Improving the Security and Privacy of Implantable Medical Devices

William H. Maisel, M.D., M.P.H., and Tadayoshi Kohno, Ph.D.

In 1982, the threat to the security of the world's drug supply was recognized when seven people died from taking Tylenol that had purposely been contaminated with cyanide. The scare spawned federal laws, regulatory modifications, and a revolution in drug packaging. These interventions greatly secured the billions of pills, capsules, tablets, and liquids that have since been consumed. Today, medical devices, like the drug supply of a generation ago, face a security vulnerability that must be addressed through regulatory and scientific actions.

Most people are familiar with common types of computer-security breaches — those caused by computer viruses, Internet hackers, and the loss or theft of laptops containing sensitive data. But concerns about security also extend to the computers embedded in sophisticated medical devices, which have become increasingly complex and often rely on intricate software and extensive automated functionality. Many devices perform complex analyses, have sophisticated decision-making capabilities, store detailed personal medical information, and communicate automatically, remotely, and wirelessly. These features have provided improved care and quality of life for millions of patients, but they also have created a susceptibility to security breaches that could compromise the performance of such devices and the safety and privacy of patients.

Appropriate security of medical devices should ensure reliable, secure communication and continued functionality while preserving patients' safety, confidentiality, and data integrity. Though there is nearly universal agreement on the importance of security for personal health information and electronic health records, there is disagreement over the security requirements for medical devices. For instance, when a modern implantable defibrillator was shown to be vulnerable to unauthorized communication, potentially harmful device reprogramming, and unauthorized data extraction, the president of the Heart Rhythm Society noted that the devices "were not designed to withstand a terrorist attack."[1,2] However, these are not entirely theoretical concerns: purposeful harm to unsuspecting patients is not limited to the Tylenol scare. For example, computer hackers sabotaged a patient-support Web site run by the Epilepsy Foundation, causing it to display flashing lights that induced seizures in some patients. Similarly, the contamination of heparin that injured dozens of patients and resulted in widespread product recalls may have been purposeful, according to 2008 testimony that the Food and Drug Administration (FDA) presented to the House Subcommittee on Oversight and Investigations. In addition, worms (self-replicating computer programs) have infected hundreds of computers that control medical devices such as magnetic resonance imaging scanners and heart monitors.

FDA officials expect that purposeful harm caused by the disruption of a specific medical device would be "exceedingly rare" but note that it is a possibility "that cannot be discounted."[3] Motivation for such actions might include the acquisition of private information for financial gain or competitive advantage; damage to a device manufacturer's reputation; sabotage by a disgruntled employee, dissatisfied customer, or terrorist to inflict financial or personal injury; or simply the satisfaction of the attacker's ego. Moreover, it is even more likely that device functionality will be disrupted and security breached accidentally. This susceptibility arises from increased wireless and network connectivity, which may lead to "collateral damage" to devices from a virus, worm, or malicious software ("malware") designed to compromise or disrupt other computer systems. Today, individual devices may automatically communicate with physicians' offices, hospitals, and manufacturers and may be open to reprogramming, data extraction, and software updates — all communication routes that present potential portals for security breaches.

Medical-device manufacturers have a legal responsibility to "be vigilant and responsive" to security threats,[3] although their specific responsibilities have not been

well delineated. For example, security regulations attached to the Health Insurance Portability and Accountability Act (HIPAA) specify a series of administrative, technical, and physical security procedures that should be used to ensure the confidentiality of protected electronic health information.[4] However, HIPAA applies only to "covered entities" — defined as health plans, health care clearinghouses, and health care providers who transmit health information electronically. Although some device companies, such as those that sell products directly to patients, may be covered entities, most are not. Furthermore, the HIPAA regulations are directed at the security of information, not at ensuring device functionality. A medical device's security and a patient's well-being can be compromised without compromising the patient information contained on the device.

Many device manufacturers use safeguards such as data validation and user authentication to provide a measure of security from viruses, worms, and other threats. Some modern devices can receive "upgrades" of their integral software (firmware) through simple downloads performed in the physician's office. This capability offers the potential to improve a device's functionality, but it also creates a portal for software contamination — though no case of intentional corruption of proprietary software in implanted devices has been reported to date. Similarly, clinically beneficial and convenient device features that permit transtelephonic and wireless device communication may increase susceptibility to security breaches. Although some wireless medical devices use data encryption and communicate over medical-grade band frequencies, others do not.[1]

Additional types of security threats remain. For example, one could disrupt therapies by flooding a device with so much inappropriate communications traffic that normal communication fails to reach it. Other schemes, like those used to prematurely drain the batteries of computer products such as iPhones, could significantly reduce the life span of a medical device by repeatedly awakening it from a sleeping state. Although it is reassuring that there hasn't yet been a widespread breach of device security, examination of early Internet security incidents provides useful insights into the potential risks. For example, one of the first Internet worms infected nearly 10% of all Internet-connected computers and caused as much as $100 million in damages, underscoring the vulnerability of inadequately protected, widely connected systems.

The FDA's current program for assessing the security of medical devices requires manufacturers to use design and validation procedures that address the confidentiality, integrity, and availability of patient data and to limit access to devices to authorized users only.[5] However, medical devices vary widely with regard to security features, because no specific security guidance or requirements have been promulgated by the FDA. In the past, the agency has not viewed itself as a key contributor to the security of medical devices, noting that "the software engineering community, not the FDA, will dictate the solutions."[3] According to a 2009 report from the Government Accountability Office, the FDA has yet to develop a policy framework for the privacy and security of personal health information.

Clearly, no single security method or mechanism could provide sufficient security for every medical device under every circumstance. The FDA's premarketing regulatory evaluation, therefore, should include a risk-based security assessment that varies with the criticality of device function and the perceived threat of compromised security. Devices with nonessential functions (e.g., cochlear implants or implantable heart monitors) and deemed to be at low risk for a security breach may require only data validation and user authentication. In contrast, devices such as insulin pumps and pacemakers that have life-sustaining functions and carry an increased risk for security breaches would require additional safeguards, such as the inclusion of redundant security features and rigorous testing and verification of security properties. A specific regulatory framework for device security, however, should be developed through a multidisciplinary, collaborative initiative led by the FDA and involving device manufacturers, the computer-security community, regulators, medical practitioners, professional medical societies, patients, and patient-advocacy groups. Ultimately, the required security controls should be commensurate with the potential risks to patients.

Medical devices have provided important health benefits for many patients, but their increasing number, automation, func-

tionality, connectivity, and remote-communication capabilities augment their security vulnerabilities. Although few patients are known to have been harmed by security breaches of medical computers or devices, the security of medical devices is not a luxury. We must develop a security paradigm for medical devices that welcomes important technological advances while ensuring the well-being of millions of medical-device recipients.

Disclosure forms provided by the authors are available with the full text of this article at NEJM.org.

Dr. Maisel is a consultant to the FDA. The opinions expressed in this article are those of the authors and do not necessarily represent the official opinions, practices, policies, or positions of the FDA.

From the Medical Device Safety Institute, Beth Israel Deaconess Medical Center, Boston (W.H.M.); and the Department of Computer Science and Engineering, University of Washington, Seattle (T.K.).

1. Halperin D, Heydt-Benjamin TS, Ransford B, et al. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero power defenses. IEEE Symposium on Security and Privacy, 2008:129-42. (Accessed March 11, 2010, at http://www.secure-medicine.org/icd-study/icd-study.pdf.)
2. Highfield R. Hacking fears over wireless pacemakers. Telegraph.co.uk, March 13, 2008. (Accessed March 11, 2010, at http://www.telegraph.co.uk/science/science-news/3336025/Hacking-fears-over-wireless-pacemakers.html.)
3. Murray J. Prepared statement for the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics (NCVHS). November 19, 2004. (Accessed March 11, 2010, at http://www.ncvhs.hhs.gov/041119p1.htm.)
4. Department of Health and Human Services. Health insurance reform: security standards; final rule. Fed Regist 2003;68(34):8334-81.
5. Food and Drug Administration. Guidance for Industry: computerized systems used in clinical investigations. Washington, DC: Department of Health and Human Services, May 2007. (Accessed March 11, 2010, at http://www.fda.gov/OHRMS/DOCKETS/98fr/04d-0440-gdl0002.pdf.)

The Specter of Financial Armageddon — Health Care and Federal Debt in the United States

Michael E. Chernew, Ph.D., Katherine Baicker, Ph.D., and John Hsu, M.D., M.B.A., M.S.C.E.

The most important force shaping the U.S. health care system over the coming decades may well be the federal debt. The government now pays for approximately half of all health care costs in the United States, and projections of growing federal debt largely reflect anticipated increases in health care spending. Because federal debt and health care policy in the United States are so deeply entwined, it is important to understand the basics of deficits and debt and their implications for health care reform.

The deficit is the gap between expenditures and revenues in any given year ($1.4 trillion in the United States in 2009), whereas debt is defined as accumulated past deficits, or the stock of what we owe ($7.5 trillion at the end of 2009).[1] Economists distinguish between two types of deficit: cyclical and structural. Cyclical deficits rise or fall in the short term in response to economic conditions. In economic downturns, tax revenue falls and government spending on public programs such as unemployment insurance increases, leading to larger deficits and higher debt. These deficits are not necessarily a problem: they can boost economic activity and mitigate economic downturns. When the economy expands, revenues rise and spending falls, creating a cyclical surplus that, holding all else constant, can reduce the debt.

In contrast, structural deficits represent an underlying, persistent imbalance between revenues and expenditures. The United States has a substantial, growing structural deficit, much of which reflects current and projected increases in federal spending on Medicare and Medicaid. This federal health care spending amounted to 5% of the gross domestic product (GDP) and 20% of federal outlays in 2009 and is forecast to reach 12% of the GDP by 2050.[1] Health care spending is thus a key driver of long-term debt. This does not mean that we cannot run a structural deficit, but deficits must be small enough that debt grows more slowly than the GDP.

So why does debt matter, and how much is too much? Economists often measure the size of the debt relative to the overall economy, or the debt-to-GDP ratio. To finance this debt, the government issues interest-bearing bonds. Doing so imposes several economic costs. First, interest payments consume an increasing share of income (1.3% of the GDP in 2009, or 5.3% of total federal spending),[1] thereby reducing the resources available for