

August 2012

MEDICAL DEVICES

FDA Should Expand Its Consideration of Information Security for Certain Types of Devices

To access this report electronically, scan this QR Code.

Don't have a QR code reader? Several are available for free online.



G A O

Accountability * Integrity * Reliability

Why GAO Did This Study

Certain medical devices have become increasingly complex, and the growing use of wireless technology in these devices has raised concerns about how protected they are against information security risks that could affect their safety and effectiveness.

FDA, an agency within the Department of Health and Human Services (HHS), is responsible for ensuring the safety and effectiveness of medical devices in the United States. FDA reviews manufacturers' applications to market medical devices during its premarket review process and monitors devices, once it has approved them, through its postmarket efforts.

In this report, GAO (1) identifies the threats, vulnerabilities, and resulting information security risks associated with active implantable medical devices, (2) determines the extent to which FDA considered information security during its premarket review of certain devices with known vulnerabilities, and (3) determines what postmarket efforts FDA has in place to identify information security problems. To address these objectives, GAO reviewed relevant documents and interviewed officials from agencies, such as FDA, HHS, the Federal Communications Commission, and the Department of Homeland Security. GAO also interviewed subject-matter experts in information security.

What GAO Recommends

GAO recommends that FDA develop and implement a plan expanding its focus on information security risks. In comments on a draft of this report, HHS concurred with GAO's recommendation and described relevant efforts FDA has initiated.

View [GAO-12-816](#). For more information, contact Marcia Crosse at (202) 512-7114 or crosse@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshusen@gao.gov.

MEDICAL DEVICES

FDA Should Expand Its Consideration of Information Security for Certain Types of Devices

What GAO Found

Several information security threats exist that can exploit vulnerabilities in active implantable medical devices, but experts caution that efforts to mitigate information security risks may adversely affect device performance. Threats to active devices—that is, devices that rely on a power source to operate—that also have wireless capability can be unintentional, such as interference from electromagnetic energy in the environment, or intentional, such as the unauthorized accessing of a device. Several experts consider certain threats to be of greater concern than others; for example, experts noted less concern about interference from electromagnetic energy than other threats. Incidents resulting from unintentional threats have occurred, such as a malfunction resulting from electromagnetic interference, but have since been addressed. Although researchers have recently demonstrated the potential for incidents resulting from intentional threats in two devices—an implantable cardioverter defibrillator and an insulin pump—no such actual incidents are known to have occurred, according to the Food and Drug Administration (FDA). Medical devices may have several such vulnerabilities that make them susceptible to unintentional and intentional threats, including untested software and firmware and limited battery life. Information security risks resulting from certain threats and vulnerabilities could affect the safety and effectiveness of medical devices. These risks include unauthorized changes of device settings resulting from a lack of appropriate access controls. Federal officials and experts noted that efforts to mitigate information security risks need to be balanced with the potential adverse effects such efforts could have on devices' performance, including limiting battery life.

FDA considered information security risks from unintentional threats, but not risks from intentional threats, during its 2001 and 2006 premarket review of two medical devices that have known vulnerabilities. Specifically, FDA considered risks from unintentional threats for four of the eight information security control areas GAO selected for its evaluation—software testing, verification, and validation; risk assessments; access control; and contingency planning. However, the agency did not consider risks from intentional threats for these areas, nor did the agency provide evidence of its review for risks from either unintentional or intentional threats for the remaining four information security control areas—risk management, patch and vulnerability management, technical audit and accountability, and security-incident-response activities. According to FDA, it did not consider information security risks from intentional threats as a realistic possibility until recently. In commenting on a draft of this report, FDA said it intends to reassess its approach for evaluating software used in medical devices, including an assessment of information security risks.

FDA has postmarket efforts, such as its adverse event reporting system, in place to identify problems with medical devices, including those related to information security. However, FDA faces challenges in using them to identify information security problems. For example, the agency's adverse event reporting system relies upon reports submitted by entities, such as manufacturers, that are more closely related to clinical risks than to information security risks. Because information security in active implantable medical devices is a relatively new issue, those reporting might not understand the relevance of information security risks.

Contents

Letter		1
	Background	5
	Several Information Security Threats Have the Potential to Exploit Medical Device Vulnerabilities	14
	FDA Considered Information Security Risks Resulting from Certain Threats during Its Review of Two Devices, and Has Plans to Enhance Its Information Security Efforts	22
	FDA Faces Challenges Identifying Information Security Problems Using Its Postmarket Efforts	27
	Conclusions	34
	Recommendation for Executive Action	35
Appendix I	Objectives, Scope, and Methodology	38
Appendix II	FDA's Adverse Event Reporting Systems	45
Appendix III	OCR and ONC Responsibilities Related to Information Security	48
Appendix IV	GAO Evaluation of FDA's Consideration of Information Security in Its Review of Two PMA Supplements	50
Appendix V	Comments from the Department of Health and Human Services	59
Appendix VI	GAO Contact and Staff Acknowledgments	62
Tables		
	Table 1: Key Information Security Control Areas to Consider for Medical Devices	13
	Table 2: Key Unintentional Threats to Active Implantable Medical Devices	14

Table 3: Key Intentional Threats to Active Implantable Medical Devices	15
Table 4: Key Vulnerabilities in Active Implantable Medical Devices	16
Table 5: Key Information Security Risks to Active Implantable Medical Devices	17
Table 6: Summary of GAO Evaluation of FDA’s Consideration of Information Security Control Areas in the Review of Two PMA Supplements	24
Table 7: Summary of Reporting Requirements for Manufacturers and User Facilities	46
Table 8: GAO Evaluation of FDA’s Consideration of Information Security in Its Review of Two PMA Supplements	51

Figures

Figure 1: Example of the Wireless Interaction between the Defibrillator, Wand, and Programmer	6
Figure 2: Example of a Continuous Glucose Monitoring System and Insulin Pump	7
Figure 3: Example of Prior Medical Device Malfunction Caused by Unintentional Interference	18
Figure 4: Example of Intentional Unauthorized Access of a Medical Device	20

Abbreviations

DHS	Department of Homeland Security
FCC	Federal Communications Commission
FDA	Food and Drug Administration
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH Act	Health Information Technology for Economics and Clinical Health Act of 2009
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	information technology
MAUDE	Manufacturer and User Facility Device Experience Database
MedSun	Medical Product Safety Network
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
ONC	Office of the National Coordinator for Health Information Technology
PMA	premarket approval

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



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 31, 2012

Congressional Requesters

In recent years, the design and development of certain active medical devices have become increasingly complex.¹ Active implantable medical devices, such as implantable cardioverter defibrillators (defibrillators), and other active devices, such as insulin pumps, use hardware, software, and networks to monitor a patient's medical status and transmit and receive related data using wireless communication.² These features improve physicians' ability to treat patients. For example, a physician can now wirelessly access a patient's defibrillator and make adjustments to the device as necessary.

However, the growing use of wireless capabilities and software has raised questions about how well these devices are protected against information security risks, as these risks might affect devices' safety and effectiveness. Information security refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to preserve their confidentiality, integrity, and availability.³ Federal officials and information security experts have recently increased their attention to how information

¹Medical devices include instruments and implements, among other things, intended to be used for the diagnosis, cure, mitigation, treatment, or prevention of a disease or intended to affect the structure or any function of the body and which are not dependent upon being metabolized to achieve these purposes. See 21 U.S.C. § 321(h). Active medical devices are those medical devices that require a power source, such as a battery, in order to function. For the purposes of this report we use the term "medical devices" or "devices" to refer to certain active medical devices.

²A defibrillator is an active implantable device that uses electrical pulses or shocks to help control life-threatening, irregular heartbeats. An insulin pump is an active medical device used to administer insulin as a treatment for diabetes.

³For the purposes of this report, we describe information security as the protection of medical devices and the wireless communication of information they contain from unintentional or intentional—but unauthorized, access—use, disclosure, disruption, modification, or destruction. Specifically, information security includes protecting confidentiality, integrity, and availability. Confidentiality refers to the assurance that the information will be protected from unauthorized access; integrity refers to the assurance that data have not been accidentally or deliberately altered; and availability is ensuring timely and reliable access to and use of information within systems including medical devices.

security risks apply to medical devices. For example, in March 2012, the Information Security and Privacy Advisory Board, a public-private federal advisory committee, offered a number of recommendations to the federal government regarding the security of medical devices, including those with wireless capabilities, and in May 2012 the Department of Homeland Security (DHS) issued a national security bulletin on security risks to medical devices.⁴

In addition, information security researchers recently manipulated two medical devices with wireless capabilities—a defibrillator and an insulin pump, a type of infusion pump—demonstrating their vulnerabilities to information security threats.⁵ Although these incidents occurred in controlled settings and did not involve actual patients, they demonstrated the possibility of intentionally exploiting the vulnerabilities of certain types of active medical devices.

Ensuring the safety and effectiveness of medical devices is the responsibility of the Food and Drug Administration (FDA)—an agency within the Department of Health and Human Services (HHS).⁶ According to FDA, to the extent that information security threats can adversely affect the safety and effectiveness of medical devices, FDA considers relevant mitigation strategies as part of its premarket review process.⁷ FDA also

⁴Information Security and Privacy Advisory Board, “Letter to The Honorable Jeffrey Zients, Acting Director of the Office of Management and Budget” (Washington, D.C.: Mar. 30, 2012). The Information Security and Privacy Advisory Board is, in part, responsible for identifying emerging issues related to information security and privacy and advises the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to federal government information systems. Also, DHS, *Attack Surface: Healthcare and Public Health Sector*, Bulletin 201205040900 (Washington, D.C.: May 2012).

⁵For example, D. Halperin et al., “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defense,” *Proceedings of the 2008 IEEE Symposium on Security and Privacy* (May 2008); N. Paul et al., “A Review of the Security of Insulin Pump Infusion Systems,” *Journal of Diabetes Science and Technology*, 5(6): 1557-62 (November 2011); and J. Radcliffe, “Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System,” presentation at 2011 Black Hat Technical Security Conference (Aug. 4, 2011).

⁶Within FDA, the Center for Devices and Radiological Health is primarily responsible for medical device reviews. Throughout this report, we use FDA to refer to this Center and the offices and divisions within it.

⁷We use the term submissions to generally include the original applications or any additional information provided by the manufacturer.

continues monitoring the use of medical devices through its postmarket efforts.

In the context of information security risks of certain active medical devices, this report (1) identifies the threats, vulnerabilities, and resulting information security risks associated with active implantable medical devices; (2) determines the extent to which FDA considered information security risks in its premarket approval (PMA) review process for certain active medical devices with known vulnerabilities; and (3) determines what postmarket efforts FDA has in place to identify information security problems involving active implantable medical devices.

To identify the threats, vulnerabilities, and resulting information security risks associated with active implantable medical devices, we reviewed available publications—such as white papers published by information security researchers and peer-reviewed journal articles—to develop an initial list of threats, vulnerabilities, and resulting information security risks. We interviewed officials from federal agencies—including FDA, other offices within HHS, the National Institute of Standards and Technology (NIST) within the Department of Commerce, the Department of Defense, DHS, the Department of Veterans Affairs, and the Federal Communications Commission (FCC)—and officials from manufacturers of medical devices. We also interviewed subject-matter experts, including information security researchers and authors of standards related to information security. We then validated our list of information security threats, vulnerabilities, and risks by providing it for review and comment to subject-matter experts. We selected these experts based on their knowledge and familiarity with the information security of medical devices. We excluded implantable medical devices lacking active components, such as hip implants. Additionally, we limited our scope to the integrity and availability aspects of information security—which generally relate to the safety and effectiveness of medical devices—and we excluded confidentiality, which generally relates to privacy. That is, we focused on the potential effect information security risks could have on the functionality of FDA-regulated devices and not on their ability to securely store or exchange personally identifiable information.

To determine the extent to which FDA considered information security risks in its PMA review process for two active medical devices with known vulnerabilities, we evaluated FDA's responses to a questionnaire we developed on the basis of key information security control areas we selected that are outlined in national guidelines and international standards related to information security. We focused our work on the

devices that were recently identified with vulnerabilities by information security researchers. We asked FDA to complete our questionnaire on the basis of two PMA supplemental applications (supplements) reviewed by the agency in 2001 and 2006. FDA confirmed that these were the most recent supplements related to the devices that had been exploited and that involved potential information security issues.⁸ We reviewed the PMA supplements rather than the original PMA applications in order to capture the most recent information related to these two devices. We evaluated FDA's responses to the questionnaire about its prior review of the two PMA supplements as well as supporting documentation, such as FDA's review memorandums and other documents submitted by the manufacturer. For one supplement, FDA provided responses and documentation for a defibrillator that has been exploited by researchers as well as the related programming wand (wand) and programmer, a specialized computer, that are used together to adjust the defibrillator.⁹ For the second supplement, FDA provided responses and documentation for the exploited insulin pump.¹⁰ We also evaluated additional documentation for another defibrillator reviewed by FDA in 2012 that has not been intentionally exploited by researchers, to obtain a more current perspective on FDA's review process for information security issues. Because we evaluated documentation for only three devices, our results are not generalizable. We also interviewed FDA officials about the agency's current efforts to address its review of information security risks to medical devices during its premarket review.

To determine what postmarket efforts FDA has in place to identify information security problems, we reviewed documents submitted by private entities, such as annual reports submitted to FDA by a manufacturer for licensed medical devices, and FDA documents related to its adverse event reporting system. We reviewed data from FDA's adverse event reporting system, collected between 2006 and 2012, to

⁸After an original PMA application is approved, a manufacturer can submit a supplement to the original PMA application to FDA for approval of changes, such as changes to the device or changes in labeling. In general, subsequent changes that affect the safety or effectiveness of the device must undergo FDA's PMA review process and manufacturers must submit a supplement to their original application for approval.

⁹This supplement was submitted to FDA for approval of the wand and programmer software used in conjunction with the defibrillator.

¹⁰This supplement was submitted to FDA for approval of modifications to the insulin pump to, in part, allow it to accept data from a sensor, which captures glucose measurements.

identify potential information security problems associated with these types of devices. We compared FDA's list of adverse event codes that could potentially identify information security issues to our own list of these codes on the basis of our own analysis. We interviewed FDA officials knowledgeable about the agency's adverse event system and these codes to clarify our questions about them. We also interviewed FDA officials to gather information on its postmarket efforts and the extent to which these efforts would be likely to detect events related to information security risks. Appendix I includes additional details on our scope and methodology.

We conducted this performance audit from August 2011 to August 2012, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Examining the information security risks of certain active medical devices, especially with respect to intentional threats, is a relatively new field for federal regulators and information security researchers. However, information security risks have long been previously considered in other contexts, such as federal information systems and the nation's critical infrastructure.¹¹

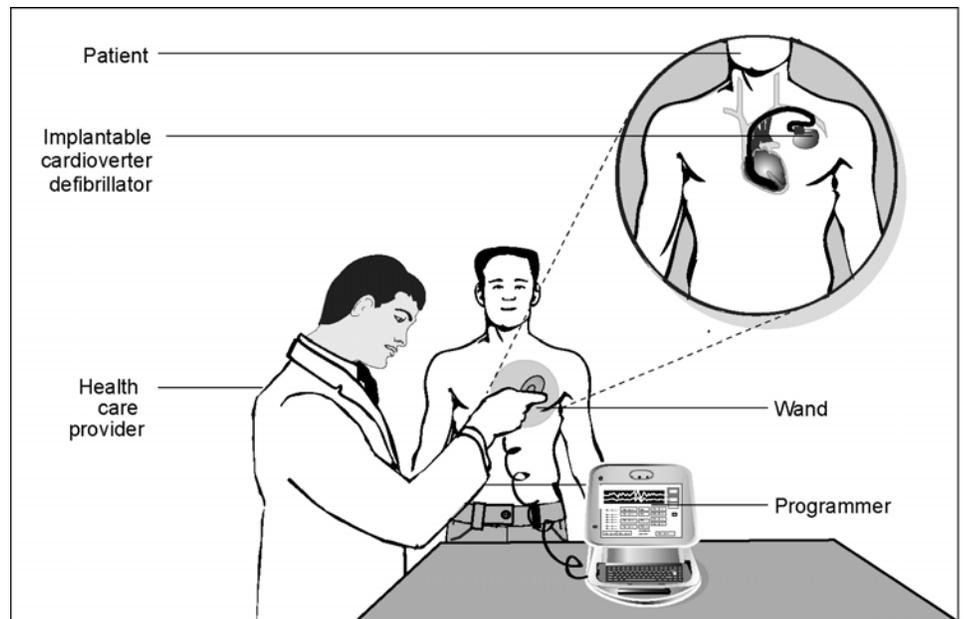
¹¹We have reported on these issues and identified them as government-wide high-risk areas. For example, see GAO, *Information Security: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*, [GAO-11-463T](#) (Washington, D.C.: Mar. 6, 2011) and *High-Risk Series: An Update*, [GAO-11-278](#) (Washington, D.C.: February 2011). We have also reported on challenges FDA faces with regulating medical products, including medical devices, which we also identified as a government-wide high-risk area. For example, see GAO, *Medical Devices: FDA's Premarket Review and Postmarket Safety Efforts*, [GAO-11-556T](#) (Washington, D.C.: Apr. 13, 2011); *Medical Devices: FDA Should Take Steps to Ensure That High-Risk Device Types Are Approved through the Most Stringent Premarket Review Process*, [GAO-09-190](#) (Washington, D.C.: Jan. 15, 2009); and [GAO-11-278](#).

Defibrillators and Insulin Pumps

Two commonly used active medical devices that incorporate electronics and wireless communications are defibrillators, including the wands and programmers used to set and adjust the defibrillators, and insulin pumps.

- A defibrillator is an active medical device that is implanted in a person's chest or abdomen. The defibrillator monitors a person's heart rhythm and delivers an electric pulse to the heart muscle to reestablish a normal heart rhythm when an abnormal heart rhythm is detected. A wand is an external device that connects to a programmer—a specialized computer used to transmit data and to check the defibrillator's functionality and usage. The wand, also called a programmer head, is held within inches of the defibrillator. The wand facilitates the wireless communication between the programmer and the defibrillator to, for example, make adjustments to the device (see fig. 1).

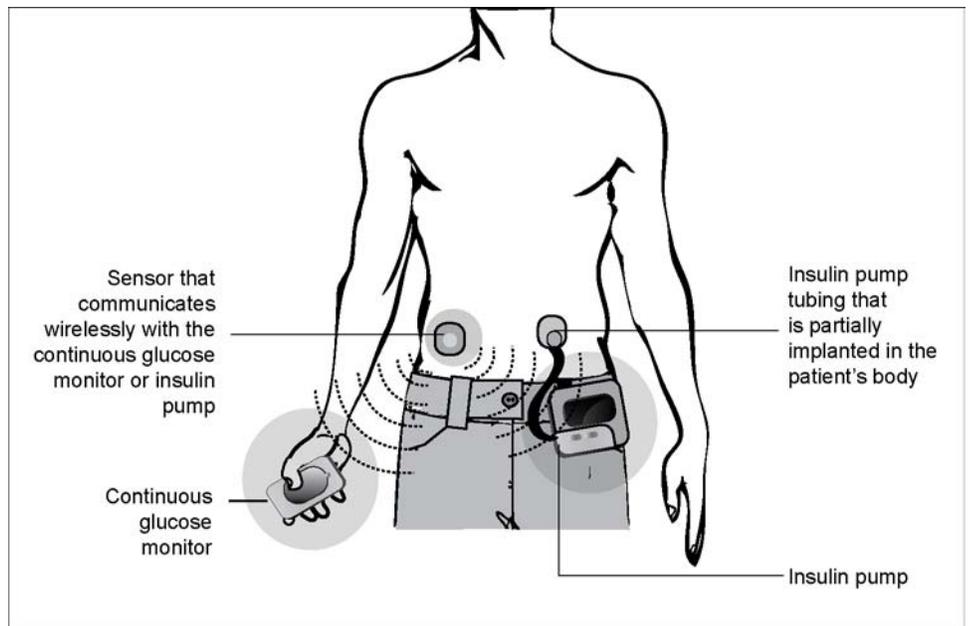
Figure 1: Example of the Wireless Interaction between the Defibrillator, Wand, and Programmer



Source: GAO.

- An insulin pump is an active medical device used in the treatment of diabetes. It replaces the need for periodic injections by delivering rapid-acting insulin using tubing that is partially implanted into the body, such as in the abdomen. Certain types of insulin pumps can work in tandem with a continuous glucose monitoring system, which regularly measures glucose levels in the blood. This monitoring system consists of a sensor inserted under the skin and an external monitor, which can be carried or attached to a person's belt. For insulin pumps working with a monitoring system, glucose measurements are wirelessly transmitted from the sensor to the monitor or from the sensor to the insulin pump (see fig. 2).¹²

Figure 2: Example of a Continuous Glucose Monitoring System and Insulin Pump



Source: GAO.

¹²According to FDA, not all insulin pumps are required to work with a continuous glucose monitor. Insulin pump manufacturers may recommend that users manually check their blood glucose rather than rely on the continuous glucose monitor. Additionally, most insulin pumps operate under direct patient control by means of a wireless handheld controller.

Information Security Threats, Vulnerabilities, and Risks

Addressing information security involves the consideration of threats, vulnerabilities, and the resulting risks.¹³ Information security threats are any circumstances or events with the potential to adversely affect operations, assets, or individuals by means of unauthorized access, destruction, disclosure, modification of information, denial of service, or a combination of these. These threats can be either unintentional, such as interference from energy generated by other devices or from the surrounding environment, or intentional, as recently demonstrated by information security researchers. Vulnerabilities are weaknesses in security procedures, internal controls, or implementation that could be exploited or triggered by a threat. Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of the adverse effects that would arise if the circumstance or event occurs and the likelihood of occurrence. Medical devices that use electronics, wireless communications, and other features are exposed to a greater number of threats, vulnerabilities, and resulting information security risks.

FDA's Responsibility for Regulating Medical Devices

FDA is the federal agency primarily responsible for evaluating the safety and effectiveness of medical devices through its premarket and postmarket efforts. FDA's regulation of medical devices is intended to provide the public with reasonable assurance that medical devices are safe and effective and do not pose a threat to the public's health.

FDA reviews thousands of submissions for new devices filed each year, a small subset of which are subject to FDA's PMA review process.¹⁴ The PMA review process is the most stringent type of FDA device review and

¹³We define information security threats, vulnerabilities, and risk using NIST definitions. See NIST, *NIST IR 7298 Revision 1: Glossary of Key Information Security Terms* (Gaithersburg, Md.: February 2011).

¹⁴FDA's other review process for medical devices is the 510(k) premarket notification process. For this process, FDA requires manufacturers to demonstrate that a new device is substantially equivalent to a device already available on the market that does not require a PMA. Substantially equivalent means the device has the same intended use as another legally marketed device and either the same technological characteristics or different technological characteristics but the manufacturer demonstrates that the device is as safe and effective as the legally marketed device and does not raise different questions of safety or effectiveness. 21 U.S.C. § 360c(i)(1)(A). FDA receives significantly more submissions through its 510(k) notification process compared to its PMA review process. For example, in fiscal year 2011, the agency received 3,833 510(k) original applications and supplements versus 746 PMA original applications and supplements.

requires manufacturers to submit evidence providing reasonable assurance that a new device is safe and effective. A PMA submission should contain administrative, scientific, and technical elements including, among other things, a description of the device model and components, documentation of clinical and nonclinical studies, and a reference to performance standards.¹⁵ If FDA approves a PMA submission, the manufacturer receives a PMA approval order. A multidisciplinary team of FDA officials, which includes relevant subject-matter experts, reviews these submissions. Additionally, FDA officials can consult with staff from its Office of Science and Engineering Laboratories who specialize in electronics, software engineering, and systems engineering. FDA can also consult with external experts, such as relevant advisory committees, which include experts in engineering and physical sciences and industry representatives. As relevant to the wireless medical devices discussed in this report, FDA may contact FCC, as needed, on certain specific, scientific or technical issues. FCC reviews certain medical devices sold in the United States to ensure that these devices meet its regulations for safe human exposure to radiofrequency energy and to ensure that requirements intended to avoid harmful interference between devices using radio waves are met. The defibrillator and insulin pump we included in our evaluation were reviewed under FDA's PMA review process.

FDA's postmarket responsibilities include monitoring the safety of thousands of medical devices already on the market and identifying, analyzing, and acting on potential risks the devices might pose to the public. One of FDA's postmarket efforts is its adverse event reporting system,¹⁶ called the Manufacturer and User Facility Device Experience

¹⁵21 C.F.R. § 814.20.

¹⁶See 21 C.F.R. pt. 803.

Database (MAUDE).¹⁷ FDA requires user facilities (e.g., hospitals) and medical device manufacturers to submit reports to the agency for serious injuries or deaths that were caused or contributed to by their devices. In addition, FDA may require that a manufacturer conduct a study on its device to gather and report additional information on the device's performance after it is available on the market.¹⁸ Appendix II includes additional information on FDA's adverse event reporting systems.

Other Federal Entities with Responsibilities Related to Information Security

DHS and NIST also have responsibilities related to mitigating information security risks, which could include those affecting medical devices.¹⁹ DHS's responsibilities include collaborating with public and private entities to analyze and reduce information security threats and vulnerabilities. DHS also coordinates preparedness activities across 18 critical-infrastructure sectors—one of which is health care—and the response efforts to information security incidents. It does this through several activities, including a reporting and alerting system of information security risks, which can include medical devices, and research and forensic

¹⁷Regulations in 21 C.F.R. pt. 803 require various entities, such as manufacturers or user facilities including hospitals, to report events from any source that reasonably suggest that a marketed medical device has or may have caused or contributed to a death or serious injury, or experienced a reportable malfunction. Caused or contributed means that a medical device was or may have been a factor in a reportable death or serious injury, or a death or serious injury was or may have been attributed to a medical device including events resulting from failure, malfunction, improper or inadequate design, manufacturing problems, labeling problems, or user error. A serious injury is defined as an injury or illness that is (1) life-threatening, (2) results in permanent impairment of a body function or permanent damage to a body structure, or (3) necessitates medical or surgical intervention to preclude permanent impairment of a body function or permanent damage to a body structure.

¹⁸According to FDA, the agency orders these studies—called postapproval studies—as a condition of approval in the PMA approval orders. These studies are used to gather information related to the postmarket performance of, or experience with, an approved device. FDA can also require manufacturers to complete “522 studies” to identify potential problems after devices have been cleared through FDA's 510(k) process.

¹⁹Two other federal entities have responsibilities related to the confidentiality aspect of information security of health care-related information. They are the Office for Civil Rights, which is responsible for developing, interpreting, and enforcing the Privacy and Security Rules called for in the 1996 Health Insurance Portability and Accountability Act, and the Office of the National Coordinator for Health Information Technology, which is the principal federal entity charged with the coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information. Both of these federal entities are in HHS. App. III has more information on these two federal entities.

activities. For example, DHS has a program where an individual or organization that becomes aware of a vulnerability can share this potentially sensitive information with the agency, which will then coordinate a response in a protected manner with vendors, customers, and other interested parties. For vulnerability information that is publicly released, DHS also supports the efforts of NIST to maintain a National Vulnerability Database that allows users to search for information security vulnerabilities pertaining to specific products or technologies.²⁰ NIST is a nonregulatory, federal agency within the Department of Commerce. Under the Federal Information Security Management Act, NIST is responsible for developing standards and guidelines to assist federal agencies in providing adequate information security for federal information and information systems.²¹ These guidelines, while targeted at federal agencies, can also be used to assess and mitigate security risks for other types of information systems and electronic devices.

Standards on Information Security and Related FDA Guidance Documents

In addition to NIST, other organizations, such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), have developed and published various standards related to information security.²² Similar to NIST guidelines, these standards describe information security control areas

²⁰DHS also sponsors the projects for Common Vulnerabilities & Exposures and Common Weakness Enumeration that provide information to the National Vulnerability Database. The Common Vulnerabilities & Exposures is a dictionary of publicly known information security vulnerabilities and exposures. The Common Weakness Enumeration is a unified measurable set of software weaknesses.

²¹This act established information security program, evaluation, and reporting requirements for federal agencies. It was enacted as title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946.

²²The ISO is a nongovernmental organization that develops and publishes international standards, including those related to information security through a consensus-based process involving a network of the national standards bodies of 164 countries. The organization uses "ISO" as the official short-form name because it would have different acronyms depending on the language used. The IEC publishes international standards for electrical, electronic, and related technologies. Its membership includes over 80 nations, including representatives from the public or private sectors.

and related criteria that could be applied to certain types of medical devices to assess and mitigate information security risks.²³

Additionally, for the past 30 years, FDA has issued guidance documents related to information security risks to medical devices resulting from unintentional threats, such as electromagnetic interference. More recently, FDA has issued draft guidance documents on using wireless technology and software in medical devices, which reference for example, the integrity and availability aspects of information security.²⁴ The agency recommends that manufacturers consult its guidance documents when designing and developing medical devices and preparing their submissions for review.

FDA's guidance documents also reference national guidelines and international standards developed by external organizations. FDA recommends, though does not require, that manufacturers consult these other guidelines and standards that might be relevant to the design and development of their medical devices. For example, FDA's guidance document on general principles of software validation cites several NIST special publications on information technology as references for both staff and manufacturers.²⁵

²³Information security control areas are categories related to multiple information security controls. These controls include specific criteria that, when implemented, can help mitigate information security risks.

²⁴FDA, *Draft Guidance for Industry and FDA Staff: Radio Frequency Wireless Technology in Medical Devices* (Rockville, Md.: Jan. 3, 2007), *Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices* (Rockville, Md.: May 11, 2005), and *Draft Guidance for Industry and FDA Staff: Total Product Life Cycle: Infusion Pump – Premarket Notification [510(k)] Submissions* (Rockville, Md.: Apr. 23, 2010).

²⁵FDA, *General Principles of Software Validation: Final Guidance for Industry and FDA Staff* (Rockville, Md.: Jan. 11, 2002) and, for example, NIST, *Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards*, SP 500-165 (Gaithersburg, Md.: September 1995), *High Integrity Software, Standards, and Guidelines*, SP 500-204 (Gaithersburg, Md.: September 1992), and *Reference Information for the Software Verification and Validation Process*, SP 500-234 (Gaithersburg, Md.: March 1996).

Key Information Security Control Areas for Medical Devices

National guidelines and international standards identify information security control areas to consider when identifying, assessing, and mitigating information security risks. Full implementation of all information security controls may not be necessary or appropriate for the mitigation of information security risks. Rather, control areas should be considered to determine what benefits should be implemented to obtain an acceptable level of information security risk. Table 1 includes a list of key information security control areas we determined were important to consider for medical devices.

Table 1: Key Information Security Control Areas to Consider for Medical Devices

Key control area	Definition
Software testing, verification, and validation	Assess software to help ensure that it functions as it was designed. This includes testing of security requirements, such as access controls.
Risk assessments	Assess identified risks in relation to recognized threats; also known as risk analysis. Risks can also refer to hazards or severity of injury and the probability of its occurrence.
Risk management	Manage and mitigate risks inherent in systems development and operations.
Access control	Determine users' permissible activities and the authorization or prohibition of these activities.
Vulnerability and patch management	Identify and address vulnerabilities and implement patches—that is, software fixes to correct an identified defect.
Technical audit and accountability	Review and examination of activities to assess the adequacy and effectiveness of device controls. The intent of this review is to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Security-incident response	Detect a problem, determine its cause, minimize the damage it causes, resolve the problem, and document each step of the response for future reference.
Contingency planning	Maintain or restore device operations in the event of emergencies or system failure.

Source: GAO analysis of FDA, NIST, ISO, and IEC information.

Within each information security control area, multiple controls, safeguards, or countermeasures can be selected to protect a system. Implementation of a risk-based approach to information security involves selecting, implementing, and monitoring appropriate controls within each control area. In cases where it is not feasible to implement a particular control, an organization can either implement compensating controls in other areas or accept a certain level of uncertainty regarding the risk as part of a formal authorization process that balances identified risks with the operational needs of a system.

Several Information Security Threats Have the Potential to Exploit Medical Device Vulnerabilities

Several information security threats have the potential to exploit different vulnerabilities in active implantable medical devices. These threats could be unintentional or intentional in nature. Vulnerabilities can include those related to, for example, the design of the device, such as limited battery capacity. The information security risks resulting from these threats and vulnerabilities could compromise the safety and effectiveness of medical devices. However, federal officials and information security researchers said efforts to mitigate these risks could adversely affect devices' performance.

Threats Have the Potential to Exploit Medical Devices' Vulnerabilities

Information security threats with the potential to exploit vulnerabilities can result from unintentional sources. Table 2 identifies and describes key unintentional threats to active implantable medical devices that could affect their functionality.

Table 2: Key Unintentional Threats to Active Implantable Medical Devices

Unintentional threat	Description
Defective software and firmware	Defective software or firmware can be an unintentional threat when software and firmware inadvertently disrupt systems due to mistakes in design, development, integration, configuration, or operation. ^a
Interference caused by electromagnetic signals in the environment	Interference caused by electromagnetic signals from sources in the environment, such as security systems used in retail stores and metal detectors.

Source: GAO analysis of white papers published by information security researchers, peer-reviewed journals, and interviews with subject-matter experts on information security.

^aFirmware is a combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device.

Threats can also result from intentional sources such as those identified and described below in table 3. These key threats could also affect the functionality of active implantable medical devices.

Table 3: Key Intentional Threats to Active Implantable Medical Devices

Intentional threat	Description
Unauthorized access	Unauthorized access could, for example, involve a malicious actor intercepting and altering signals sent wirelessly to the medical device.
Malware	Malware is a malicious software program designed to carry out annoying or harmful actions. It often masquerades as or is embedded in useful programs so that users are induced to activate it.
Denial-of-service attack	A denial-of-service attack could be launched using computer worms or viruses that overwhelm a device by excessive communication attempts, making the device unusable by either slowing or blocking functionality or draining the device's battery.

Source: GAO analysis of white papers published by information security researchers, peer-reviewed journals, and interviews with subject-matter experts on information security.

Several of the experts we consulted noted that certain intentional information security threats were of greater concern than other threats. For example, approximately half of the nine experts expressed greater concern regarding the threats of unauthorized access or denial-of-service attacks, with two experts citing their own research related to unauthorized access in controlled settings. Additionally, experts made distinctions among intentional threats and the likelihood of their occurring. For example, one expert cited malware as one of the greatest threats to active implantable medical devices because his work demonstrated the device could accept unauthentic firmware updates. However, other experts considered malware as less of a concern because, according to these experts, certain devices are currently designed so that it would be difficult to install and propagate malware. Experts expressed less concern with unintentional threats to medical devices. For example, some of the experts that commented on our list of key threats considered unintentional interference, such as from electromagnetic signals in the environment, as less of a concern than other threats, in part, because FCC regulates radio use so as to avoid harmful interference. Additionally, FDA regulates the potential effects such interference could have on medical devices' performance, and manufacturers have focused on this type of unintentional threat for over 10 years.

Various potential vulnerabilities in active implantable medical devices are susceptible to exploitation by the unintentional and intentional threats described above. Table 4 below identifies and describes key potential vulnerabilities in these medical devices.

Table 4: Key Vulnerabilities in Active Implantable Medical Devices

Vulnerability	Description
Limited battery capacity	The limited capacity of batteries used in certain medical devices hinders the possibility of adding security features to the device because such features can require more power than the battery can deliver. The limited battery capacity makes these medical devices susceptible to an attack that would drain the battery and render the device inoperable.
Remote access	Although remote access is a useful feature of certain medical devices, it could be exploited by a malicious actor, possibly affecting the device's functionality.
Continuous use of wireless communication	Wireless communication allows medical devices to communicate; however, it could create a point of entry for unauthorized users to modify the device, especially if the wireless communication is continuously enabled.
Unencrypted data transfer	Unencrypted data transfer is susceptible to manipulation. For example, a malicious actor could access and modify data that are not securely transmitted, affecting patient safety by altering information used in administering therapy.
Untested software and firmware	Untested software can be a vulnerability when there is a security issue in software and firmware that has not been identified and addressed. ^a This can cause vulnerabilities that make a device susceptible to unintentional or intentional threats.
Susceptibility to electromagnetic (e.g., cellular) or other types of unintentional interference	Susceptibility to interference—caused by electromagnetic (e.g., cellular) or other types of energy—could affect the functionality of certain medical devices. For example, if these medical devices are not designed with resistance to electromagnetic interference, their functionality can be affected.
Limited or nonexistent authentication process and authorization procedures	A limited or nonexistent authentication process and authorization procedures could leave certain medical devices susceptible to unauthorized activities, such as changes to the devices' settings. Authentication is the verification of a user's identity—often by requesting some type of information, such as a password—prior to granting access to the device. Authorization is the granting or denying of access rights to a device.
Disabling of warning mechanisms	Warning mechanisms—such as a vibration or loud tone—could be disabled on certain medical devices. If these mechanisms were disabled, a patient would not be alerted if, for example, unauthorized modifications were made to the device.
Design based on older technologies	Certain medical devices can be designed using older technologies, such as older versions of software or firmware. Additionally, these devices might not have been designed with security as a key consideration.
Inability to update or install security patches	The inability to update or install security patches in certain medical devices could prevent identified software defects from being addressed. Patches are software fixes to correct an identified defect.

Source: GAO analysis of white papers published by information security researchers, peer-reviewed journals, and interviews with subject-matter experts on information security.

^aFirmware is a combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device.

The experts we consulted also noted that addressing these vulnerabilities in active implantable devices could create additional challenges. For example, several of the experts with whom we spoke noted that one way in which medical devices are vulnerable is that they have limited or nonexistent authorization and authentication capabilities; that is, the devices do not distinguish between communications from authorized and

unauthorized users. However, several experts also noted that implementing typical protocols to ensure appropriate authorization creates potential access and safety challenges. These challenges could arise if enhanced authorization procedures hindered health professionals' ability to provide care to patients in emergency situations. For example, a physician in the emergency room might not be able to make life-saving modifications to a patient's pacemaker if the physician does not have the appropriate authorization to access the device.²⁶

Information Security Risks Could Adversely Affect the Safety and Effectiveness of Medical Devices

Information security risks resulting from the exploitation of vulnerabilities by threats could adversely affect the safety and effectiveness of active implantable medical devices. As technology evolves and medical devices become more complex in design and functionality, the potential for these risks occurring is also likely to increase. According to DHS, in order for medical devices to be considered safe, they must also be secure. Key information security risks to these medical devices and related examples are described in table 5.

Table 5: Key Information Security Risks to Active Implantable Medical Devices

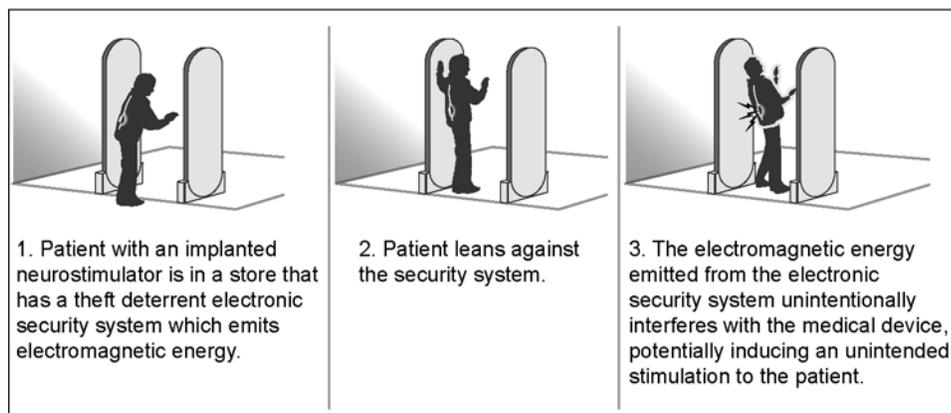
Risk	Example
Unauthorized change of device settings	An unauthorized change could be made to a medical device's settings because, for example, the device lacks appropriate access controls.
Unauthorized change to or disabling of therapies	An unauthorized change to or disabling of therapies administered by a medical device could be done unintentionally by a careless individual or intentionally by a malicious actor. Such an event could occur if, for example, the device lacks an appropriate authentication process or authorization procedures.
Loss or disclosure of sensitive data	Sensitive data stored on a medical device could be destroyed or modified by an unauthorized person. Such an event could occur if, for example, the device lacks encryption or an appropriate authentication process or authorization procedures.
Device malfunction	A device malfunction could result if medical device functionality was disrupted by a type of unintentional interference, such as from electromagnetic energy.

Source: GAO analysis of white papers published by information security researchers, peer-reviewed journals, and interviews with subject-matter experts on information security.

²⁶A pacemaker is a small device that sends electrical impulses to the heart muscle to maintain a suitable heart rate and rhythm. Implanted just under the skin of the chest, pacemakers can be used to treat cardiac conditions, such as congestive heart failure.

Several federal officials and information security researchers noted that some information security risks to active implantable medical devices have long been considered by FDA and manufacturers, such as device failures resulting from different sources of unintentional interference. For example, in the late 1960s, concerns were raised regarding the interference of electromagnetic energy on implanted pacemakers, potentially resulting in the device not working properly. These concerns prompted FDA to release guidance on electromagnetic energy and medical devices.²⁷ In the late 1990s, FDA became aware of interference between electromagnetic energy generated from antitheft systems and metal detectors with other implanted devices, such as neurostimulators, potentially resulting in an inappropriate jolt or shock (see fig. 3).²⁸ FDA and manufacturers now recommend that those with neurostimulators avoid lingering near or leaning against such systems and metal detectors.

Figure 3: Example of Prior Medical Device Malfunction Caused by Unintentional Interference



Source: GAO.

²⁷FDA, *An FDA Medical Device Standards Publication: Electromagnetic Compatibility Standard for Medical Devices*, MDS-201-0004 (Silver Spring, Md.: Oct. 1, 1979). FDA has since released additional, related guidance. For example, see FDA, *Draft Radio Frequency Wireless Technology in Medical Devices* (Rockville, Md.: Jan. 3, 2007).

²⁸Neurostimulators are implantable medical devices that can be used as treatment for various disorders, such as tremors from Parkinson's disease. These devices provide electrical stimulation to specific parts of the body to, for example, treat these tremors by targeting areas of the brain that control movement.

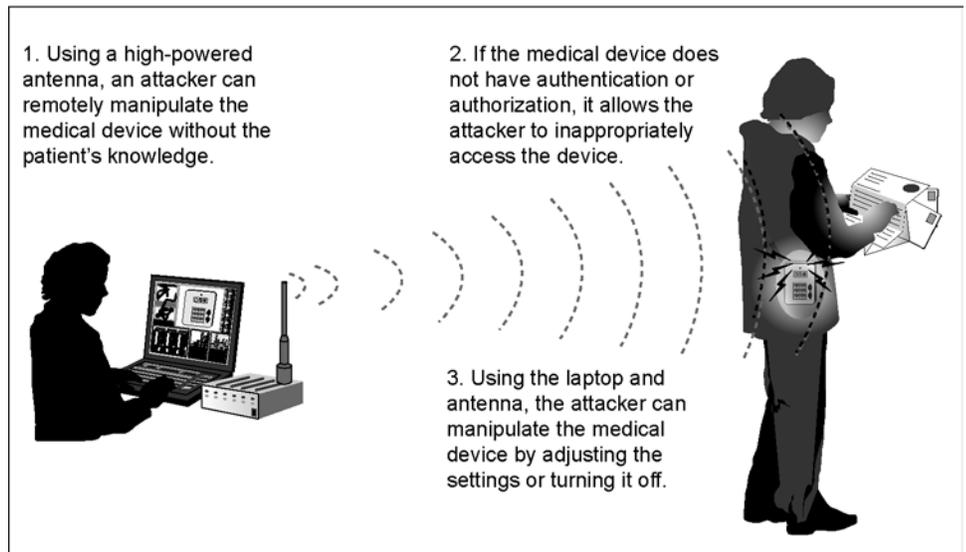
In contrast, federal officials and information security researchers noted that, to date, there have been no documented information security incidents resulting from the exploitation of vulnerabilities in these types of medical devices by intentional threats in real-world settings. However, there have been four separate demonstrations in controlled settings, showing that the intentional exploitation of vulnerabilities in certain medical devices is possible. Each of these demonstrations involved laboratory tests and did not result in patient harm or death. The first demonstration occurred in 2008, when a team of academic researchers, working in a controlled setting, showed that they could remotely exploit a defibrillator by delivering a command, using the associated wand and programmer.²⁹ A second demonstration occurred in 2010, when a team of academic researchers remotely exploited an insulin pump, preventing it from operating properly.³⁰ Two additional demonstrations occurred in 2011, when two security experts, also working in controlled settings, showed on separate occasions that they could also remotely exploit an insulin pump.³¹ Both of these experts demonstrated they could manipulate the amount of insulin dispensed by the device. These demonstrations occurred at varying distances. For example, one demonstration occurred at a distance of 100 feet, while another occurred at approximately 300 feet. Figure 4 below depicts an example of a demonstration of the exploitation of a medical device's vulnerability.

²⁹D. Halperin et al., "Pacemakers and Implantable Cardiac Defibrillators," 10.

³⁰N. Paul et al., "Security of Infusion Systems," 1559.

³¹For example, see J. Radcliffe, "Hacking Medical Devices."

Figure 4: Example of Intentional Unauthorized Access of a Medical Device



Source: GAO.

According to manufacturer officials, medical devices undergo testing for vulnerabilities that could be exploited. The identified vulnerabilities are then addressed. However, these officials acknowledged that recent incidents have increased their awareness of potential information security risks resulting from intentional threats and have resulted in changes in testing procedures. For example, according to officials from one manufacturer, information security risks resulting from malicious intent are now being considered, and officials are incorporating enhanced security procedures into the design of their medical devices. These officials also stressed that these demonstrations by information security researchers, while informative, should not overshadow the clinical benefits offered by medical devices.³²

³²These officials also noted that security breaches resulting from malicious intent involve criminal activity and a unique and rare set of circumstances. They said the risk of a criminal attack should not overshadow the primary focus for evaluating medical devices; that is, evaluating the benefits these devices can offer and the potential risks posed by their regular operation.

Mitigation Strategies for Information Security Risks Could Adversely Affect Medical Devices' Performance

Federal officials and information security researchers we spoke with noted that some mitigation strategies could adversely affect certain medical devices' performance. For example, a pacemaker cannot be immune to all electrical signals because the device needs to be able to detect the electrical signals naturally generated by the patient's heart to determine if the pulses are irregular. Similarly, for the information security risk associated with using older versions of software, a potential mitigation strategy would be to have these medical devices operate using newer versions. However, according to FDA officials, software in implanted medical devices, such as pacemakers, typically is not frequently updated; rather, the software is updated on an as-needed basis. As with any device that uses software, such updates or other modifications could introduce unanticipated software problems that could adversely affect the functionality of a device, particularly if the software had not been properly tested prior to being used. According to FDA, the majority of software-related medical device problems occur because devices are using software that has been revised since the medical device was reviewed by FDA.³³ FDA officials explained that manufacturers choose to rely on older software because its vulnerabilities are better understood by both manufacturers and regulators.

Federal officials and other experts also noted that addressing information security risks for certain medical devices involves additional safety considerations that are not typically necessary for other types of products. For example, incorporating encryption into the medical device could mitigate the information security risk of unauthorized changes to the settings of the device. However, experts we spoke with said adding encryption to a device could drain its battery more quickly, making it necessary to change the battery more frequently. Changing the battery for active implantable devices, such as a pacemaker, involves undergoing a surgical procedure, which has its own potential health risks. In contrast, two information security researchers we spoke with said that, in their opinion, technology has advanced such that encryption can be added to a medical device without using as much energy as before. However, manufacturers have chosen not to take advantage of this newer

³³According to FDA, the majority of these software-related medical device problems occur after the device has been reviewed. The agency also noted the importance of adequate design, development, testing, and version control of revisions to the software used in medical devices.

technology, in part, because of the potential for increased costs in producing the device, according to other experts.

FDA officials and other experts also noted that information security risks could vary for different devices because each device has unique vulnerabilities and a device's susceptibility to threats is based on factors such as its design. For example, FDA officials noted that the wireless capabilities between a defibrillator and the associated wand and programmer are different than those used by certain insulin pumps. These differences not only affect how these respective devices operate, but also the susceptibility to information security threats.

An increasing awareness of intentional and unintentional information security threats, vulnerabilities, and resulting risks to medical devices now exists. Addressing these risks requires a comprehensive approach that balances mitigating potential information security risks and maintaining a device's safety and effectiveness.

FDA Considered Information Security Risks Resulting from Certain Threats during Its Review of Two Devices, and Has Plans to Enhance Its Information Security Efforts

For the two medical devices that have known vulnerabilities, FDA considered information security risks from unintentional threats, but not risks from intentional threats during its premarket review of the related supplements. FDA stated that it did not generally consider intentional information security threats in its review process at the time these devices were reviewed. FDA officials also told us the agency intends to enhance its information security efforts by reviewing how it approaches the evaluation of software used in medical devices. However, the agency has not yet defined specific, information security-related areas it will examine as part of this review, nor has it established specific milestones for completing it.

FDA Officials Considered Information Security Risks from Unintentional Threats, but Not from Intentional Threats in Their Review of Two PMA Supplements

In the reviews of two PMA supplements for medical devices with known vulnerabilities conducted in 2001 and 2006, FDA officials considered information security risks resulting from unintentional threats, but not from intentional threats. Specifically, FDA considered information security risks in four of the eight information security control areas we selected—software testing, verification, and validation; risk assessments; access control; and contingency planning (see table 6 below and app. IV for more details on our evaluation). We reviewed the PMA supplements and supporting documentation for a defibrillator and its associated wand and

programmer, and for a specific wireless insulin pump system that incorporates a continuous glucose monitor. For example, FDA reviewed the manufacturer's strategy to mitigate information security risks associated with software testing, verification, and validation resulting from unintentional threats to the wand and insulin pump from radio frequency and electromagnetic energy. Additionally, FDA officials told us that the manufacturer addressed access control for the defibrillator, wand, and programmer by requiring that they be used collectively in order to make adjustments. In order to have its settings changed, the defibrillator must communicate with the programmer. The wand, which facilitates the communication between the defibrillator and the programmer, is designed to be used within inches of the defibrillator. All three of these devices are designed to be used together in a health care setting.

Table 6: Summary of GAO Evaluation of FDA’s Consideration of Information Security Control Areas in the Review of Two PMA Supplements

Select control area and examples of associated activities	FDA’s consideration of the information security control area
Software testing, verification, and validation For example: verifying that software requirements are consistently fulfilled and validating that software meets user needs and intended uses, in addition to testing for security requirements such as access control	●
Risk assessments For example: reviewing possible hazards, causes of adverse outcomes resulting from unintentional or intentional threats, and risk controls	●
Risk management For example: establishing and maintaining an ongoing process to identify risks and to implement and evaluate risk-control activities	○
Access control For example: establishing appropriate processes or measures to limit or restrict access to a medical device	●
Patch and vulnerability management For example: establishing a patch and vulnerability management process, including identifying and prioritizing vulnerabilities to be addressed	○
Technical audit and accountability For example: determining what activities will be audited, monitored, and reviewed	○
Security-incident response For example: establishing how manufacturers will identify and respond to security incidents	○
Contingency planning For example: identifying preventative measures for defined scenarios that could result in the loss of critical performance by the device	●

Source: GAO analysis of FDA data.

Key:

● = FDA considered all key practices for this security control area during its review of the supplements.

◐ = FDA considered some key practices for this security control area during its review of the supplements.

○ = FDA did not consider any of the key practices for this security control area during its review of the supplements.

However, FDA did not consider risks from unintentional threats for the four remaining information security control areas—risk management, patch and vulnerability management, technical audit and accountability, and security-incident response. Additionally, FDA did not consider information security risks resulting from intentional threats for any of the eight information security control areas. Specifically, on the basis of the support the agency provided for these two PMA supplements, FDA did

not demonstrate that it had considered the potential benefits of mitigation strategies to protect devices against information security risks from certain unintentional or intentional threats in light of the appropriate level of acceptable risk for medical devices with known vulnerabilities.

FDA officials told us that since the agency reviewed these PMA supplements in 2001 and 2006, respectively, their consideration of information security has changed. To support this, FDA provided additional examples from an original PMA application for a defibrillator reviewed in 2012. This additional evidence showed that the agency had generally enhanced its consideration of information security during its PMA review for those four information security control areas previously identified—software testing, verification, and validation; risk assessments; access control; and contingency planning. For example, FDA conducted a more comprehensive review of the manufacturer’s software verification and validation documentation, and included software-testing documentation, electromagnetic-compatibility testing, electromagnetic-interference testing, and frequency testing. FDA also provided evidence of its consideration of a fifth information security control area—risk management—in this newer PMA application.

However, FDA did not provide any evidence showing its consideration of security-specific tests. For example, FDA did not provide evidence showing testing of attempts to enter incorrect or invalid data in the device or the use of fuzzing, an information security-related testing technique that uses random data to discover software errors and security flaws. FDA also did not demonstrate its consideration of information security risks resulting from unintentional threats related to the remaining three information security controls we selected, including patch and vulnerability management, despite guidelines from NIST and other sources on the importance of these issues. Additionally, when reviewing the manufacturer’s risk management plan, FDA did not consider information security risks resulting from intentional threats. Thus, while it continues to consider some information security risks resulting from unintentional threats, such as interference, FDA has not begun to consider risks resulting from intentional threats.

FDA officials acknowledged the limitations of their review process for information security issues. They explained that, as part of the agency’s PMA review process, they consider various risks with a focus on the most relevant risks that could result in harm to patients. According to officials, they tend to consider the most relevant risks to be clinical risks, such as an increased risk of heart failure from having an implanted defibrillator,

and not information security risks, such as the reprogramming of a device by a malicious actor.³⁴ FDA officials said they also consider the intended use of the device and the type of setting in which the device will be used, both of which are determined by the manufacturer. For example, FDA officials would review a scalpel for potential clinical risks resulting from its intended use in a clinical setting. However, the agency cannot control how devices are used in other settings, or if devices are misused. They noted that a scalpel could become a dangerous weapon if misused by a malicious actor.

FDA officials also noted that they consider information security risks in the context of a clinical situation. For example, officials said they have long considered information security risks resulting from unintentional threats, such as from interference or from defective software. However, they acknowledged they have only recently considered information security risks resulting from intentional threats because they did not previously consider such threats as reasonable and likely at the time of their earlier reviews in 2001 and 2006. They noted that, although conducted in controlled settings, researchers' recent demonstrations of vulnerabilities in two medical devices support the possibility that incidents caused by information security risks resulting from intentional threats could occur.

FDA Intends to Enhance Its Efforts Related to Information Security

FDA officials said that in the future the agency intends to enhance its efforts related to information security. For example, officials said the agency will consider information security risks resulting from intentional threats when reviewing manufacturers' submissions for new devices. Officials said that they will consider whether the manufacturer identified the appropriate information security risks resulting from intentional threats and, if applicable, what proposed mitigation strategies the manufacturer included.

FDA officials also told us that the agency is currently planning to review its approach to evaluating software used in medical devices. Officials said the review of its approach will be conducted by a contractor and will involve an analysis of how the agency considers software in medical devices during premarket reviews. This review is to include an

³⁴According to FDA, manufacturers describe the possible relevant and reasonable risks, which can include information security risks, as part of their submissions. If FDA officials identify other potential risks, they can request additional evidence from the manufacturer.

examination of FDA's resources and evaluative tools. It will also include a comparison of FDA's approach to reviewing software in medical devices to the approaches of other sectors that also make or use high-risk and complex software products, such as the aviation and nuclear industries. According to officials, this effort is also intended to identify external resources the agency can draw upon for evaluating information security risks, such as those supported by other federal agencies. For example, FDA officials said they currently do not utilize information security resources available from DHS and NIST, such as the National Vulnerability Database, but acknowledged that such a database could be a useful tool in identifying vulnerabilities relevant to medical devices.

According to the agency's preliminary planning information, the FDA review does not explicitly mention information security issues such as malware, patching and vulnerability management, or the use of security-related testing techniques. Additionally, in commenting on a draft of this report, HHS noted that FDA anticipates completing the review on the agency's approach to evaluating software in medical devices in calendar year 2012. HHS also noted that FDA will include an assessment of information security risks for medical devices. However, HHS did not provide any milestones, including for when any changes might be implemented, or any description for how this review would address specific aspects of information security. By not identifying which specific aspects of information security the agency intends to consider in its review or establishing a specific schedule to demonstrate that it is addressing the emerging issue of intentional threats, FDA may miss an opportunity to more fully consider information security issues in its medical device review process.

FDA Faces Challenges Identifying Information Security Problems Using Its Postmarket Efforts

FDA has various postmarket efforts in place to identify problems with medical devices, including those related to information security. Despite having postmarket efforts in place, FDA faces challenges in using them to identify information security problems.

FDA Has Adverse Event Reporting and Other Postmarket Efforts in Place to Identify Problems with Medical Devices, including Those Related to Information Security

FDA has various postmarket efforts in place to identify problems with medical devices once they have been approved for marketing, including any problems related to information security. One of these efforts is its adverse event reporting system, MAUDE.³⁵ MAUDE stores adverse event reports submitted by reporters, which include manufacturers, user facilities (e.g., hospitals), and voluntary reporters. FDA requires manufacturers and user facilities to submit information regarding adverse events involving medical devices and submit reports on these events to FDA. However, FDA does not have these same requirements for other medical device users, including consumers and health care providers. Regardless of whether reporters are required to submit adverse event reports, FDA must wait for reporters to recognize and submit information on suspected adverse events before the agency can become aware of and identify device problems through this system.³⁶

For those adverse events that are reported, FDA stated that it is able to conduct systematic reviews and searches of these reports. According to FDA, it systematically reviews all information that it receives in the MAUDE database and follows up with reporters when the agency believes that such follow-up is necessary or would provide additional, useful information. Additionally, FDA can search within MAUDE to determine if any of the reporters cited information security issues when submitting details about the adverse events. Searches can be conducted using categories of codes that FDA has developed. These codes are used by reporters to describe types of adverse events. These codes

³⁵Adverse event reporting provides a mechanism for FDA to collect information regarding the performance of marketed devices. This information is used by FDA and device manufacturers to identify and monitor significant adverse events involving medical devices. Specifically, FDA uses MAUDE to identify signals of unanticipated medical device issues as well as to monitor trends of known medical device issues. This information may aid in revealing potential health hazards and risk factors that could include those related to information security risks. Also, some of FDA's adverse event reporting systems, including MAUDE, are characterized as passive surveillance systems because they do not actively recognize problems. Because these systems are dependent upon reporters to identify problems with devices and submit adverse event reports to FDA, significant underreporting occurs. See app. II for more information about these systems and their respective reporting requirements.

³⁶According to FDA officials, FDA analysts with specialized clinical, engineering, and regulatory expertise review reports received by MAUDE.

include device-problem codes that are used to describe details such as the reason behind a device's failure.³⁷

According to FDA officials, there are 10 codes in MAUDE that reporters primarily could select when reporting an adverse event to indicate—and allow FDA to subsequently identify—that an information security problem had occurred. For example, 3 of these codes are used to describe adverse events that resulted from (1) an application issue, (2) the unauthorized access to a computer system, or (3) a computer-security issue. Using these 10 codes, FDA had not identified any information security problems involving active implantable medical devices, as of April 2012.³⁸

In addition to these 10 codes, we identified additional codes that could indicate an information security problem had occurred due to an unintentional threat.³⁹ Using these additional codes, FDA has identified potential information security problems involving active implantable medical devices. For example, one adverse event involved a pacemaker and a computer-software issue. Specifically, the pacemaker's programmer was slow to start and experienced some errors, but no patient involvement or complications were reported and the programmer was returned for repair. Thus, although FDA does not categorize its codes as specifically related to information security problems, it has

³⁷Device-problem codes describe device failures or issues related to the device that are encountered during the event and are one of three categories of event problem codes. The other two categories of event-problem codes include component codes—which indicate what specific component or assembly of the device was associated with the event—and patient-problem codes—which indicate the effects that an event may have had on the patient, including signs, symptoms, syndromes, or diagnoses. In addition to event-problem codes, FDA also has a class of codes called manufacturer-evaluation codes. These codes are also divided into three categories—(1) manufacturer-evaluation-method codes, which describe how a manufacturer evaluated a reportable incident, (2) manufacturer-results codes, which describe what a manufacturer found when testing a device, and (3) manufacturer-conclusion codes, which describe what a manufacturer concluded from the testing of a device.

³⁸Using these 10 codes, FDA had identified three adverse events related to information security risks as of April 2012. However, these adverse events did not involve active implantable medical devices and were therefore excluded because they were beyond the scope of this report.

³⁹FDA does not consider these additional codes we identified as related to information security, but rather as related to other issues, such as design problems.

codes in place that could potentially identify information security problems resulting from both unintentional and intentional threats.

A second postmarket effort that FDA has in place to identify problems is its process for requiring manufacturers to conduct postmarket surveillance studies.⁴⁰ Manufacturers may be required to conduct postmarket surveillance studies to continue to systematically evaluate device performance while the device is in commercial distribution. For example, FDA officials could order a postmarket surveillance study for a defibrillator because its failure would have serious adverse health effects for a patient. It is possible these studies could identify vulnerabilities or unintentional threats that might adversely affect medical devices, but postmarket surveillance studies typically focus on clinical outcomes that might affect patients. At the time of our review, FDA officials said that, while they could require manufacturers to conduct postmarket studies to focus on information security risks, they did not currently have plans to request that any manufacturers do so. FDA officials explained that these studies are intended to address residual questions from clinical trials for a medical device. These lingering questions typically relate to the medical device's clinical risks to patients, such as whether the use of a particular device is appropriate for a specific patient population, rather than to its information security risks.

A third postmarket effort is FDA's requirement for manufacturers to prepare annual PMA postapproval reports (annual reports).⁴¹ Among the issues manufacturers must include in these reports are the rationales for any changes they made to the medical device during the preceding year, including changes made because of an adverse event. For example, these annual reports could potentially include information related to a

⁴⁰FDA orders these studies—called postapproval studies—as a condition of approval in the PMA approval orders, and they are used to gather information related to postmarket performance of, or experience with, an approved device. FDA can also require manufacturers to complete “522 studies” to identify potential problems after devices have been cleared through FDA's 510(k) process.

⁴¹Manufacturers whose devices were approved through the PMA review process are required to prepare periodic reports under the PMA approval order. Under this order, FDA typically specifies that the manufacturer is to submit its report 1 year from the date of approval of the original PMA and annually thereafter. PMA reports must include specific information, such as bibliographies of reports from scientific literature concerning the device and that are known to or that reasonably should be known to the manufacturer and that were not previously submitted as part of its PMA application.

problem due to an information security risk if the problem led the manufacturer to change the device, such as a modification to the device's software. Manufacturers are also required to include any information about defects related to their medical devices that have been identified in scientific literature—including published reports on clinical studies of similar devices or unpublished reports of data from clinical investigations involving their devices—that are known or that reasonably should be known to them. We reviewed the annual reports for the two active medical devices with known vulnerabilities to determine if the manufacturer had noted the research conducted by information security researchers demonstrating the devices' susceptibility to intentional threats.

For the defibrillator, we found references to other published reports discussing adverse events resulting from unintentional threats, such as from the adverse effect electromagnetic interference had on the defibrillator's functionality. However, no potential information security problems due to intentional information security threats were included in these reports, including any references to the 2008 exploitation by researchers. Additionally, no potential information security problems were included in the annual reports we reviewed for the insulin pump exploited by researchers in 2010.

FDA Faces Challenges in Using Its Adverse Event Reporting System to Identify Information Security Problems

Despite having postmarket efforts in place, FDA faces challenges with identifying information security problems, should they occur. We have previously reported on some challenges associated with adverse event reporting, such as the inherent weaknesses associated with passive surveillance systems.⁴² For example, MAUDE is a passive system and FDA relies upon reporters to recognize and submit information on suspected adverse events. According to FDA, because of this dependence upon reporters, significant underreporting occurs. This underreporting affects FDA's ability to estimate the magnitude of a problem because the number of reports submitted might not be representative of the total number of patients that experienced the adverse event.

⁴²GAO, *Drug Safety: FDA Has Begun Efforts to Enhance Postmarket Safety, but Additional Actions Are Needed*, [GAO-10-68](#) (Washington, D.C.: Nov. 9, 2009).

Underreporting can also occur because individuals are either unfamiliar with reporting requirements for devices or because reporting can be time-consuming. Additionally, FDA and other experts told us that underreporting of information security problems in medical devices could result from a lack of understanding or awareness among adverse event reporters about how information security problems apply to these devices. They noted that information security is a relatively new issue area with respect to its applicability to medical devices, which could make it a difficult type of problem to understand and report to FDA. Some health care providers might not fully understand, and therefore may not report, information security problems whether resulting from unintentional or intentional threats, as providers have instead been trained to focus on clinical problems associated with medical devices. FDA officials said that they were uncertain if reporters would recognize that an information security problem was relevant or even had occurred. For example, an adverse event report could note that a patient complained of chest pains and experienced an increase in heart rate, but the report might not include any indication that a possible information security issue was a factor; that is, the reporter might not note that the patient's device had recently been programmed because the health care provider did not consider this information relevant or necessary.

Besides underreporting, another weakness inherent in MAUDE is FDA's inability to establish causality because reporters might submit insufficient or inadequate information about an adverse event. For example, a reporter might fail to include specific details about an adverse event—such as that the event occurred while a medical device was being reprogrammed. Because the manufacturer generally conducts any follow-up investigation, if FDA wanted more information about an adverse event, FDA could notify manufacturers in writing that the agency required additional information about manufacturers' reports. However, FDA officials told us that the more time passes from the time an adverse event occurred to the actual investigation, the more difficult it is to obtain detailed information. Also, officials request additional information from manufacturers on a case-by-case basis. In addition to the challenge of establishing causality, FDA officials told us it would also be difficult to determine the motivation behind an adverse event, such as if it was caused by a malicious actor. Without such details and contextual information related to the cause of and motivation behind an adverse event, FDA would be limited in its ability to later identify the problem as related to information security and determine if it resulted from an intentional threat. Because of these inherent weaknesses associated with MAUDE as a passive surveillance system, it is possible that information

security problems involving medical devices could have occurred but not have been reported to FDA or have not been identified as information security problems by the agency.

FDA's Planned Postmarket Improvement Initiatives Might Strengthen Its Ability to Identify Information Security Problems

FDA has two planned initiatives that are intended to improve its postmarket efforts in order to more accurately identify and analyze problems associated with medical devices. According to FDA, these initiatives are not specifically intended to improve FDA's ability to identify information security problems; however, these initiatives might strengthen FDA's ability to do so by providing the agency with additional information. One initiative is the Unique Device Identification effort for the postmarket surveillance of devices, which, according to FDA, will allow the agency to aggregate adverse event reports in order to more accurately analyze them when conducting signal analyses.⁴³ The initiative will also allow FDA to identify specific devices included in adverse event reports, allowing for more rapid and effective corrective actions that can focus on specific devices, according to one agency official.⁴⁴ Additionally, this official told us that although this effort was not specifically designed to help FDA identify information security problems involving medical devices, it will help FDA identify specific device models that could encounter information security problems.

Another postmarket initiative is the development of FDA's new adverse event reporting system. According to FDA, the agency is in the process of developing a new system to replace MAUDE by September 2013.⁴⁵ MAUDE, which is currently over 15 years old, was not designed to handle

⁴³The Food and Drug Administration Amendments Act of 2007 directs FDA to promulgate regulations establishing a Unique Device Identification system for medical devices. The system is to require that the label of devices bear a unique identifier, unless otherwise specified or exempt. The unique identifier shall adequately identify the device through distribution and use and may include information on the lot or serial number. Pub. L. No. 110-85, § 226, 121 Stat. 823, 854 (Sept. 27, 2007).

⁴⁴In July 2012, FDA published its proposed rule on implementing Unique Device Identification in the *Federal Register* for public comment. 77 Fed. Reg. 40736 (July 10, 2012).

⁴⁵Once operational, this new system will replace MAUDE as FDA's passive surveillance system for devices and will be compatible with FDA's drug and vaccine adverse event reporting systems to allow for cross-center communication within the agency. Such communication may be useful in handling drug-device or biologic-device issues that may be found in combination products.

the capacity or complexity of medical device adverse event information that exists today. FDA expects the new system—the FDA Adverse Event Reporting System—to perform similar functions as MAUDE but also allow for greater capacity for storing adverse events and enhanced search capability compared to MAUDE. However, according to FDA, transitioning from MAUDE to this new system will not automatically make it easier to identify information security problems because, like MAUDE, the system is designed to collect information that indicates that a medical device has caused or contributed to a serious injury or death, which is more closely associated with clinical risks than information security risks. Because this new system will also be a passive surveillance system, FDA will still rely on reporters to recognize and submit information on information security problems involving medical devices before the agency can search for and subsequently identify them. Still, FDA officials told us that this new system will also include the 10 codes that reporters currently can use to indicate that an information security problem has occurred. If FDA is able to conduct more complex searches under this new system, the search results might strengthen the agency’s ability to identify information security problems involving medical devices.

Conclusions

As active implantable medical devices increasingly use newer technologies, such as wireless capabilities, their susceptibility to various information security risks also increases. Although the risks resulting from unintentional threats have long been known, information security risks resulting from intentional threats have only recently been confirmed. While FDA has considered some information security risks associated with unintentional threats during its PMA review process, such as interference, it has not considered others, such as patch and vulnerability management. Additionally, FDA has not considered information security risks resulting from intentional threats. FDA has also not utilized available resources, such as the National Vulnerabilities Database sponsored and maintained by DHS and NIST. Also, FDA’s postmarket efforts have several limitations, and it is unclear if the agency could successfully identify information security problems with active implantable medical devices were they to occur. Although FDA intends to review its evaluation of software used in medical devices, according to the agency’s preliminary planning information, the review does not explicitly mention information security issues such as malware, patching and vulnerability management, or the use of security-related testing techniques. Furthermore FDA has not established specific milestones, including for when it will implement any changes, for the review.

Recommendation for Executive Action

To better ensure the safety and effectiveness of active implantable medical devices, we are recommending that the Secretary of Health and Human Services direct the Commissioner of FDA to develop and implement a more comprehensive plan to assist the agency in enhancing its review and surveillance of medical devices as technology evolves, and that will incorporate the multiple aspects of information security. This plan should include, at a minimum, four actions, such as determining how FDA can

- increase its focus on manufacturers' identification of potential unintentional and intentional threats, vulnerabilities, the resulting information security risks, and strategies to mitigate these risks during its PMA review process;
- utilize available resources, including those from other entities, such as other federal agencies;
- leverage its postmarket efforts to identify and investigate information security problems; and
- establish specific milestones for completing this review and implementing these changes.

Agency and Third Party Comments

HHS, FCC, NIST (within the Department of Commerce), DHS, and the Departments of Defense and of Veterans Affairs reviewed a draft of this report. HHS provided written comments, which we have reprinted in Appendix V. HHS, FCC, NIST, and the Department of Veterans Affairs provided technical comments, which we have incorporated as appropriate. DHS and the Department of Defense did not provide comments on a draft of this report. A third party also reviewed relevant sections of this report and provided technical comments, which we have incorporated as appropriate.

In its comments, HHS concurred with our recommendation and described relevant efforts FDA has initiated. HHS described FDA's efforts to identify and address information security concerns to ensure the safety of medical devices. For example, HHS noted that FDA is establishing collaborative relationships with DHS, NIST, and the Department of Defense, and is engaging other stakeholders to consider the potential applicability of standards from other sectors, such as industrial control, to medical devices. HHS also noted FDA's postmarket efforts to address information security, including evaluating and enhancing surveillance tools to identify

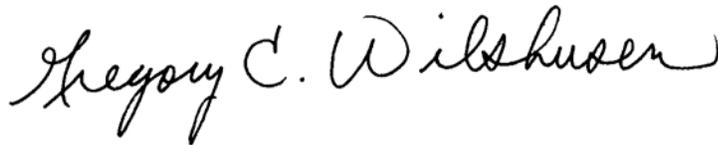
and investigate information security problems. For example, HHS said FDA is in the process of releasing its “National Postmarket Surveillance Plan” designed to enhance national coordination of information sharing for adverse events related to medical devices.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Chairman of the FCC and the Secretaries of Commerce, Defense, Health and Human Services, Homeland Security, and Veterans Affairs and to other interested parties. The report will also be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Marcia Crosse at (202) 512-7114 or crossem@gao.gov or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VI.



Marcia Crosse
Director, Health Care



Gregory C. Wilshusen
Director, Information Security Issues

List of Requesters

The Honorable Edward J. Markey
Ranking Member
Committee on Natural Resources
House of Representatives

The Honorable Donna Edwards
Ranking Member
Subcommittee on Technology and Innovation
Committee on Science, Space, and Technology
House of Representatives

The Honorable Anna G. Eshoo
Ranking Member
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) identify the threats, vulnerabilities, and resulting information security risks associated with active implantable medical devices; (2) determine the extent to which the Food and Drug Administration (FDA) considered information security risks in its premarket approval (PMA) review process for certain active medical devices with known vulnerabilities; and (3) determine what postmarket efforts FDA has in place to identify information security problems involving active implantable medical devices.

To identify the threats, vulnerabilities, and resulting information security risks associated with active implantable medical devices, we reviewed available publications, such as white papers published by information security researchers and peer-reviewed journal articles. We reviewed these publications to identify an initial list of threats, vulnerabilities, and resulting information security risks associated with these types of medical devices. These publications also included information related to the two devices that researchers have demonstrated are susceptible to intentional threats—an implantable cardioverter defibrillator (defibrillator) and an insulin pump. We also obtained relevant information through interviews with officials from federal agencies, including from FDA, the Department of Health and Human Services (HHS), the National Institute of Standards and Technology (NIST) within the Department of Commerce, the Department of Defense, the Department of Homeland Security (DHS), the Department of Veterans Affairs, and the Federal Communications Commission (FCC). We also interviewed manufacturer officials and subject-matter experts, including information security researchers and authors of standards related to information security. After developing these initial lists of threats, vulnerabilities, and information security risks, we sent them to experts to obtain their concurrence and comments. We selected these experts on the basis of their knowledge and familiarity with the information security of medical devices. Of the 15 experts to whom we sent our tables, 9 provided us with responses. We then analyzed these responses to validate our identified threats, vulnerabilities, and resulting information security risks associated with these medical devices. We did not include implantable medical devices lacking active components, such as hip implants. We limited our identification of threats, vulnerabilities, and information security risks to those associated with medical devices that deliver medicine, monitor body functions, or provide support to organs and tissues. Additionally, we limited our scope to the integrity and availability aspects of information security—which generally relate to the safety and effectiveness of medical devices—and not confidentiality, which generally relates to privacy. We focused on the potential effect that information security risks could have on the functionality of FDA-regulated

devices and not on their ability to store or exchange personally identifiable information.

To determine the extent to which FDA considered information security risks in its PMA review for two medical devices with known vulnerabilities, we reviewed FDA's recommended guidance documents related to information security issues. We also reviewed national guidelines, such as those developed by NIST, and international standards, such as those developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), related to information security.¹ These national guidelines and international standards include those recommended by FDA to manufacturers for use when designing and developing medical devices as well as others applicable to information security in general and to other areas, such as federal information and information systems. These guidelines and standards also include

- NIST Special Publication 800-40, *Creating a Patch and Vulnerability Management Program*;²
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*;³
- NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*;⁴

¹The ISO is a nongovernmental organization that develops and publishes international standards, including those related to information security through a consensus-based process involving a network of the national standards bodies of 164 countries. The organization uses "ISO" as the official short-form name because it would have different acronyms depending on the language used. The IEC publishes international standards for electrical, electronic, and related technologies. Its membership includes national committees from over 70 nations, which are comprised of representatives from each country's public or private sectors.

²NIST, *Creating a Patch and Vulnerability Management Program*, SP 800-40 Version 2.0 (Gaithersburg, Md.: November 2005).

³NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 3 (Gaithersburg, Md.: August 2009).

⁴NIST, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, SP 800-66 Revision 1 (Gaithersburg, Md.: October 2008).

- IEC 62304: 2006, *Medical Device Software—Software Life Cycle Processes*;⁵
- IEC 60601-1: 2005, *Medical Electrical Equipment—Part 1: General Requirements for Basic Safety and Essential Performance*;⁶
- IEC Standard 80001-1: 2010, *Application of Risk Management for IT Networks Incorporating Medical Devices—Part 1: Roles, Responsibilities and Activities*;⁷
- ISO, International Standard 14971: 2007, *Medical Devices—Application of Risk Management to Medical Devices*;⁸
- DHS, *Recommended Practice for Patch Management of Control Systems*;⁹
- PCI Security Standards Council, *Payment Card Industry Data Security Standard*;¹⁰ and
- various FDA guidance documents.

⁵Association for the Advancement of Medical Instrumentation, *Medical Device Software—Software Life Cycle Processes*, ANSI/AAMI/IEC 62304:2006 (Arlington, Va.: June 2006).

⁶Association for the Advancement of Medical Instrumentation, *Medical Electrical Equipment—Part 1: General Requirements for Basic Safety and Essential Performance*, ANSI/AAMI ES60601-1:2005 (Arlington, Va.: February 2006).

⁷Association for the Advancement of Medical Instrumentation, *Application of Risk Management for IT Networks Incorporating Medical Devices—Part 1: Roles, Responsibilities and Activities*, ANSI/AAMI/IEC 80001-1:2010 (Arlington, Va.: October 2010).

⁸Association for the Advancement of Medical Instrumentation, *Medical Devices—Application of Risk Management to Medical Devices*, ANSI/AAMI/ISO 14971:2007/(R)2010 (Arlington, Va.: October 2010).

⁹DHS, National Cyber Security Division Control Systems Security Program, *Recommended Practice for Patch Management of Control Systems* (Idaho: December 2008).

¹⁰PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessments Procedures, Version 2.0* (Wakefield, Mass.: October 2010).

These documents varied in detail from providing general rules at a high level to specific activities related to information security. From these documents, we determined the key information security controls and associated criteria that could be used to assess and mitigate information security risks for certain active medical devices.¹¹ We did not conduct an extensive analysis of all information security controls that could be used in the evaluation of information security issues for these medical devices. Instead, we focused on eight key information security control areas that included a range of criteria that would be applicable when evaluating FDA's review of information security risks in its PMA review process. The specific areas we selected were (1) software testing, verification, and validation; (2) risk assessments; (3) risk management; (4) access control; (5) patch and vulnerability management; (6) security-incident response; (7) contingency planning; and (8) technical audit and accountability. For each of these information security control areas, we selected the criteria that illustrated the range of activities that could be considered by FDA during its PMA review process.

We then used these key information security control areas and associated criteria to develop a questionnaire for FDA to complete on the basis of its prior review of two PMA supplement applications (supplements).¹² Our selection of supplements was informed by devices that have recently identified vulnerabilities, such as those devices that information security researchers have exploited in controlled settings, and discussions with FDA. We reviewed the PMA supplements rather than the original PMA applications in order to capture the most recent information related to these two devices.

¹¹Information security control areas are categories related to multiple information security controls. These controls include specific criteria that when implemented can help mitigate information security risks.

¹²After an original PMA application is approved, a manufacturer can submit a supplement to the original PMA application to FDA for approval of changes, such as changes to the device or the manufacturing process used in its production. In general, subsequent changes that affect the safety or effectiveness of the device must undergo FDA's PMA review process and manufacturers must submit a supplement to their original application for approval.

We evaluated FDA's responses to this questionnaire and supporting documentation, such as FDA's review memorandums and other documents submitted by the manufacturer. FDA provided responses for one supplement related to the defibrillator exploited by information security researchers and responses and documentation for the programming wand (wand) and the programmer used with the defibrillator.¹³ FDA also provided responses and documentation for a second supplement related to the exploited insulin pump.¹⁴ The particular defibrillator and insulin pump we considered in our evaluation are the only two devices we identified that have been intentionally exploited by researchers. Although the defibrillator-related supplement was reviewed in 2001 and the insulin pump supplement was reviewed in 2006, FDA identified these supplements as being the most recent ones related to the devices involving potential information security issues and the most appropriate for our evaluation. We also evaluated additional documentation for another defibrillator reviewed by FDA in 2012 that has not been intentionally exploited by researchers to obtain a more current perspective on FDA's review process for information security issues. Because we evaluated documentation for only three devices, our results are not generalizable. We also interviewed FDA officials about the agency's current efforts to address information security risks in medical devices during its premarket review.

To determine what postmarket efforts FDA has in place to identify information security problems involving active implantable medical devices, we obtained and reviewed FDA guidance documents related to different postmarket efforts, including *Medical Device Reporting for Manufacturers*, *Draft Guidance for Industry and FDA Staff: Annual Reports for Approved Premarket Approval Applications (PMA)*, and *Guidance for Industry and FDA Staff: Procedures for Handling Post-*

¹³A wand is an external device that connects to a programmer—a specialized computer that records data from the device—in this case the defibrillator. The wand, also called a programmer head, is held within inches of the defibrillator. The wand facilitates the communication between the programmer and the defibrillator to, for example, make adjustments to the device. Also, this supplement was submitted to FDA for approval of the wand and programmer software used in conjunction with the defibrillator.

¹⁴This supplement was submitted to FDA for approval of modifications to the insulin pump to, in part, allow it to accept data from a sensor, which captures glucose measurements.

*Approval Studies Imposed by PMA Order.*¹⁵ We also reviewed FDA information related to its adverse event reporting system, including the different codes FDA uses to characterize different types of adverse events. We requested that FDA search its adverse event reporting system for any potential information security problems involving these medical devices using 10 codes that FDA had stated could potentially indicate an information security problem had occurred. We then reviewed FDA's other codes on its website to determine whether there were any additional codes that could be used to identify information security problems. We identified these codes using key words or phrases that we considered possibly related to information security. We then asked FDA to search its adverse event reporting system using the additional codes that we identified as possibly related to information security. We did not independently verify FDA's results for any of its searches. We obtained and reviewed the manufacturer's annual reports for the defibrillator for the years 2008 through 2011, after researchers demonstrated the intentional exploitation of the device in controlled settings in 2008. We also reviewed manufacturer's annual reports for the insulin pump for 2010 and 2011, after researchers demonstrated the intentional exploitation of the device in controlled settings in 2010. We reviewed these reports to determine whether they included any indication of these demonstrations. Additionally, we interviewed FDA officials in its Office of Surveillance and Biometrics and Office of Device Evaluation, among others, on the agency's different postmarket efforts, including its adverse event reporting system and postmarket studies, to determine how FDA has identified or might identify information security problems through these and other efforts. We also interviewed officials from relevant industry associations, including the Medical Device Manufacturers Association and Advanced Medical Technology Association, and officials from other agencies, including DHS and FCC, about challenges associated with identifying information security problems, including those specific to the issue of information security and those inherent to FDA and its adverse event reporting system.

¹⁵FDA, *Draft Guidance for Industry and FDA Staff: Annual Reports for Approved Premarket Approval Applications (PMA)* (Rockville, Md.: Oct. 26, 2006) and *Guidance for Industry and FDA Staff: Procedures for Handling Post-Approval Studies Imposed by PMA Order* (Rockville, Md.: June 15, 2009).

We conducted this performance audit from August 2011 to August 2012, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: FDA's Adverse Event Reporting Systems

The submission of adverse event reports is intended to enable the Food and Drug Administration (FDA) to collect information regarding reportable issues with medical devices. FDA seeks to use reports submitted by manufacturers and user facilities, among others, to assess the underlying cause and seriousness of an adverse event.¹ FDA also uses adverse event data to identify issues with medical devices that may require additional investigation. According to FDA, adverse event reports are best used for two purposes. First, they are used to capture qualitative snapshots of adverse events for a particular device or device type, such as the types of malfunctions or clinical events or both associated with the device. Second, they are used in signal detection, such as for identifying unexpected events associated with a particular device or device type.

Adverse event reports are to be submitted to FDA through mandatory and voluntary sources. Mandatory adverse event reporting by manufacturers and user facilities enables FDA to obtain specific safety data related to medical devices from these reporters. Since 1984, the Medical Device Reporting regulations have required manufacturers and user facilities who have received complaints of device-related deaths, serious injuries, and malfunctions, such as instances where patients required admission to the hospital or became permanently disabled, to notify FDA.² (See table 7 for summaries of these reporting requirements.) These mandatory adverse event reports are entered into FDA's Manufacturer and User Facility Device Experience Database (MAUDE). FDA also collects data obtained through voluntary adverse event reporting.

¹A user facility is a hospital, ambulatory surgical facility, nursing home, outpatient diagnostic facility, or outpatient treatment facility that is not a physician's office.

²21 C.F.R. pt. 803. Also, serious injuries are defined as life-threatening events, events that result in permanent impairment of a body function or permanent damage to a body structure, and events that require medical or surgical intervention to preclude permanent impairment or damage. Malfunctions are defined as the failure of a device to meet its performance specifications or otherwise not perform as intended. Device-related means that the event was or may have been attributable to a medical device, or that a device was, or may have been, a factor in an event including those occurring as a result of device failure, malfunction, improper or inadequate design, poor manufacture, inadequate labeling, or use-related error.

Appendix II: FDA's Adverse Event Reporting Systems

Table 7: Summary of Reporting Requirements for Manufacturers and User Facilities

Reporter	What to report	To whom	When
Manufacturer	30-day reports of deaths, serious injuries and malfunction. ^a	FDA	Within 30 calendar days from becoming aware of an event
Manufacturer	5-day reports on events that require remedial action to prevent an unreasonable risk of substantial harm to the public health and other types of events designated by FDA	FDA	Within 5 work days from becoming aware of an event
Manufacturer	Baseline reports to identify and provide basic data on each device that is subject of an adverse event report.	FDA	With 30 calendar and 5 work day reports when device or device family is reported for the first time. Interim and annual updates are also required if any baseline information changes after initial submission.
User facility ^a	Death	FDA and Manufacturer	Within 10 work days
User facility	Serious injury ^b	Manufacturer, FDA only if manufacturer unknown	Within 10 work days
User facility	Annual reports of death and serious injury ^c	FDA	January 1

Source: FDA.

^aA user facility is a hospital, ambulatory surgical facility, nursing home, outpatient diagnostic facility, or outpatient treatment facility that is not a physician's office.

^bSerious injuries are defined as life-threatening events, events that result in permanent impairment of a body function or permanent damage to a body structure, and events that require medical or surgical intervention to preclude permanent impairment or damage. Malfunctions are defined as the failure of a device to meet its performance specifications or otherwise not perform as intended.

^cUser facilities are required to file annual reports that summarize their adverse event reports. 21 C.F.R. pt. 803, Subpart C.

In addition to MAUDE, FDA has other adverse event reporting systems in place to capture adverse events associated with medical devices. One of these is the Medical Product Safety Network (MedSun) system. MedSun collects voluntary report information from a limited number of hospitals and user facilities. All reports received through MedSun are entered into the MAUDE system. Launched in 2002, the primary goal of MedSun is to enable FDA to work collaboratively with specific device-user facilities in the clinical community to identify, understand, and solve problems with the use of devices. MedSun user facilities are required to report device problems that result in serious illness, injury, or death. MedSun user facilities are also encouraged to voluntarily report other types of problems with devices, such as "close-calls," potential for harm, and other safety concerns. Once a problem has been identified, FDA works with the MedSun user facilities' representatives to clarify and understand the problem. Subsequent reports and lessons learned from these collaborations are then shared with the greater clinical community so that

all clinicians may take necessary preventative actions to address device problems. Currently, 350 user facilities participate in the MedSun network. Participants are recruited from all regions of the country using the American Hospital Association Membership Listing.³

FDA's voluntary adverse event reporting system, MedWatch, was created in 1993 to encourage voluntary reporting by interested parties, such as consumers of medical devices, and health care professionals, such as physicians. These parties can use MedWatch to report serious adverse reactions, product quality problems, therapeutic failure, and product-use errors associated with human medical products, including drugs, biologic products, and medical devices, among other things. Consumers can submit information about their experiences either online or by fax, mail, or phone. Consumers can also request that their physicians either complete the MedWatch form for them or help them complete the form, given that these providers have test results and other clinical information that will help FDA better evaluate the MedWatch reports.

Adverse event reports submitted to FDA through MedSun or MedWatch are eventually entered into MAUDE. MAUDE data consist of voluntary reports since June 1993, user-facility reports since 1991, distributor reports since 1993, and manufacturer reports since 1996. MAUDE may not include reports made according to exemptions, variances, or alternative reporting forms authorized by regulation. FDA is in the process of developing a new system to replace MAUDE, the FDA Adverse Event Reporting System, which the agency plans to implement by September 2013. According to FDA, this new system will perform similar functions as MAUDE, but will also allow for (1) greater capacity for storing adverse event data, and (2) greater search capability than MAUDE.

³The American Hospital Association is the national organization that represents and serves all types of hospitals, health care networks, and their patients and communities. This organization consists of almost 5,000 hospitals, health care systems, networks, and other providers as well as 40,000 individual members, which are listed in a member directory on its website.

Appendix III: OCR and ONC Responsibilities Related to Information Security

Two federal entities that have specific responsibilities related to developing and implementing policies with respect to the confidentiality aspect of information security in terms of protected health information. These entities are the Office for Civil Rights (OCR) and the Office of the National Coordinator for Health Information Technology (ONC), both within the Department of Health and Human Services (HHS).

OCR

OCR is responsible for developing, interpreting, and enforcing the Privacy and Security Rules called for in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).¹ OCR enforces the Privacy and Security Rules by investigating complaints that individuals have filed with the Office in instances where they believe a covered entity violated health information privacy rights or committed another violation of the rules.² OCR may also conduct periodic audits to ensure that covered entities are in compliance with Privacy and Security Rules. In calendar year 2011, OCR conducted a total of 3,898 investigations. Of these investigations, OCR determined no violation had occurred in 33 percent of them (1,303 investigations) and, for the remaining 67 percent (2,595 investigations), obtained corrective action. OCR has also issued guidance documents for covered entities on how to comply with the HIPAA Privacy and Security Rules.³

¹Congress passed HIPAA to, among other things, provide for national standards to facilitate the electronic transmission of health information as well as standards to protect the privacy and security of individuals' health information. HHS promulgated Privacy and Security Rules to implement the act. HIPAA's Privacy and Security Rules define the circumstances under which protected health information may be used and disclosed by covered entities to other entities. To ensure that this protected health information is not subject to unauthorized access, the Security Rule specifies a series of administrative, technical, and physical security safeguards for covered entities to implement to ensure the confidentiality of electronic protected health information. 45 C.F.R. §§ 164.302-164.318.

²Covered entities are defined as health plans that provide or pay for the medical care of individuals, health care providers that electronically transmit health information in connection with any of the specific transactions regulated by the subchapters of the *Code of Federal Regulations* containing the Security and Privacy Rules, and health care clearinghouses that receive health information from other entities and process or facilitate the processing of that information into standard or nonstandard format for those entities. 45 C.F.R. § 160.103.

³For example, OCR, *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (Washington, D.C.: July 2010). OCR also conducts education and outreach to foster compliance with the rules.

ONC

ONC was formally established by the Health Information Technology for Economics and Clinical Health Act of 2009 (HITECH Act).⁴ It is charged with promoting the development of a nationwide health information technology (IT) infrastructure that allows the secure exchange of health information. For example, ONC has developed a federal health IT strategic plan for working with the private and public sectors to implement different health IT efforts.⁵ In this plan ONC addresses, among other things, privacy and security issues related to health IT. The plan also includes strategies related to identifying health IT system security vulnerabilities as well as health IT privacy and security requirements and best practices. ONC has also developed the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* in order to establish a policy framework for electronic health information exchange to help guide nationwide adoption of health IT and help improve the availability of health information and health care quality.⁶ ONC also assesses gaps and weaknesses in current privacy and security policies in light of evolving technology, and works with federal entities to address these issues. Additionally, ONC incorporates privacy and security in its programs, which are designed to implement HITECH initiatives, including certification of electronic health records, as well as supporting the efforts of several related initiatives to facilitate nationwide adoption of health IT. For example, one initiative relates to developing information security and best practices for safeguarding protected health information in electronic health records, while another initiative relates to identifying standards, protocols, legal agreements, specifications, and services, to enable secure health information exchanges.

⁴The HITECH Act was enacted as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act. Pub. L. No. 111-5, Div. A, Tit. XIII, 123 Stat. 115, 226-279 and Div. B, Tit. IV, 123 Stat. 115, 467-496 (Feb. 17, 2009). Among other things, it promotes the use of health IT and strengthens certain privacy and security requirements.

⁵ONC, *Federal Health Information Technology Strategic Plan: 2011-2015* (Washington, D.C.: September 2011).

⁶ONC, *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (Washington, D.C.: December 2008).

Appendix IV: GAO Evaluation of FDA's Consideration of Information Security in Its Review of Two PMA Supplements

Table 8 includes the results of our evaluation of the evidence provided by the Food and Drug Administration (FDA) regarding its consideration of information security in its review of two premarket approval (PMA) supplements reviewed in 2001 and 2006 related to active medical devices with known vulnerabilities. Specifically, the supplements and supporting materials were for a defibrillator and its associated programming wand (wand) and programmer, and a specific insulin pump with wireless capabilities. This evidence was provided to FDA in the respective PMA supplements to the original applications by the manufacturer.¹

Although the defibrillator-related supplement was reviewed in 2001 and the insulin pump supplement was reviewed in 2006, FDA officials identified these supplements as being the most recent ones related to the devices involving potential information security issues and the most appropriate for our evaluation.

¹After an original PMA application is approved, a manufacturer can submit a supplement to the original PMA application to FDA for approval of changes, such as changes to the device or the manufacturing process used in its production. In general, subsequent changes that affect the safety or effectiveness of the device must undergo FDA's PMA review process and manufacturers must submit a supplement to their original application for approval.

Table 8: GAO Evaluation of FDA's Consideration of Information Security in Its Review of Two PMA Supplements

Selected information security control areas and criteria	GAO's evaluation
<p>1. Software testing, verification, and validation</p> <p>The manufacturer should test all software requirements through a variety of test methods. Such testing should include</p> <ul style="list-style-type: none"> • addressing issues related to information security vulnerabilities such as: <ul style="list-style-type: none"> • immunity from radio-frequency interference, • telemetry (remote transmission of data), and • electromagnetic compatibility (correct operation and avoidance of electromagnetic interference); • validating that software specifications conform to user needs and intended uses and verify that software requirements are consistently fulfilled, including planning, traceability, configuration management, and information security vulnerabilities; and • reporting on problems detected in the product, classified by type, scope, and criticality. 	<p>Defibrillator/Wand/Programmer:</p> <p>FDA demonstrated evidence of review of software testing, verification, and validation for the wand and software, including:</p> <ul style="list-style-type: none"> • a variety of test methods testing new and updated features of the wand, such as software testing, firmware testing, and system testing, which includes compatibility testing, technical-manual review, and anomaly inducement; and • verification and validation addressing issues related to unintentional information security vulnerabilities such as <ul style="list-style-type: none"> • radio-frequency interference and immunity from interference, • telemetry modes and issues with transmission of data, and • electromagnetic compatibility. <p>FDA did not provide evidence that it had reviewed the following:</p> <ul style="list-style-type: none"> • The original software testing, verification, or validation for the defibrillator itself. • Any security-specific requirements, such as <ul style="list-style-type: none"> • code protection; • security functionality verification; • software and information integrity, other than testing for unintentional information security threats related to issues such as information exchange; • information input validation, including providing invalid, unexpected, or random data and monitoring for crashes, other than anomaly-inducement testing; • failing built-in code assertions; or • finding potential memory leaks which would help identify security problems. • Software problem reports created by the manufacturer in the event of an issue, such as an information security-related vulnerability. <p>According to FDA, software testing would have been done with the original submission for the defibrillator. Also, FDA noted that the mitigations for this version of the software and programmer are related to access and proximity. FDA explained that this device and programmer can only work together as a pair when they are in close proximity. However, FDA did not provide us with any documentation of its software testing and that close proximity specifically addresses security-specific requirements, such as code protection.</p>

**Appendix IV: GAO Evaluation of FDA's
Consideration of Information Security in Its
Review of Two PMA Supplements**

**Selected information security control areas and
criteria**

GAO's evaluation

Insulin pump:

FDA demonstrated evidence of review of software testing, verification, and validation that included

- software requirements for both the pump and software used to download data from the pump to a computer;
- testing of radio-frequency software specifications;
- testing of remote setup and use;
- testing for electromagnetic compatibility;
- testing procedures and results, and traceability of testing results to specifications requirements; and
- problem reports for anomalies identified during software testing, including requests for additional information and consultation with subject-matter experts.

FDA demonstrated limited evidence of review of security-specific requirements that addressed

- a few cases of input data validation and
- general requirements to establish a firewall and intrusion-detection system.

FDA did not provide evidence that the manufacturer's testing included software-security testing for

- code protection;
- security functionality verification;
- information integrity;
- providing invalid, unexpected, or random data and monitoring for crashes;
- failing built-in code assertions; or
- finding potential memory leaks that would help identify security problems.

Further, FDA did not provide evidence showing a review of the software manufacturer's test results. In addition, the requirements did not address detailed examples of data validation such as verifying boundary parameters or specific configuration requirements for the firewall and intrusion detection system.

According to FDA, the agency was unaware of any evidence of intentional threats to these devices at the time of the review and, therefore, this concern was not considered.

**Appendix IV: GAO Evaluation of FDA's
Consideration of Information Security in Its
Review of Two PMA Supplements**

Selected information security control areas and criteria

GAO's evaluation

2. Risk assessments

Manufacturers should

- perform a risk analysis as early as possible to determine how the device could cause harm. The risk analysis should include
 - a review of the hazards,
 - severity of harm,
 - possible causes of adverse outcomes (including those originating with radio-frequency wireless systems), and
 - risk-control measures to reduce risks.

Defibrillator/Wand/Programmer

FDA provided evidence that it had reviewed the risk analysis, including

- a review of the hazards;
- possible causes of adverse outcomes of hazards such as electromagnetic fields, electromagnetic interference, and possible corruption of data of the wand and its telemetry electronics module; and
- risk-control measures to reduce risks, such as software integrity checks.

FDA stated that the determination of likelihood and effect of hazards, which may address severity of harm, were not assigned nor requested from the manufacturer.

FDA did not demonstrate evidence of review of intentional information security issues such as the vulnerabilities that have been exploited. FDA did not review or request information from the manufacturer showing that information security-related risks had been considered, such as those dealing with information security vulnerabilities that could be exploited by intentional threats. Further, FDA stated that it did not consider intentional information security hazards during its review.

Insulin pump:

FDA demonstrated evidence of review of risk analysis that included

- a review of the hazards;
- severity of harm;
- possible adverse outcomes including those dealing with radio-frequency wireless systems and electromagnetic interference, review of software misconfiguration issues, and possible corruption of data; and
- risk-control measures to reduce risks including software-integrity checks; however, several of the risk-control measures relied primarily on proper user training.

FDA did not demonstrate evidence of review of intentional information security issues such as the vulnerabilities that have been exploited. FDA did not review or request information from the manufacturer showing that information security-related risks had been considered, such as those dealing with information security vulnerabilities that could be exploited by intentional threats. Further, FDA stated that it did not consider intentional information security hazards during its review.

FDA did not request additional information for an anomaly dealing with a lack of input filtering. FDA did not request that the manufacturer correct this problem.

**Appendix IV: GAO Evaluation of FDA's
Consideration of Information Security in Its
Review of Two PMA Supplements**

Selected information security control areas and criteria	GAO's evaluation
<p>3. Risk management</p> <p>The manufacturer should establish, document, and maintain an ongoing process for</p> <ul style="list-style-type: none"> • identifying hazards or risks associated with a medical device, • estimating and evaluating the associated risks, • undertaking risk-control activities, and • monitoring the effectiveness of the controls during and after the production of the device. 	<p>Defibrillator/Wand/Programmer:</p> <p>FDA did not provide evidence of review of an ongoing risk-management process that would include intentional information security threats.</p> <p>However, according to FDA, there is no context for an ongoing review of risk management. Subsequent changes to a device would be provided to FDA by the manufacturer for review in future submissions.</p> <hr/> <p>Insulin pump:</p> <p>FDA did not provide evidence of review of an ongoing risk-management process that would include intentional information security threats.</p> <p>However, according to FDA, there is no context for an ongoing review of risk management. Subsequent changes to a device would be provided to FDA by the manufacturer for review in future submissions.</p>
<p>4. Access Control</p> <p>The manufacturer should describe the means in which the device can be accessed and develop access-control policies. This can include processes for</p> <ul style="list-style-type: none"> • authorizing access; • selecting the basis for restricting access; • selecting the access-control method (e.g., identity-based, role-based, or other reasonable and appropriate means of access); and • protection against or limits on the effects of denial of service attacks. <p>The manufacturer should establish appropriate controls for</p> <ul style="list-style-type: none"> • protection against unauthorized wireless access to device control or data and • limitations or restrictions for proper operation and wireless communications. <p>Manufacturers should establish emergency access procedures, and describe</p> <ul style="list-style-type: none"> • if systems automatically default to settings and functionalities, or if the emergency mode would be activated by an authorized individual, and • who is authorized to have emergency access. 	<p>Defibrillator/Wand/Programmer:</p> <p>FDA provided limited evidence that it had evaluated the manufacturer's means to appropriately restrict access to the defibrillator, programmer, and wand. Specifically, FDA stated that it had determined that</p> <ul style="list-style-type: none"> • a primary means of restricting access to the programmer and implanted defibrillator is that both are obtained by prescription only and only used together in health care facilities; and • physical proximity is an access-control method since the wand must be in close proximity to the defibrillator to connect to and access the data on the defibrillator. <p>FDA provided limited evidence that the manufacturer addressed controls to prevent unauthorized wireless access to device control or data. This included</p> <ul style="list-style-type: none"> • a summary discussion of the pairing mechanism used by all defibrillators to link a programmer to a defibrillator. FDA stated that it would have reviewed the specific pairing method for the programmer and defibrillator in the original submission, and neither the original submission nor evidence of security-specific access controls for pairing was provided for review. <p>FDA stated that it reviewed emergency access procedures in the original review of the defibrillator. This review would have included</p> <ul style="list-style-type: none"> • the defibrillator's emergency pacing modes that will be initiated in the event of failure, • default programming modes that can be initiated by the defibrillator itself in the case of emergency (such as an error state), and • a physician's ability to initiate pacing or defibrillation in an emergency. <p>However, the original review was not provided to us.</p> <p>FDA did not provide documentation to demonstrate its review of the defibrillator's protection against or limits of the effects of denial of service attacks.</p>

**Appendix IV: GAO Evaluation of FDA's
Consideration of Information Security in Its
Review of Two PMA Supplements**

Selected information security control areas and criteria

GAO's evaluation

Insulin pump:

FDA provided limited evidence that it had evaluated the manufacturer's means to appropriately restrict access to the device. Specifically,

- FDA stated this is a prescription-use-only device and the primary user is the patient; as a result, access for the insulin pump is typically not restricted, except for a lock-out mechanism for pediatric patients.

FDA did not provide any documentation to show

- protection against unauthorized wireless access to the pump,
- control or data limitations or restrictions,
- selecting the access-control method,
- protection against unauthorized wireless access to device control or data, or
- limitations or restrictions for proper operation and wireless communications.

FDA did not address emergency access procedures in its review. The agency stated that instructions and training for insulin pumps typically include use of manual injections of insulin as a backup in the event the device fails.

FDA stated that at the time of this PMA review, FDA guidance for software or infusion pumps did not identify the need to address information security risks, therefore, the review did not address access controls. Further, FDA did not provide documentation to demonstrate its review of the device's protection against or limits on the effects of denial-of-service attacks.

5. Patch and vulnerability management

An organization should have a process for identifying and addressing vulnerabilities and implementing patches.

Defibrillator/Wand/Programmer:

FDA did not provide evidence that the manufacturer had demonstrated a process for identifying and addressing newly-identified vulnerabilities and implementing patches as part of this PMA supplement.

According to FDA, as patches or vulnerabilities are identified, there are several regulatory strategies that can be followed depending on the perceived severity of risk, including changes to all new devices, a plan to changed devices in the field, or a combination. However, FDA did not provide evidence of having implemented such a strategy for this or other medical devices.

Insulin pump:

FDA did not provide evidence that the manufacturer had demonstrated a process for identifying and addressing newly-identified vulnerabilities and implementing patches. For example, as of 2008 the programming language used to create the software for the insulin pump was no longer supported.

According to FDA, subsequent changes to a device would be provided to FDA by the manufacturer for review in future submissions.

**Appendix IV: GAO Evaluation of FDA's
Consideration of Information Security in Its
Review of Two PMA Supplements**

Selected information security control areas and criteria

GAO's evaluation

6. Technical audit and accountability

The manufacturer should

- determine what activities will be tracked or audited, including what data needs to be captured;
- determine what activities will be monitored (e.g., creation, reading, updating, or deleting, or a mix of the above, files or records);
- review and analyze information-system audit records for indications of inappropriate or unusual activity; and
- report findings to designated officials.

Defibrillator/Wand/Programmer:

FDA stated that the implanted defibrillator does contain a log to help to understand how the defibrillator has performed over time. FDA stated this log is primarily reviewed in the context of patient treatment, not information security issues.

Although FDA stated that this defibrillator has a log that tracks how the defibrillator has performed over time, evidence of this log was not found in any of the attachments provided by FDA.

Also, details of the log were not discussed, including if the manufacturer determined

- what activities will be tracked or audited, including what data needs to be captured;
- what activities will be monitored (e.g., creation, reading, updating, or deleting, or a mix of the above, files or records);
- how to review and analyze information-system audit records for indications of inappropriate or unusual activity; and
- how to report finding to designated officials.

The application for the programmer and the defibrillator did not include a review of the event log components as these were unchanged from previous versions.

Insulin pump:

FDA did not provide any documentation showing it had reviewed the manufacturer's audit and accountability documentation. FDA stated that insulin pumps typically include an event log, which identifies device actions. The time period available for review is limited by the hardware used on the device. However, the capabilities for the device log in this premarket approval are not clear. Specifically, no details were provided regarding if the manufacturer determined

- what activities will be tracked or audited, including what data needs to be captured;
- what activities will be monitored (e.g., creation, reading, updating, or deleting, or a mix of the above, files or records);
- how to review and analyze information-system audit records for indications of inappropriate or unusual activity; and
- how to report finding to designated officials.

According to FDA, some of the activities listed for this control area are not typically addressed in premarket review, but in the continuous monitoring of the device's performance once it is in use. However, the agency did not provide evidence of having implemented a process dealing with the monitoring of this particular device.

Selected information security control areas and criteria

GAO's evaluation

7. Security-incident response

Defibrillator/Wand/Programmer:

- The manufacturer should
- determine what constitutes a security incident,
 - determine how the manufacturer will respond to an incident,
 - establish a reporting mechanism and a process to coordinate responses, and
 - provide direct technical assistance to other entities involved.
- In addition, the manufacturer should
- identify and respond to suspected or known security incidents;
 - mitigate, to the extent practicable, harmful effects of security incidents that are known to the manufacturer; and
 - document security incidents and their outcomes.

- For incident response
- FDA interpreted the term "incident" to mean either manufacturing-process errors or medical-device errors.
- FDA reported that it did not review if the manufacturer had adequate policies or procedures that address goals of incident response. FDA stated that its regulations do not specifically identify a requirement to review security incidents. However
- a manufacturer is required to review every complaint that is made for its device; and
 - procedures to review complaints made for the defibrillator or programmer would have been reviewed as part of FDA's regulations regarding device manufacture which would have been done on the original premarket approval submission.

Insulin pump:

FDA provided evidence that the manufacturer's application provided evidence of a call center. However, FDA stated that they did not explicitly require that the call center be prepared to address information security incidents. FDA stated that at the time of this premarket approval review, FDA guidance for software or infusion pumps did not identify the need to address information security. FDA did not provide evidence that they evaluated the manufacturer's security-incident response process.

According to FDA, the premarket review would not typically cover the manufacturer's response to a device-related incident. Such information would likely be covered in manufacturer documents that address all device-related events and are not specific to information security. However, FDA did not provide us with such documentation.

8. Contingency Planning

Defibrillator/Wand/Programmer:

- The manufacturer should
- identify preventive measures for each defined scenario that could result in a loss of critical performance by the device;
 - finalize the set of contingency procedures that should be invoked for all identified effects, including emergency mode operation;
 - develop backup requirements; and
 - restore lost data.

According to FDA, the manufacturer identified certain preventative measures for the defibrillator, including a fail-safe mode that allows the defibrillator to continue to function effectively when an error or failure occurs; however, these measures were not provided for our review.

For the wand application, the manufacturer

- considered fail-safe scenarios related to unintentional information security threats, such as power loss, communication loss, and programmer and wand operation under various conditions that could result in a loss of critical performance and tested these scenarios; and
- described emergency programming that can be performed as part of contingency procedures.

FDA stated that appropriate back up requirements for the defibrillator were not reviewed for this device submission.

**Appendix IV: GAO Evaluation of FDA's
Consideration of Information Security in Its
Review of Two PMA Supplements**

**Selected information security control areas and
criteria**

GAO's evaluation

Insulin pump:

According to FDA, the manufacturer

- had identified certain preventative measures for defined scenarios that could result in a loss of critical performance by the device based on unintentional threat; for example, if the battery were depleted, an alarm would sound to notify the user to change the batteries. The manufacturer had also tested for malfunction related to unintentional hardware issues and included an example of testing to prevent over-delivery; and
- had provided a means to back up the software data.

FDA stated that it did not address whether the manufacturer had developed data backup plan requirements for the device or if the manufacturer could restore any lost data to the device.

While FDA did not provide any documentation showing a review of the manufacturer's contingency planning documents for the device, agency officials stated that if the device were to fail, the patient would manually inject the insulin.

Source: GAO analysis of FDA documentation and responses to GAO questionnaire.

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



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

Marcia Crosse, Director
Health Care
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

AUG 14 2012

Dear Ms. Crosse:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "MEDICAL DEVICES: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices" (GAO 12-816).

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

Sincerely,

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

Jim R. Esquea
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED "MEDICAL DEVICES: FDA SHOULD EXPAND ITS CONSIDERATION OF INFORMATION SECURITY FOR CERTAIN TYPES OF DEVICES" (GAO-12-816)

The Department appreciates the opportunity to review and comment on this draft report.

The principles of data security are well established, and a range of possible mitigations to address medical device confidentiality, integrity, and availability concerns are also well-known in the software engineering community. To ensure the safety and effectiveness of active implantable medical devices as technology evolves, HHS concurs with GAO that the Agency continuously develop and implement new strategies designed to assist the agency in its medical device premarket review and postmarket surveillance efforts relative to information security. As described in GAO's report, the Center for Devices and Radiological Health (CDRH) at FDA has taken steps to identify and address information security concerns to ensure the safety of medical device products.

GAO Recommendation:

That FDA develop and implement a more comprehensive plan to assist the agency in enhancing its review and surveillance of medical devices, as technology evolves, and that will incorporate the multiple aspects of information security.

This plan should include, at a minimum, four actions, such as determining how FDA can:

- *increase its focus on manufacturers' identification of potential unintentional and intentional threats, vulnerabilities, and resulting information security risk, and strategies to mitigate these risks during its PMA review process;*
- *utilize available resources, including those from other entities, such as other federal agencies;*
- *leverage its postmarket efforts to identify and investigate information security problems; and*
- *establish a specific schedule for completing this review and implementing these changes.*

FDA continues to identify and leverage available resources, including those from other entities and federal agencies in an effort to ensure the Agency keeps pace with technological innovation. Current efforts include establishing collaborative relationships with the Department of Homeland Security, the National Institute of Standards and Technology, the Department of Defense, and federal law enforcement agencies.

CDRH continues to examine its consensus standards strategy in the area of wearable and implanted devices including exploring the possibility of using and adapting available standards from other cyberphysical system sectors such as industrial control. The Center has engaged with stakeholders to begin the process of studying what is available from other sectors and, where appropriate, tailoring it to the health sector.

One area of focus in device postmarket efforts involves evaluating and enhancing surveillance tools that will identify and investigate information security problems. For example, CDRH is in

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED "MEDICAL DEVICES: FDA SHOULD EXPAND ITS CONSIDERATION OF INFORMATION SECURITY FOR CERTAIN TYPES OF DEVICES" (GAO-12-816)

the process of releasing its "National Postmarket Surveillance Plan" designed to strengthen national coordination of information sharing for adverse events related to medical devices. Additionally, the recently passed Food and Drug Administration Safety and Innovation Act (FDASIA) expands FDA's Sentinel Initiative to include devices. As a result of these two initiatives, CDRH expects its postmarket surveillance efforts to be enhanced considerably and in a fashion that will monitor targeted risk areas such as current and future information security oversight needs.

While these efforts are designed to ensure CDRH maintains pace with advances in technology and is able to promptly identify safety issues with marketed medical devices, they will also inform and support the premarket review process. CDRH continually incorporates its experiences from both the pre and postmarket program areas into standard operating procedures and policies to ensure the timely evaluation of potential unintentional and intentional threats, vulnerabilities, and possible information security risks, and the timely development and deployment of strategies to mitigate these risks.

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Marcia Crosse, (202) 512-7114 or crossem@gao.gov
Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Tom Conahan, Assistant Director; Vijay D'Souza, Assistant Director; Kaitlin Coffey; West Coile; Neil Doherty; Lynn Espedido; Nancy Glover; Rosanna Guerrero; Cathleen Hamann; Gay Hee Lee; Lee McCracken; and Monica Perez-Nelson made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

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

Public Affairs

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

