop mechanisms to protect patients in a more timely and efficient fashion.

12

GAO
Accountability * Integrity * Reliability

Background
Postmarket Risk Evaluation

The FDA includes five centers that are responsible for ensuring the safety and effectiveness of different types of products. Three play an important role in the postmarket risk evaluation of medical products:

- The Center for Biologics Evaluation and Research is responsible, among other things, for ensuring the safety and effectiveness of biological products such as vaccines, tissues, and blood products.
- The Center for Devices and Radiological Health is charged with, among other things, ensuring the safety and effectiveness of medical devices.[4]
- The Center for Drug Evaluation and Research is responsible for, among other things, ensuring the safety and effectiveness of all over-the-counter and prescription drugs.

[4]These do not include medical devices used for collecting, processing, testing, manufacturing, and administration of licensed blood, blood components, and cellular products, which are governed by the Center for Biologics Evaluation and Research.

13

GAO
Accountability * Integrity * Reliability

Background
Postmarket Risk Evaluation

As concerns regarding the safety of medical products have increased, calls for improving the ability to monitor the postmarket performance of the products have also grown.

- In 2005, the Secretary of HHS requested that FDA work to improve the agency's ability to track the performance of a medical product during its entire life cycle, recommending, among other things, that the agency explore creating a public-private collaboration and leveraging existing large, electronic databases.
- In 2006, the Institute of Medicine of the National Academies[5] made several recommendations to guide FDA in developing a "more structured way to determine the level of postmarket scrutiny and data requirements, in other words, to match the evaluation of drugs with the way that they will be used in the population."
- In 2006, we issued a report identifying areas needing improvement in FDA's decision-making and oversight process and, among other things, recommended that FDA systematically track postmarket drug safety issues.[6]

[5]The Institute of Medicine was created by the National Academy of Sciences in 1970 to provide advice to the federal government on issues relating to medical care, research, and education.

[6]GAO, *Drug Safety: Improvement Needed in FDA's Postmarket Decision-making and Oversight Process*, GAO-06-402 (Washington, D.C.: Mar. 31, 2006).

14

GAO
Accountability * Integrity * Reliability

Background
Postmarket Risk Evaluation

In 2007, FDAAA mandated that the Secretary of HHS "establish and maintain procedures" for an "active postmarket risk identification and analysis system." Specifically, the act required that the Secretary develop a system that

- provides standardized reporting of data on all serious adverse events;
- provides active adverse event surveillance from federal health-related electronic data, private sector health-related data, and other data deemed necessary by the Secretary to identify adverse events and potential drug safety signals;
- identifies adverse event trends and patterns from the health-related data the system accesses;
- provides reports on a regular basis to the Secretary concerning adverse event trends and patterns, rate of occurrence, and other information the Secretary deems appropriate, which may include data on comparative national adverse event trends; and
- allows the program to export data in a form appropriate for further aggregation, statistical analysis, and reporting.

The act sets the goal of having access to data from 25 million patients by July 1, 2010, and 100 million patients by July 1, 2012.

15

GAO
Accountability * Integrity * Reliability

Background
The Sentinel System

Additionally, the act states that the Secretary shall, not later than 2 years after the date of the enactment, in collaboration with public, academic, and private entities,

- develop methods to obtain access to disparate data sources and
- develop validated methods for the establishment of a postmarket risk identification and analysis system to link and analyze safety data from multiple sources.

In response to the FDAAA call for an active postmarket risk evaluation system, FDA announced in May 2008 the start of its Sentinel initiative, which includes planning for development of a long-term national, integrated, electronic system for monitoring medical product safety. In addition, the planned system is intended to be a mechanism to obtain access to disparate data sources and analyze health care data from multiple sources (see fig. 1).

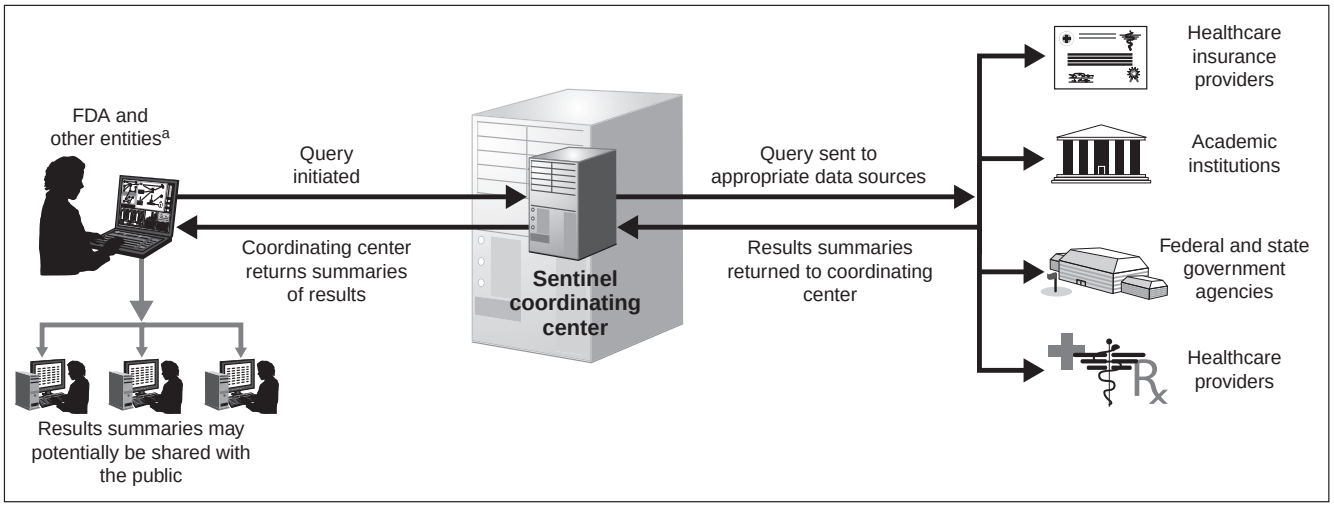
FDA anticipates that users of the planned system would transmit questions through a coordinating center (likely operated by a nonprofit entity) to holders of health data, who would perform analysis of their data and provide responses through the center. FDA currently envisions that its partners would not transfer personal health information as part of their initial responses to Sentinel questions, although officials acknowledge that the results of the responses to queries of this type would in some cases require follow-up involving access to personal health information.

16

GAO
Accountability * Integrity * Reliability

Background
The Sentinel System

Figure 1: Overview of the Planned Sentinel Query Process



Source: GAO based on FDA data.

[a]Pharmaceutical companies are potential partners in the system, but may be limited in their capabilities. According to FDA officials, partners in the pharmaceutical industry are not to have access to personal health information but may be provided access to results summaries.

17

GAO
Accountability * Integrity * Reliability

Background
Fair Information Practices

FDAAA contains provisions requiring FDA to address privacy and security within its postmarket analysis system. Widely accepted guidelines exist for the protection of privacy and security of sensitive information that have driven programmatic requirements for privacy and security.

The Fair Information Practices are a set of privacy protection principles first proposed in 1973 by a U.S. government advisory committee. These principles, with some variation, are used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union. The widely adopted version developed by the Organization for Economic Cooperation and Development (OECD) is shown in the table on the following page.

18

GAO
Accountability * Integrity * Reliability

Background
Fair Information Practices

Table 1: Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: OECD.

19

GAO
Accountability * Integrity * Reliability

Background

Relevant Laws and Guidance

No single federal law governs all use or disclosure of personal information. Instead, there are a number of separate statutes and guidance that provide privacy and security protections for information used for specific purposes or maintained by specific entities.

The Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) set privacy and security requirements for personal health information maintained by certain types of health care organizations, likely including a significant portion of the personal health information held by potential partners in the Sentinel system. The Privacy and Security Rules were intended to protect the privacy and security of individually identifiable health information held by an entity covered by the act.

- The HIPAA Privacy Rule requires covered entities to take such actions as (1) making reasonable efforts to disclose or use only the minimum personal health information necessary; (2) providing notice of privacy practices; (3) assuring individuals the right to review and obtain a copy of their protected health information and request corrections of inaccurate or incomplete data; (4) safeguarding protected health information from inappropriate use or disclosure; and (5) obtaining written authorization or consent for most uses and disclosures of personal health information other than for treatment, payment, and health care operations, or as required by law.

20

GAO
Accountability * Integrity * Reliability

Background

Relevant Laws and Guidance

- The HIPAA Security Rule sets standards for safeguards to protect the confidentiality, integrity, and availability of protected health information in electronic form, including administrative safeguards, such as information access management; physical safeguards, such as facility access controls; technical safeguards, such as transmission security to protect electronic protected health information and control access to it; and standards for contracts and other arrangements with business partners.

The *Privacy Act of 1974* serves as the major mechanism for controlling the collection, use, and disclosure of personally identifiable information within the federal government. The act requires federal agencies to provide safeguards for all information contained in systems of records (any grouping of records containing personal information retrieved by individual identifier) that they maintain. The act also requires agencies to publish notices about these systems of records, which are intended to inform the public of how personal information is collected, maintained, used, and disseminated.

21

GAO
Accountability * Integrity * Reliability

Background

Relevant Laws and Guidance

The *E-Government Act of 2002* requires agencies to conduct privacy impact assessments and would likely have implications for FDA and Sentinel's federal partners. Section 208 of the E-Government Act of 2002 strives to enhance protection of personal information in government information systems by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system.

The *Federal Information Security Management Act of 2002* (FISMA)[7] is the primary law governing information security in the federal government; it addresses the protection of personal information in the context of securing federal agency information and systems. FISMA requires that federal agency information security programs include periodic assessments of risk; policies and procedures that are based on risk assessments; and plans for providing adequate information security for networks, facilities, information systems, or groups of information systems. In addition, FISMA mandates security awareness training; periodic testing and evaluation; a process for planning, implementing, evaluating, and documenting remedial actions; procedures for detecting, reporting, and responding to security incidents; and plans and procedures for continuity of operations for information systems that support the operations and assets of an agency.

[7]FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

GAO
Accountability * Integrity * Reliability

Background
Relevant Laws and Guidance

A number of other laws and regulations also set requirements concerning the privacy and security of personal health information.[8] For example, individual state laws may set constraints and other requirements on the use of personal health information by certain Sentinel partners. These laws include areas such as mental health and HIV/AIDS treatment. For example, Massachusetts state law[9] prohibits the disclosure of HIV/AIDS test results or the identity of the test subject to anyone other than the subject without written authorization.

Finally, the National Institute of Standards and Technology (NIST) established technical guidance and standards used by government, industry, and academia. Key publications relevant to Sentinel include guidance for planning, establishing, and terminating system interconnections;[10] standards for categorizing information and information systems;[11] and minimum security requirements for protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.[12]

[8]The recently enacted Health Information Technology for Economic and Clinical Health (HITECH) Act contains provisions relating to the promotion and testing of health information technology, and privacy and security protections for health information technology. HITECH Act Title XIII, American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (Feb.17, 2009).

[9]Mass. Gen. Laws ch. 111, § 70F.

[10]NIST, *Security Guide for Interconnecting Information Technology Systems*, Special Publication 800-47 (Washington D.C., August 2002).

[11]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standard (FIPS) 199 (Washington D.C., February 2004).

[12]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Washington D.C., March 2006).

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

FDA is in the early stages of planning and developing Sentinel and has yet to make decisions relating to governance, an architecture, data sources, research methodologies, and a privacy and security framework. In addition, FDA has not yet set milestones for development of the system that will support the initiative.

Despite the project's being in such an early planning stage, FDA officials expect to be able to meet milestones established in FDAAA. FDAAA requires that the agency's postmarket risk assessment system will have access to data from 25 million patients by July 1, 2010, and 100 million patients by July 1, 2012. FDA officials have indicated that the involvement of federal partners with large databases of patient records, such as the Centers for Medicaid & Medicare Services, the Department of Defense, and the Department of Veterans Affairs, will allow them to meet this milestone. Additionally, FDAAA requires FDA to develop methods to obtain access to disparate data sources and to establish a postmarket risk identification and analysis system to link and analyze safety data from multiple sources no later than 2 years after the date of the enactment. FDA officials plan to address this requirement by gathering data from supporting projects and issuing contracts to assess specific aspects of future Sentinel system development, such as governance structures and data sources.

24

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

To establish a basic system concept and define preliminary requirements, FDA has completed the following activities:

- Established a senior management team to solicit input from various FDA components on the overall direction of the system. The team has met on a monthly basis to review early progress, including the scope and direction of the system and the results of stakeholder meetings.
- Held outreach meetings with key stakeholders in both the federal and private sectors, including the health care industry, vendors, and patient and consumer advocacy groups. Stakeholders have been asked to provide input on issues such as approaches to data collection, establishing appropriate governance and operational policies, and determining funding sources.
- Created a federal partners working group to share information and discuss issues related to ongoing efforts being carried out by federal agencies that are complementary to Sentinel. This working group includes representatives from the Centers for Disease Control and Prevention, Centers for Medicare & Medicaid Services, National Institutes of Health, Department of Defense, and Department of Veterans Affairs.

25

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

To further define requirements and assess the feasibility of technology options for the system, FDA has obtained input from several non-FDA projects, including the following:

- The eHealth Initiative (eHI) Foundation's Connecting for Drug Safety Collaboration Pilot is exploring opportunities to use electronic clinical information to identify and assess safety signals associated with marketed pharmaceuticals.
- The Centers for Medicaid & Medicare Services (CMS) Project, which is designed to establish an environment to execute queries on Medicare Part D[13] data relating to medical product postmarket risk and surveillance.
- The Observation Medical Outcomes Partnership, a public/private partnership supported by the Foundation for the National Institutes of Health, is initiating a project using data from commercial health information brokers and health care providers to conduct a series of experiments to assess the value, feasibility, and utility of analyzing observational data to identify and evaluate the safety risks and potential benefits of prescription drugs.

[13]The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) established an outpatient drug benefit, known as Medicare Part D, that provides prescription drug coverage for beneficiaries who opt to enroll in the program. Congress designed Medicare Part D to be a market-driven program that promotes competition among private health plans.

26

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

Beyond these early planning efforts, FDA has yet to make a variety of key programmatic decisions that may affect privacy and security. Specifically:

- A governing and operating structure has not yet been established to oversee and enforce policies and procedures among the variety of public and private sector entities that are expected to participate in the system. FDA has contracted with eHI to examine approaches toward potential governance models and to identify and prioritize principles, attributes, and other considerations.
- An architecture has not yet been developed to enable efficient, secure queries of distributed data sources; exchange of relevant product safety information; communications among partners; and transfer and storage of query results. To explore potential models for such an architecture, FDA has contracted with Harvard Pilgrim Healthcare to define and critically evaluate possible database models for use in Sentinel, as well as issues related to policy, performance, privacy and security, benefits to stakeholders, and data standards.

27

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

- Partners in the initiative have not yet been identified. As mandated by FDAAA, the agency intends to develop the Sentinel initiative in collaboration with public, academic, and private-sector entities. Some of these entities will likely also be major sources of data for the system. Neither collaborating partners nor other data sources have yet been identified. To this end, FDA has awarded various contracts including one to Booz Allen Hamilton to identify potential data sources and describe types of electronic health care data. Potential collaborators include federal agencies (such as CMS and the Department of Defense), patient and consumer organizations, health care provider groups, pharmaceutical companies, health plans, insurance companies, and academic institutions.
- Key methodologies for conducting research on adverse drug events have not yet been defined. According to FDA officials, the success of Sentinel will depend largely on the sensitivity, specificity, robustness, and flexibility of the analytical methods it uses. This research is necessary to understand the strengths and limitations of existing methods that might be employed in the system. FDA has contracted with the Group Health Cooperative Center for Health Studies to identify, describe, and evaluate current methods that Sentinel may employ.

28

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

- Finally, a policy framework for the privacy and security of personal health information has not yet been developed. FDA acknowledges the importance of strong privacy and security safeguards, and it is assessing how to implement appropriate protections. As part of its efforts to obtain the views of patients, consumers, and health care professionals regarding, among other things, privacy and security concerns related to the use of personal health information, FDA contracted with eHI to research and analyze existing or proposed policies, rules, regulations, and other requirements related to the protection of privacy and security and recommend strategies for engaging the participation of patients, consumers, and health care professionals.

FDA officials believe additional research and evaluation are needed in these areas and have issued contracts to various entities to address these needs. According to FDA, these contracts were awarded in early fall 2008, and final reports are to be available starting in spring 2009.

29

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

FDA faces a number of key privacy and security challenges as it plans for the development of the Sentinel system.

Consistent application of protections. One major challenge will be ensuring that appropriate legal mechanisms are established to protect privacy and security consistently across all elements of the system, parts of which may be controlled by a variety of partner organizations. The variety of partners creates a complex legal environment in which existing privacy and security requirements may not apply to all participants. If adequate agreements and enforcement mechanisms are not established to ensure that a minimum set of standard requirements is applied consistently, there may be potential gaps in privacy and security protections.

Establishing privacy and security requirements that apply consistently to all entities is key to ensuring that no particular entity with inadequate protections compromises the overall privacy and security of personal health information. In this regard, the National Committee on Vital and Health Statistics[14]—a key advisory committee—has made recommendations in the past aimed at ensuring that HIPAA Privacy Rule protections are applied consistently across all entities handling personal health information.

[14]The National Committee on Vital and Health Statistics was established in 1949 as a public advisory committee that is statutorily authorized to advise the Secretary of HHS on health data, statistics, and national health information policy, including the implementation of health information technology standards.

30

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

Experts have raised concerns that FDA's potential delegation of day-to-day operation of the Sentinel coordinating center to a nonfederal entity may result in legal gaps in privacy and security protections, because such an organization may not meet the definitions for a HIPAA-covered entity and may not be covered by laws such as the Privacy Act and FISMA. Because of what experts viewed as the potential inapplicability of these legal requirements to the entity administering this coordinating center, these experts expressed concern that an appropriate agreement be established between FDA and this entity to ensure that privacy and security requirements are in place.

Further, while FDAAA requires that all Sentinel partners ensure that data are not used in a manner that would violate the HIPAA Privacy Rule, there is no similar requirement that all partners abide by security requirements. Without explicit provisions in individual agreements between FDA and Sentinel partners, potential gaps could occur in applicable security protections. For example, although most health plans or health providers would be covered entities under HIPAA and would have to abide by the HIPAA Security Rule, a pharmaceutical company or an academic institution might not be covered—in this case, such an entity might not have to comply with HIPAA security requirements if these were not stipulated in its agreement with FDA.

31

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

Similarly, concerns have also been raised regarding the enforcement of data use agreements, which specify how personal health information will be used and the safeguards that will be in place to protect its confidentiality. Under the HIPAA Privacy Rule, such agreements are unenforceable by HHS against partners that are not HIPAA-covered entities, and covered entities are not liable for breaches of the data use agreement by the recipients of partially de-identified data. Such agreements are to be the basis for sharing partially de-identified data among Sentinel partners for public health purposes. Again, explicit provisions in individual agreements between FDA and Sentinel partners could address this concern.

Because existing legal requirements for privacy and security are unlikely to apply consistently across potential partners, and the enforceability of the HIPAA Privacy Rule's provisions among partners may be limited, FDA faces the challenge of ensuring that adequate privacy and security controls for the protection of personal health information are appropriately incorporated into cooperative agreements, contracts, and memorandums of understanding so that these protections are applied consistently by all partners throughout the system.

32

GAO
Accountability * Integrity * Reliability

Sentinel Is in the Early Stages of Development

Limiting use to clear and specific purposes. A second challenge FDA faces is defining clear and specific purposes for the use of personal health information for Sentinel, and ensuring that uses are limited to these purposes. Defining a clear and specific purpose may be difficult because of the differing levels of privacy protection defined under HIPAA for different types of uses. Furthermore, because of a wide range of potential users with significantly different missions and the ready availability of large databases of personal health information, FDA faces the challenge of ensuring that uses of data are limited to defined program purposes.

33

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Limiting Use to Clear and Specific Purposes

Establishing a clear and specific purpose and limiting the use and disclosure of personal data to that purpose are key to assuring individuals that their personal information will not be used for unauthorized purposes.

- The purpose specification principle states that the purpose for the collection of personal information should be disclosed before the collection is made and upon any change to that purpose.
- The use limitation principle provides that personal information should not be disclosed or used for other than a specified purpose without consent of the individual or legal authority.
- The HIPAA Privacy Rule also limits the uses and disclosures of an individual's personal health information by covered entities. Specifically, HIPAA requires covered entities to make reasonable efforts to disclose or use only the minimum information necessary to accomplish the intended purpose, with certain exceptions, such as for treatment or as required by law.

34

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Limiting Use to Clear and Specific Purposes

Determining an appropriate set of specific purposes for Sentinel will entail striking a balance between narrow and broad definitions. A purpose that is too narrowly defined may unnecessarily limit the system's usefulness and make it unattractive for private sector data sources to participate. On the other hand, an overly permissive definition may allow partners to use personal health information for inappropriate purposes.

FDAAA directs FDA to collaborate with public, private, and academic entities for the purpose of "advanced analysis of drug safety data." Without additional guidance, this language could be interpreted to encompass a wide range of uses. These allowable uses could fall into different HIPAA categories, with varying requirements for protection.

35

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Limiting Use to Clear and Specific Purposes

It is not yet clear under which HIPAA purpose category Sentinel's postmarket risk evaluation purpose will fall, but it is likely to be included in one of the following categories defined by the HIPAA Privacy Rule:

- Public health activities, which include use and disclosure by a covered entity to public health authorities authorized by law to collect or receive information necessary to prevent or control disease and to entities subject to FDA regulation for adverse event reporting and postmarket evaluation.
  - Disclosure under this category would be permitted without need for further authorization.
- Research, which refers to use and disclosure by a covered entity for any "systematic investigation" that could develop or contribute to generalizable knowledge.
  - Use under this category would require that the covered entity satisfy additional requirements. For example, to use or disclose personal health information for research purposes without need for individual authorization requires that the covered entity receive a waiver or that the covered entity obtain a representation from the researcher that states, among other things, that the use or disclosure of the personal health information is only for preparing a research protocol and that no personal health information will be removed from the covered entity.

36

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Limiting Use to Clear and Specific Purposes

Officials from eHI and privacy experts have stated that establishing how Sentinel's uses appropriately fall into these purpose categories will be difficult because distinctions between public health and research are very subtle. However, as indicated, the decision could have ramifications for the extent of legal requirements in place for protecting personal health information. For example, there may be ambiguities relating to authorization and individual consent, which are treated differently depending on the category.

37

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Limiting Use to Clear and Specific Purposes

In addition, privacy experts have expressed concern that the variety of public and private organizations and business missions involved in the project could make it difficult to effectively limit the use of the personal health information to postmarket risk evaluation. Sentinel, as currently planned, is expected to encompass millions of health records; access to this large amount of data could be very useful for analyses or other uses that go beyond assessing postmarket drug safety. For example, commercial users may seek to use the data for purposes such as marketing campaigns or tracking patient medical product usage and physicians' prescription patterns. Further, academic users may wish to publish data they have used to support their research results. Uses such as these may be inappropriate and could have the potential to compromise patient privacy if not effectively controlled.

As we previously reported in our 2006 report on the use of commercial data, consolidating large databases poses the risk that the use of data goes beyond the original system scope and intended uses.[15] Sentinel could face this risk if the program seeks to bring together disparate, large databases of personal health information to be analyzed by multiple entities.

[15]GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington, D.C.: Apr. 4, 2006).

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Limiting Use to Clear and Specific Purposes

Similarly, in 2007, we raised concerns about the risks associated with the availability of large amounts of aggregated data in our review of a planned data-mining program at the Department of Homeland Security.[16] We stated that with the ability to facilitate a broad range of potential queries and analyses and aggregate large quantities of previously isolated pieces of information, the program could produce aggregated, organized information that organizations could be tempted to use for purposes beyond that originally specified when the information was collected.

If adequate precautions are not taken to limit secondary uses of data, there is increased risk that personal health information may be used for purposes not intended for Sentinel.

[16]GAO, *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks*, GAO-07-293 (Washington, D.C.: Feb. 28, 2007).

39

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Ensuring public confidence. A third challenge that FDA faces is to build public trust through mechanisms that will ensure public involvement and also appropriately inform the public of the program's planned uses of their personal health information as well as the privacy protections that will be applied to it.

Regarding public involvement, privacy experts acknowledge that it would be extremely difficult or impractical to obtain individual consent for Sentinel's planned use of personal health information, given the vast number of records involved and the need for timely results. Further, HIPAA specifically allows for the use of such information without individual consent or authorization for purposes of promoting public health.

This may lead to some instances of uses of personal health information that individuals may find objectionable. FDA has acknowledged that risk and is trying to ensure that the public's concerns are adequately addressed through public meetings and the creation of a transparent, inclusive process for the development of the system. Other mechanisms for public involvement in the development of the system could include adding privacy advocates and representatives of consumer organizations to governing boards to ensure that matters of public concern are raised and addressed.

40

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Ensuring Public Confidence

With regard to informing the public of the program's planned uses of personal health information, the fair information practices and the HIPAA Privacy Rule generally require some mechanism for informing individuals about how personal information is to be used and protected:

- The openness principle states that the public should be informed about privacy policies and practices, and that individuals should have ready means of learning about the use of personal information.
- The HIPAA Privacy Rule requires that most covered entities provide a notice of their privacy practices. In addition to describing types of uses and disclosures, the notice, among other things, must also state the covered entity's duties to protect privacy and individuals' rights.

In addition to informing individuals of what steps an entity is taking to protect the privacy of the personal information, privacy notices also help to ensure an organization's accountability for its stated policies.

41

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges
Ensuring Public Confidence

According to experts, it may be difficult to develop a privacy notice that is at a level of detail that appropriately informs all segments of the public about the privacy protections in place for Sentinel, as well as promotes a clear understanding of how their personal health information is being used. They cited previous experience with privacy notices—such as those required of financial institutions by the Gramm-Leach Bliley Act—which have been difficult for consumers to read and understand.

In prior work, we have highlighted the use of a layered approach to creating privacy notices in order to improve comprehension. For example, we stated that at one layer, the notice could provide a brief description of the information required, the primary purpose for the collection, and associated uses and sharing of such data. A second layer could include additional details about the system or program's uses and the circumstances under which data could be shared.[17] Using a layered approach to privacy notices could enhance effectiveness in communicating with individual patients.

[17]GAO, *Privacy: Alternatives Exist for Enhancing Protection for Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).

42

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges
Ensuring Public Confidence

The many sources and large number of records involved also suggest that multiple channels of communication may be needed to ensure that as many individuals as possible are informed.

For example, in addition to publishing a notice in the *Federal Register* as required by the Privacy Act or a privacy impact assessment as required by the E-Government Act, other communication methods may be useful, including disseminating information through a central Web site, developing a publication on Sentinel privacy measures, developing notices for health care providers and other collaborating partners and/or data sources to use when they collect personal health information, and conducting outreach to consumer and public advocacy groups.

Without ensuring transparency into Sentinel's privacy policies and procedures, FDA may risk losing the public's confidence in its ability to protect their personal health information.

43

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Mitigating risks associated with de-identified data. A fourth challenge FDA faces is ensuring that de-identified data—which it plans to use in most cases when presenting the results of Sentinel analysis—is not used to re-identify individuals, as may be possible in certain circumstances. Further, in cases in which de-identified data may not be sufficient to fulfill program goals, FDA faces the challenge of ensuring that disclosure of personally identifiable health information is limited, monitored, and controlled.

De-identification is the process of stripping data of fields that uniquely identify individuals. According to the Privacy Rule, information is de-identified when the data fields are insufficient to identify an individual and when there is no reasonable basis to believe that the data can be used to re-identify an individual. According to the Privacy Rule, de-identification can be achieved by stripping out fields that uniquely identify individuals, including

- names,
- geographic subdivisions smaller than a state,
- Social Security numbers, and
- dates of birth.

44

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Mitigating Risks Associated with De-identified Data

HIPAA also allows covered entities to use an expert opinion to determine whether data have been de-identified. Under the Privacy Rule, once data have been successfully de-identified using an approved method, those data can be used and disclosed freely without being subject to the privacy rule.

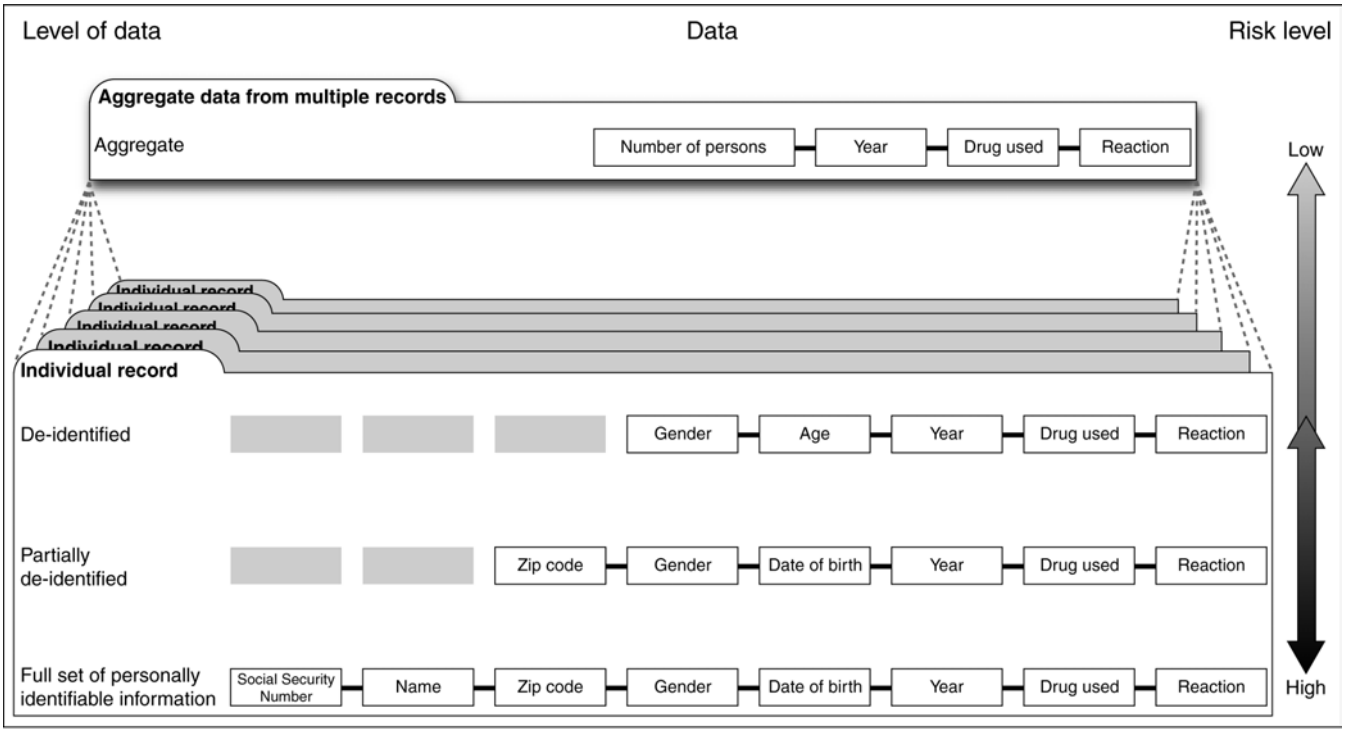
Various levels of de-identification are possible, and the risk of re-identification varies accordingly (see fig. 2). FDA officials have stated that their plan is to provide analytical results using only summary information known as aggregate output data, the least risky type of de-identified data. Experts generally agree that there is reduced risk of re-identification when this type of data is used. However, ensuring that de-identified data are not re-identified when disclosed to outside entities will pose challenges for FDA because useful analysis may require that riskier levels of de-identified data be used.

45

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges
Mitigating Risks Associated with De-identified Data

Figure 2: Levels of De-identified Data



Source: GAO analysis of industry and FDA data.

46

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges
Mitigating Risks Associated with De-identified Data

However, the eHI project has found that aggregate data are often not useful as a research tool and that "limited data sets," which include some identifying information, are often needed instead. Such data sets pose increased privacy risks because it may be possible to combine data fields in these limited data sets with other publicly available data to re-identify individuals. For example, according to published research by an expert in the field, 87 percent of individuals are uniquely identifiable given their gender, ZIP code, and date of birth.[18]

Because of the significant risk of re-identification, the use of certain methods of de-identifying data, such as limited data sets, may require additional controls to mitigate risks. Actions to reduce the risk of re-identification could include

- using the least identifiable form of data to respond to queries,
- ensuring that contractual requirements prohibit recipients from re-identifying individuals and ensuring that individuals are not contacted or their personal health information otherwise disclosed, and
- establishing enhanced security controls to protect the data from inadvertent disclosure, given the risk of re-identification.

[18]L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5 (2002).

47

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Mitigating Risks Associated with De-identified Data

According to FDA officials, while de-identified data may provide all necessary information for a majority of information queries, there are instances in which users may require access to personally identifiable health information to fully process query requests. For example, users may require personal health information to

- independently verify and validate certain results or perform targeted follow-up on a particular query or
- track individuals across de-identified output or aggregate results from various data sources in order to minimize double counting and produce more accurate query results.

Providing partners access to personally identifiable health information introduces significant privacy and security risks that would likely require increased protection measures and oversight. Such measures could include

- monitoring and strictly limiting disclosure of personally identifiable health information to where there is a justified need and
- establishing stringent procedures for protecting the privacy and security of sensitive personally identifiable health information when such disclosure occurs between partners.

If these challenges are not addressed, individuals' sensitive health information could be inappropriately disclosed, and individuals' privacy could be compromised.

48

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing comprehensive security controls. FDA faces the challenge of determining the appropriate security controls that Sentinel will need to protect personal health information from loss or unauthorized disclosure to the extent that it is transferred between Sentinel partners. In doing so, FDA will need to establish a uniform set of security controls for all of its partners to ensure that potential weaknesses in controls at partner systems do not place personal health information in Sentinel at unnecessary risk of unauthorized disclosure, use, modification, or destruction. Such controls will need to demonstrate that the security of personal health information is protected both at rest and in transmission among Sentinel and its partners.

Safeguarding personal health information is critical because its loss or unauthorized disclosure can lead to serious adverse consequences for individuals. The confidentiality of personal health information could be threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information.

49

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges
Establishing Comprehensive Security Controls

Through its planned distributed network of public and private partners, Sentinel queries may involve the exchange of electronic health information among partners in the public and private sector when secondary analysis is required. Although FDA does not anticipate that electronic health information will be routinely exchanged among partners, the large number of potential partners could provide many potential access points through which sensitive information could be compromised. Given this risk, FDAAA mandates that personal health information not be revealed in disclosing the results of analysis of drug safety signals and trends or responding to inquiries regarding drug safety signals and trends.

A basic objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing access controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and the disruption of service. Such controls include protecting the physical boundary around a set of information resources, assigning unique user accounts to specific users to distinguish one user from another, and employing cryptography such as encryption to prevent unauthorized access to computing resources, programs, and information.

50

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing Comprehensive Security Controls

Information security risks to the system could originate from within the system itself as well as from its partners. Within the system, inadequate security controls could lead to loss or disclosure of sensitive information. For example, if the system fails to ensure that controls adequately protect external and internal boundaries, that users are identified and authenticated, and that appropriate levels of encryption are consistently applied to protect sensitive data, there may be increased risk that individuals could gain unauthorized access to personal health information.

51

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing Comprehensive Security Controls

Security risks could arise among Sentinel partners if their systems do not contain adequate security controls and personal health information is inadvertently disclosed, either from partner systems or while that information is being transmitted from one system to another.

- As previously reported,[19] the aggregate effect of inadequate access controls and weaknesses in other system controls places information and information systems supporting a larger system (such as Sentinel) at increased risk of unauthorized disclosure, use, modification, or destruction, possibly without detection. These weaknesses increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information—including personally identifiable information—on supporting systems.

[19]GAO, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program*, GAO-07-870 (Washington, D.C.: July 13, 2007).

52

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing Comprehensive Security Controls

- Additionally, according to NIST,[20] interconnecting information technology systems can expose the participating organizations to risk. If the interconnection is not properly designed, security failures could compromise the connected systems and the data that they store, process, or transmit. Similarly, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system and its data.

If appropriate security controls are not implemented and maintained within the system and among Sentinel partners, there is increased risk of unauthorized disclosure, use, modification, or destruction of personal health information.

[20]NIST, *Security Guide for Interconnecting Information Technology Systems*, Special Publication 800-47 (Washington, D.C.: August 2002).

53

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing oversight and enforcement. Finally, concerns about the wide range of expected Sentinel partners as well as the authority that a nonprofit entity would have over these entities highlight the challenge that FDA will face in creating and implementing an effective oversight and enforcement mechanism to ensure, among other things, the privacy and security of personal health information maintained by Sentinel.

Oversight and enforcement are key mechanisms for ensuring that security and privacy controls are consistently implemented and effective at mitigating risks. For example, federal agencies are subject to oversight, as required by FISMA.[21] FISMA states that continuous monitoring of security controls is a key part of managing enterprise risk and maintaining an accurate understanding of security risks. Additional oversight is applied through reporting requirements to the Office of Management and Budget (OMB) and the Congress. In setting annual reporting requirements, OMB has directed agencies to provide details regarding their privacy protections for personally identifiable information as well as information security measures. An effective oversight and enforcement program is also consistent with the accountability principle, which states that individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of the fair information practices.

[21]FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing Oversight and Enforcement

The wide range of partners expected in Sentinel creates an oversight and enforcement challenge for FDA. FDA has previously used a variety of mechanisms, including cooperative agreements and memorandums of understanding, to establish collaborative relationships with various members of the public and private sector. Similarly, Sentinel will likely require a range of contractual arrangements with its many partners.

An official with the Observation Medical Outcomes Partnership—one of the projects that is informing Sentinel's planned development—said that different contractual arrangements were needed depending on the type of data in use and the partner performing the analysis. Additionally, FDA has indicated that some organizations may choose to provide data to Sentinel via secondary contracts with Sentinel partners rather than belonging to the partnership themselves; such relationships would require different contractual arrangements. Further, some partners may restrict access to the data sets they own, requiring the ability to choose whether to respond to individual queries.

55

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing Oversight and Enforcement

Factors such as these could complicate FDA's ability to establish a comprehensive oversight and enforcement mechanism. Agreements will likely need to include provisions requiring strict adherence to established security and privacy standards. However, beyond stating such requirements consistently, it may not be possible for FDA to establish the same enforcement and oversight mechanisms for all of its partners.

56

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing Oversight and Enforcement

In addition, it is unclear what authority the nonprofit entity that is expected to operate the coordinating center will have over Sentinel partners, as FDA has not yet determined which nonprofit entity, if any, will be responsible for this function. One possible entity under consideration by FDA is the Reagan-Udall Foundation, established by FDAAA to advance the mission of the FDA and enhance product safety, among other things.

- Under FDAAA, the Reagan-Udall Foundation is authorized to award grants to or enter into contracts, memorandums of understanding, or cooperative agreements with a wide range of entities, including public-private partnerships, academic institutions, and industry, to advance its goals and priorities.
- FDAAA requires the foundation to establish a Board of Directors whose duties include establishing policies for the execution of memorandums of understanding and cooperative agreements between the foundation and other entities.

57

GAO
Accountability * Integrity * Reliability

FDA Faces Privacy and Security Challenges

Establishing Oversight and Enforcement

Experts have raised concerns with designating Reagan-Udall to implement key Sentinel functions because most of the funds for the foundation's operations are expected to originate from private industry. Under these circumstances, it may be difficult to ensure that security and privacy requirements are strictly enforced. Thus far, budget provisions have directed FDA to withhold funds from Reagan-Udall.

If adequate oversight and enforcement mechanisms are not in place, privacy and security requirements may not be appropriately implemented by all partners, potentially placing personal health information at increased risk.

While FDA officials acknowledge that they face privacy and security challenges and have taken steps to begin exploring these issues, they have not yet established a plan or milestones for fully addressing them and incorporating the results into the development of Sentinel.

58

GAO
Accountability * Integrity * Reliability

Conclusions

The Sentinel system is still in the early stages of development. FDA has made progress in laying the groundwork for establishing the system, but many critical decisions remain to be made, including decisions about how the project is to be managed, who its many partners will be, and what privacy and security controls will be implemented. FDA has not yet established a plan or milestones for development of the system or for making these critical decisions.

Although personal health information is not expected to be exchanged as part of most routine Sentinel operations, FDA will face a number of privacy and security challenges in developing the system, including (1) applying protections consistently, (2) limiting use of personal health information to a clear and specific purpose, (3) ensuring appropriate public involvement, (4) mitigating risks associated with de-identified data, (5) establishing comprehensive security controls, and (6) establishing oversight and enforcement mechanisms. FDA has yet to develop a plan, including milestones, to address these challenges. Until challenges are addressed, concerns are likely to remain that the Sentinel initiative may not be fully addressing risks to the privacy and security of personal health information.

59

GAO
Accountability * Integrity * Reliability

Recommendation for Executive Action

We are not making recommendations for further legislative actions. However, given the privacy and security challenges we have identified, we recommend that the Commissioner of FDA develop a plan, including milestones, for developing the Sentinel system and for addressing the privacy and security challenges associated with

- ensuring consistent application of protections to all Sentinel partners,
- limiting use of personal health information to a clear and specific purpose,
- involving the public in the development of the system and informing the public of the program's planned uses of personal health information and privacy protections,
- using de-identified data,
- establishing adequate security controls, and
- overseeing and enforcing key privacy and security requirements.

60

GAO
Accountability * Integrity * Reliability

Agency Comments and Our Evaluation

In comments on a draft of this briefing provided via e-mail by the GAO Coordinator of the HHS Office of the Assistant Secretary for Legislation, FDA generally agreed that there are many privacy and security challenges related to the Sentinel initiative and that attention will need to be paid to computer security with respect to the transmission of queries and summaries of results. However, FDA asserted that privacy and security challenges raised by the use and transfer of personal health information would be largely alleviated by current plans for the Sentinel system, which call for all personal health information to remain with the entities that have custody of it and only analytical results to be shared. FDA acknowledged that secondary analysis involving personal health information may be necessary and that the privacy challenges we identified would be relevant to such analysis, but stated that this analysis would likely take place outside the bounds of the Sentinel system.

GAO
Accountability * Integrity * Reliability

Agency Comments and Our Evaluation

Regardless of whether secondary analysis using personal health information is within the bounds of the Sentinel system, such analysis remains a key element in an overall assessment of the data privacy, confidentiality, and security issues related to accessing, transmitting, and maintaining data for FDA's postmarket risk identification and analysis system. Any analysis involving the transfer of personal health information could introduce significant privacy and security risks, and would thus require privacy and security protections and oversight commensurate to this increased risk. Thus the privacy and security challenges we have identified remain of critical importance as planning for the Sentinel system moves forward.

FDA generally agreed with the recommendation made in this briefing, with the exception of the challenge associated with using de-identified data. Regarding this challenge, FDA asserted that activities involving the disclosure of personal health information would be outside the scope of the Sentinel system. However, as previously discussed, the use and disclosure of personal health information through secondary analysis is also an important consideration, and in this regard the challenge associated with using de-identified data will need to be addressed to ensure that risks to the privacy and security of personal health information are fully addressed.

FDA also provided technical comments, which we incorporated into the briefing as appropriate.

Appendix II: Comments from the Food and Drug Administration

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

MAY 19 2009

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

Dear Mr. Wilshusen:

Enclosed are comments on the U.S. Government Accountability Office's (GAO) report entitled: Privacy and Security: Food and Drug Administration Faces Challenges in Establishing Protections for its Postmarket Risk Analysis System (GAO-09-355).

The Department appreciates the opportunity to review this report before its publication.

Sincerely,

Barbara Pisaro Clark

Barbara Pisaro Clark
Acting Assistant Secretary for Legislation

Attachment

DEPARTMENT OF HEALTH & HUMAN SERVICES

Food and Drug Administration
Silver Spring, MD 20993

DATE: May 15, 2009

TO: Acting Assistant Secretary for Legislation

FROM: Acting Commissioner of Food and Drugs

SUBJECT: FDA's General Comments to GAO's Draft Report Entitled, *Privacy and Security—Food and Drug Administration Faces Challenges in Establishing Protections for its Postmarket Risk Analysis System (GAO-09-355)*

FDA is providing the attached general comments to the U.S. Government Accountability Office's draft report entitled, *Privacy and Security--Food and Drug Administration Faces Challenges in Establishing Protections for its Postmarket Risk Analysis System (GAO-09-355).*

FDA appreciates the opportunity to review and comment on this draft report before it is published.

Joshua M. Sharfstein, M.D.
Principal Deputy Commissioner
Acting Commissioner of Food and Drugs

Attachment

FDA's General Comments to the U.S. Government Accountability Office's Draft Report, *Privacy and Security – Food and Drug Administration Faces Challenges in Establishing Protections for its Postmarket Risk Analysis System (GAO-09-355)*

The Food and Drug Administration (FDA) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report, and we agree with GAO's overall recommendation to develop a plan (with multiple milestones), which is completely consistent with ongoing FDA efforts. However, we are very concerned that the report contains inaccuracies that seriously misrepresent the program and will lead readers of the report, especially patients and consumers, to believe that their protected health information[1] is at risk. These inaccuracies most likely result from a fundamental misunderstanding of how phase 1 Sentinel will be implemented. We would like to provide you with some key clarifications.

Phase 1[2] of Sentinel

As explained in the Sentinel report and in most every summary of the initiative or discussion of Sentinel, we have emphasized that FDA is working towards establishing a ***distributed network***. This means that no protected health information will be transferred to the agency. In fact, no protected health information will be transferred at all. All health information will remain under the control of current data owners, behind existing firewalls, protected by privacy and security safeguards. Participating data owners will continue to manage their data protected in their secure environment. Those data owners who wish to participate in Sentinel will perform data searches and analyses of their own data upon request and submit only summaries of their findings as part of Sentinel. To reiterate, data from individual data holders will not be centralized or aggregated in any way into a common database.

Privacy and Security

Protecting the privacy and security of protected health information, as well as the security of all information FDA receives, is of paramount concern to FDA and part of FDA's ongoing responsibilities as it fulfills its mission to protect public health. We work every day to protect the security of the data we receive. Thus, from the beginning of this program, we have sought to engage thought leaders in the privacy and security field at every juncture. One of the first contracts we let under the initiative involved the identification and analysis of potential privacy issues that might need to be addressed. (This report is complete and has been posted on FDA's Sentinel Web site.)

We understand that there may well be a need for further studies of signals obtained through Sentinel. However, the Agency's expects that such studies would take place outside of Sentinel in precisely the same manner that we investigate public health concerns today. For example, an

[1] The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information *"protected health information (PHI)*. See http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

[2] We refer to the initial roll out of Sentinel as *phase 1*, recognizing that as the availability of electronic health records increases, coupled with advances in data standards development, Sentinel will necessarily evolve.

analysis might be carried out pursuant to a contract between FDA and an individual data holder. In such a case, privacy challenges such as those identified in the GAO report could become relevant within the framework of this specific contractual agreement, but would not involve Sentinel. If protected health information were to be transmitted by a participating data holder for analysis at any point, including during a follow-up analysis, controls and measures consistent with the Health Insurance Portability and Accountability Act (HIPAA) or with the Privacy Act would be put into place and tested to ensure the security of protected health information. In fact, all systems that process, publish, transmit, or store FDA information or information on behalf of FDA must be protected in accordance with the Federal Information Security Management Act (FISMA). Because Sentinel is being sponsored by FDA and is being established in response to the FDA Amendments Act of 2007, Sentinel must be assessed as part of the FDA Certification and Accreditation (C&A) process as required by FISMA. The C&A process, milestones, and project plan will be provided by the FDA Security Office and executed by the FDA Security Office contractors once the environment is ready. The C&A will be completed prior to moving Sentinel into production.

Computer Security

The draft report mentions computer security issues within the context of the privacy concerns on which the report focuses. Because Sentinel will be a distributed network and protected health information will not be transmitted as part of Sentinel, there is not a risk of security breaches resulting in disclosure of protected health information. FDA recognizes, however, that attention will need to be paid to computer security with respect to the transmission of queries and results summaries, and FDA will require implementation of policies and procedures to ensure computer security at each stage of the process. This and other issues need to be carefully explored in the governance structure; we expect to post an analysis of issues related to governance for public comment in several weeks.

Graphic Figure

To communicate the intended structure of Sentinel, the draft report uses a figure, titled *Overview of the Planned Sentinel Query Process,* both on the Highlights page and as slide 17 of the GAO presentation to Congress. Because FDA is concerned that the figure that was used may mislead some readers about important aspects of the proposed system, we have attached a new version of the figure to explain what is intended; the attached figure explains the Sentinel query process as planned by FDA. The following points clarify specific concerns we have about the earlier figure included in the draft GAO report.

- *FDA and other partners*—This would be more accurate if it read "FDA and other entities" and was depicted by an image of a person looking at graphs and data. The current display gives the impression that this is a fully automated system that does not include human participation and expertise. As policies and procedures are developed for Sentinel, they will include descriptions of who will be able to access this resource and under what circumstances. Other entities besides FDA and "partners" may have access.
- *Partner initiates query*—This would be more accurate if it read "Query initiated." As noted above, once established, policies and procedures will determine who has access to initiate queries.

2

- *Sentinel Coordinating Center*—The drawing of a "server" does not adequately portray the responsibilities of the coordinating center. Coordinating center personnel will perform a number of key roles including determining appropriate methodologies and data sources for obtaining meaningful responses to a query. The coordinating center will not be just an IT architecture to administer queries and receive results.
- *Academic institutions and Federal and state government agencies*—Without further qualification, this is potentially confusing. Only those academic institutions and federal and state government agencies with automated healthcare data will be recipients of queries.
- *Results returned to coordinating center*—This would be clearer if it read "Result summaries returned to Sentinel Coordinating Center." Results summaries will not include protected health information.
- *Coordinating center returns results*—This would be clearer if it read "Sentinel Coordinating Center returns summary results." Results summaries will not include protected health information.
- *Results may potentially be shared with the public*—This would be more accurate if it read "Result summaries will be used to help inform health care decisions" and was, as in FDA's figure, depicted by an image of people sitting around a table discussing documents. The summary results received in response to Sentinel queries will be considered with other available data to provide information about medical products to help inform their proper use.

3

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, John de Ferrari, Assistant Director; Idris Adjerid; Monica Anatalio; Susan Czachor; Season Dietrich; Neil Doherty; Nancy Glover; and Rebecca Eyler 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 Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to 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 Web site, http://www.gao.gov/ordering.htm.

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

Ralph Dawn, Managing Director, dawnr@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