AN ALERT FROM THE BDO TECHNOLOGY & LIFE SCIENCES PRACTICE

BDO KNOWS:
LIFE SCIENCES

CYBER ALERT: FDA ISSUES NEW CYBERSECURITY GUIDELINES FOR MEDICAL DEVICE MANUFACTURERS

Following a spate of major data breaches — resulting in over 112 million compromised health records in 2015 alone — healthcare is the latest industry to face heightened regulatory scrutiny of its cyber preparedness.

The Cybersecurity Act of 2015, a provision of the omnibus spending bill passed in December, requires the Department of Health and Human Services (HHS) to submit a report to Congress assessing the preparedness of the healthcare industry in responding to cyber threats within the next year, with the goal of establishing a "single, voluntary, national, health-specific cybersecurity framework." As part of this mandate, HHS must create a cybersecurity task force comprised of regulatory agencies, industry stakeholders and cyber experts to help (1) plan a single system for the federal government to share intelligence regarding cybersecurity threats to the healthcare industry, and (2) recommend protections for networked medical devices and electronic health records.

On the heels of the bill's enactment, the U.S. Food and Drug Administration (FDA) has issued a new set of draft postmarket guidance for the management of cybersecurity in medical devices, outlining recommended steps medical device manufacturers should take to address growing cybersecurity threats and minimize risk to patients.

SUMMARY

In a follow-up to its October 2014 premarket cybersecurity guidance, the FDA's draft guidance addresses recommendations for managing postmarket cybersecurity vulnerabilities for marketed devices, advocating for a risk-based and proactive approach. While the guidance is primarily aimed at manufacturers, it notes that medical device cybersecurity is a shared responsibility between all healthcare stakeholders including healthcare facilities, patients and providers.

The FDA encourages manufacturers to embrace "good cyber hygiene" through ongoing risk assessment and monitoring, routine device cyber maintenance and implementation of necessary actions to mitigate device functionality and patient safety risks. In addition, the agency promotes information and intelligence sharing (a key provision of the Cybersecurity Act of 2015) within the medical device community. "Voluntary" participation in an Information Sharing Analysis Organization (ISAO) is considered a critical component of a manufacturer's proactive cyber strategy and is considered a mitigating circumstance when an issue arises.

The FDA calls for manufacturers to adopt a comprehensive cybersecurity risk management program and documented process for identifying hazardous cyber vulnerabilities in line with the National Institute of Standards and Technology

HOW DO I GET MORE INFORMATION?

For more information about how medical device manufacturers and healthcare organizations can improve their cybersecurity preparedness, please contact:

SHAHRYAR SHAGHAGHI
BDO Technology Advisory Services National Practice Leader
sshaghaghi@bdo.com

RYAN STARKES
BDO Life Sciences Practice Leader and Assurance Partner
rstarkes@bdo.com

DAVID FRIEND
BDO Chief Transformation Officer and Managing Director of BDO's Center for Healthcare Excellence & Innovation
dfriend@bdo.com

PATRICK PILCH
BDO Healthcare Advisory Practice Leader and Managing Director
ppilch@bdo.com

MAURICE LIDDELL
BDO IT Security & Infrastructure Services National Leader
mliddell@bdo.com

DALE TIMMONS
BDO Management and Technology Advisory National Leader
dtimmons@bdo.com

Read more ▶

Framework for Improving Critical Infrastructure Cybersecurity, which includes the core principles of "Identify, Protect, Detect, Respond and Recover." Such a program should include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

When evaluating potential cyber risks, manufacturers should focus on assessing the risk to the device's "essential clinical performance" and consider the following:

1) The exploitability of the cybersecurity vulnerability.
2) The severity of the health impact to patients should the vulnerability be exploited.

In instances where the "essential clinical performance" of a device could be compromised, the manufacturer is required to notify the agency. Reporting requirements are not enforced if the following circumstances are met:

1) No known serious adverse effects or deaths associated with the vulnerability.
2) The manufacturer sufficiently remediates the issue within 30 days of learning of the vulnerability.
3) The manufacturer is a participant of an ISAO.

A device with an unacceptable level of risk to its essential clinical performance may be considered in violation of the Federal Food, Drug & Cosmetics Act and subject to enforcement actions.

BDO INSIGHTS

The FDA refers to medical device cybersecurity as a "shared responsibility." We often talk of "multi-factor authentication" and "layered defense" as core cybersecurity strategies, and the same lens should be applied to the entire healthcare ecosystem. While manufacturers are ultimately responsible for identifying and remediating potential cyber vulnerabilities associated with their medical devices, hospitals and healthcare systems must safeguard their networks from potential breaches of security via medical devices. Medical device manufacturers are only the first line of defense.

The domino effect of a healthcare data breach sheds light on the importance of information sharing, a growing area of focus in cyber strategy and policy. The Cybersecurity Information Sharing Act (CISA), also part of the omnibus spending bill, offers prescriptive advice on furthering collaboration between the government and private sector, as well as industry collaboration within the private sector. While we will likely see an uptick in threat intelligence sharing across all industries, concerns about protecting competitive information and privacy risk have yet to be addressed. The level of sharing remains to be seen, and will dictate the effectiveness of ISAOs and other information sharing systems in mitigating cyber risk. Participation in ISAOs or Information Sharing and Analysis Centers (ISACs) will likely remain voluntary in the near-term; however, as exemplified by the FDA, regulatory entities will increasingly consider participation when assessing cyber preparedness.

Healthcare organizations and medical device manufacturers are well-advised to seek assistance from consultants and technology specialists experienced in developing risk management frameworks and strategies to navigate complex security and compliance issues. BDO has deep experience in the medical device and healthcare industries and assists companies in conducting security risk assessments, testing controls, conducting security monitoring and developing and executing on incident response plans, in addition to implementing cybersecurity risk management programs, strategy and governance.

BDO TECHNOLOGY & LIFE SCIENCES PRACTICE

BDO is a national professional services firm providing assurance, tax, financial advisory and consulting services to a wide range of publicly traded and privately held companies. Guided by core values including competence, honesty and integrity, professionalism, dedication, responsibility and accountability for 100 years, we have provided quality service and leadership through the active involvement of our most experienced and committed professionals.

BDO works with a wide variety of technology clients, ranging from multinational Fortune 500 corporations to more entrepreneurial businesses, on myriad accounting, tax and other financial issues.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through 63 offices and more than 450 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,408 offices in 154 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

© 2016 BDO USA, LLP. All rights reserved.