GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-12-816, a report to congressional requesters

August 2012

MEDICAL DEVICES

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

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

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.