Regulators Driving Professional Liability Risks for Medical Device Industry

New regulations protecting data captured in medical devices and the shift to electronic health records are driving a convergence that should cause medical device manufacturers and software developers to sit up and take notice.

Earlier this year, the U.S. Health and Human Services agency extended the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to contractors, subcontractors and other entities that capture protected health data in their work on behalf of a HIPAA-covered entity.1

At the same time, one of the health care reform actions within the Affordable Care Act (ACA) is the implementation of electronic medical records and electronic billing, which is expected to reduce waste and inefficiencies from the current health care records system over time.2

In June, the Food and Drug Administration (FDA) issued draft guidelines for medical device manufacturers and health care facilities to help ensure that appropriate safeguards are in place to reduce the risk of failure due to a cyberattack.3

According to Joe Coray, vice president and global practice leader of The Hartford’s Technology & Life Science Practice, as these regulatory developments unfold, software developers and medical device manufacturers can face new, potentially unexpected risks that in all likelihood are not covered by their existing insurance programs.

“There is a need to bring these new exposures to the attention of software developers and device manufacturers who may not have previously considered professional liability coverage.”

— Joe Coray, Vice President and Global Practice Leader, Technology & Life Science, The Hartford

“THE ACA is trying to make health care more efficient by increasing interoperability, and the new HIPAA regulations are designed to strengthen the private and security protection of patient data,” Coray explained. “Both are positive developments, but they also mean that software developers and medical device manufacturers must take a much harder look at their professional liability risks connected to data privacy.”

Under the new HIPAA Omnibus Rule, which took effect in March 2013, companies that service medical devices and their operating systems, and have access to the patient information the devices contain, may now be considered “business associates” that must comply with the HIPAA Security Rule, which requires appropriate administrative, physical and technical safeguards to protect electronic health information.4

As part of its guidelines, the FDA noted that medical devices with embedded software may have vulnerabilities and recommended that manufacturers have cybersecurity practices and policies in place to safeguard the patients and the data captured by the device connected to these devices.

“The interoperability between electronic health care record software and other health care IT networks and databases, and their potential impact to the privacy and security of electronic private health care information (ePHI), is creating new challenges,” Coray said. “The systems need to interact, so that electronic records and billing can happen smoothly, without compromising data privacy or security.”

Evolving Exposures

“The Hartford has been educating agents and software developers regarding the potential application of HIPAA to software products because developers are hosting or controlling protected electronic health care data.

“It is important for these companies to recognize the implications of the move to electronic records in terms of their own liability exposure,” said Coray. “Regardless of how the data is transmitted, it should be secured, so it cannot be accessed or tampered with.”

If a patient’s protected information is breached, the offending software company or device manufacturer may also face private litigation, in addition to government fines.

“There is potential for civil action against the doctor, the network, device makers, the software developer or other businesses that support those entities,” Coray noted.

Software companies and those that host data may have an obligation to ensure their products are compliant in protecting that information.

“Consider a scenario in which neither a software developer nor its client have appropriate security measures in place. A data breach occurs, causing economic loss for the client, who then sues the software developer,” said Coray.

To comply with HIPAA, medical device software providers will need to consider implementing, among other measures, patch management programs to protect against viruses and other malicious code.

“In the past, some manufacturers of medical devices with embedded software, such as insulin pumps, pacemakers or imaging equipment, may have not applied software security patches to the device’s operating system out of concern that altering the software could affect the device’s performance or violate FDA approvals, explained Coray.

“There are a need to bring these new exposures to the attention of software developers and device manufacturers who may not have previously considered professional liability coverage,” said Coray. He noted that agents, brokers and insurers play a critical role in helping these companies understand how these new areas of risk can best be addressed via a combination of insurance products and proactive risk management practices.

“Traditional thinking about data security and privacy has been focused on credit cards and bank account information,” said Coray. “But today more than ever, ensuring the privacy and security of personal health care information warrants the same level of concern as protecting financial data.”

Joe Coray can be reached at joseph.coray@thehartford.com. To learn more about The Hartford’s Technology & Life Science Practice, visit www.thehartford.com/technology.

6. “The Hartford” is the insurance companies of The Hartford Financial Services Group, Inc.

JULY/AUGUST 2013