Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Serious And Immense Impact Of A Medical Device Hack

By **attorneys at Wilson Sonsini Goodrich & Rosati PC**

Law360, New York (January 12, 2017, 12:52 PM EST) --

Charles J. Andres

On Aug. 25th 2016, the investment firm Muddy Waters Research announced it had taken a short position in St. Jude Medical Inc., and released a report suggesting a "strong possibility that close to half of" St. Jude revenues were about to disappear for a period of roughly two years because St. Jude's implantable cardiac devices were allegedly vulnerable to cyber-attacks.[1] The report further stated that the cyber-attacks included crash attacks that cause devices to malfunction — including by apparently pacing at a potentially dangerous rate and a battery drain attack that could be particularly harmful to device-dependent users.[2]

The Muddy Waters report was largely based on analysis conducted by the cybersecurity company, MedSec Holdings Inc. MedSec Chief Executive Officer Justine Bone suggested that St. Jude's products had an "astounding" level of problems, including lack of encryption and authentication between devices, which could allow hackers to tap into implanted devices.[3] MedSec had negotiated compensation tied to the success of Muddy Waters' trade position, and Bone stated that partnering with Muddy Waters was the most powerful way to inflict pain on St. Jude for what she called its "negligent level of attention to cybersecurity."[4]

At the time of the Muddy Waters report, St. Jude was in the process of being acquired by Abbott Laboratories for $25 billion. St. Jude shareholders were slated to receive, for each share of St. Jude common stock held, $46.75 in cash and 0.8708 share of Abbott common stock, representing about $85 per St. Jude share, by the end of the year. In contrast, upon release of the Muddy Waters report, St. Jude stock closed at $77.82, well below the deal value, leading analysts to speculate about the prospect of the acquisition by Abbott.

In response, St. Jude filed suit in the District Court for the District of Minnesota against Muddy Waters and MedSec claiming that the allegations of cybersecurity vulnerabilities are false. St. Jude further alleged that the two companies used "false and misleading tactics" to scare patients, drop share prices and make cash on the side as a result. St Jude also released a rebuttal report stating that the researchers at MedSec used "flawed test methodology on outdated software," demonstrating a "lack of understanding of medical device technology."[5] As the case has proceeded, Muddy Waters released additional videos and expert reports elaborating on its allegations. Abbott's deal with St. Jude recently closed, and the company has continued to assert that these allegations are exaggerated and untrue.

In this article, we explore selected ramifications of a medical device hack, and provide some suggested

practices for companies who offer medical devices to the public.

The Regulatory Landscape

Companies that manufacture and sell medical devices to the public face a complex regulatory landscape. A host of different government agencies enforce laws that impose obligations on medical device manufacturers whose devices gather, store or transmit information.

HIPAA

For example, the Health Insurance Portability and Accountability regulations issued and enforced by the U.S. Department of Health and Human Services, govern the privacy and security of protected health information (PHI). [6] The HIPAA rules require implementation of reasonable and appropriate administrative, physical, technical and organizational data security safeguards, which include data security risk assessments, and ongoing risk management efforts to reduce cyber risks and vulnerabilities. Compliance with the HIPAA rules is mandatory for device manufacturers who collect or transfer PHI. [7]

Device manufacturers and others who fail to comply with HIPAA rules may face significant penalties. For example, in August 2016, HHS imposed a $5.55 million penalty in a settlement with Advocate Health Care Network due, in part, to an alleged failure to conduct a data security risk assessment and to implement reasonable physical security measures. In about the same time frame, HHS settled a case against Oregon Health & Science University (OHSU) that included a $2.7 million civil penalty. The case was based on allegations that OHSU's risk assessment did not cover all electronic PHI that it maintained, and that OHSU did not reasonably and appropriately address documented vulnerabilities and risks in a timely manner. These settlements underscore the importance of conducting regular risk assessments, ensuring that the device manufacturer's data security mechanisms meet ever-evolving threats, and confirming up-to-date HIPAA compliance.

The FTC

In addition to the specific rules that govern PHI, the Federal Trade Commission has taken a similar approach to data security more generally. Relying on the very broad language in Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts and practices in or affecting commerce, the FTC has brought over 60 enforcement actions against companies that allegedly failed to maintain adequate data security. Some of these actions were based on allegations that a company engaged in a deceptive practice if it did not have measures in place that matched the public representations it made about its data security efforts.[8] Even without an affirmative representation, however, the FTC could challenge a device manufacturer's data security practices as unfair if the manufacturer failed to employ reasonable and appropriate measures to prevent unauthorized access to the information it collected.

The FTC's enforcement actions, virtually all of which are settlements, require companies to implement and maintain data security programs that contain administrative, technical and physical safeguards appropriate given the size and complexity of the business and the sensitivity of the personal information collected from or about consumers. Similar to HHS, the FTC expects companies to engage in regular risk assessments. Device manufactures should consider implementing data security plans that meet these standards and should review their public statements, including their privacy policies, to ensure that their practices are consistent with any public commitments.

The SEC

Public medical device companies should also consider whether a security vulnerability or data breach should be disclosed to investors and, by extension, to the U.S. Securities and Exchange Commission. The SEC has the authority to investigate possible violations of the federal securities laws, which include failures of public companies to make adequate disclosures, withhold material information, and/or misrepresent to, or mislead, investors.[9]

In 2011, the SEC issued written guidance to public companies to assist them in "assessing what, if any, disclosures should be provided [to shareholders/investors] about cybersecurity matters." The guidance notes that "[a]lthough no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents," if a public company experiences a "material cyberattack" it "would not be sufficient" for the company to merely disclose that a risk of cyberattacks exists (i.e., via standard risk factors) but rather the public company may be required to disclose specifics regarding the cyber event and its potential costs and consequences. Outside of standard risk factor disclosure, the SEC recommends that companies review other disclosures such as the management's discussion and analysis of financial condition and results of operations (MD&A), business, legal proceedings, and financial statement sections.

In 2014, former SEC Commissioner Luis Aguilar publicly stated that cybersecurity is "of particular concern to the SEC" and that he hoped the disclosures discussed in the 2011 guidance "helped investors and public companies to focus and assess cybersecurity issues." Current SEC Chairwoman Mary Jo White has reaffirmed the SEC's focus on cybersecurity.[10] Of course, the dispositive question in determining whether disclosure is required is whether the cyberattack/security vulnerability is material to investors. In the recent past, many companies who have suffered large cybersecurity breaches have not reported these in their period or current reports on Form 10-K, 10-Q or 8-K, and there have been limited SEC enforcement actions for failure to disclose breaches.

Increasing scrutiny and public awareness of cyber incidents, however, could lead to a tightening of disclosure standards. Public companies should be careful to ensure proper disclosure.

The FDA

Finally, medical device companies should also consider the U.S. Food and Drug Administration's role in any medical device hack, especially where the hack could result in harm or death to patients.

The FDA regulates medical devices under e.g., the Medical Device Amendments of 1976, and is keenly concerned with the safety and effectiveness of any medical device. Recognizing that cybersecurity of connected medical devices could present a growing problem, the FDA issued guidance on post-management security in 2016.[11] While the FDA's guidance touches on a number of areas, when evaluating post-market risk, the FDA encourages companies to:

1. Monitor cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;

2. Understand, assess and detect the presence and impact of a vulnerability;

3. Establish and communicate processes for vulnerability intake and handling;

4. Clearly define essential clinical performance of the device to develop mitigations that protect, respond and recover from the cybersecurity risk;

5. Adopt a coordinated vulnerability disclosure policy and practice; and

6. Deploy mitigations that address cybersecurity risk early and prior to exploitation.

The FDA has enforcement authority over medical device manufacturers. If a medical device: (a) has uncontrolled risk, including a cybersecurity risk, to essential clinical performance that (b) may reasonably cause serious adverse health consequences or death, then the manufacturer may be in violation of the Federal Food, Drug and Cosmetic Act (FDCA). FDCA violations may subject the device manufacturer to FDA enforcement actions, which can include seizure and recall of medical devices.

Thus, if a medical device hack endangers the health or safety of patients, the medical device manufacturers should work with the FDA[12] to mitigate the hacking associated risks in an expeditious manner. Companies should be prepared to recall medical devices that contain the vulnerability, re-engineer the medical device or its software to remove the hacking vulnerability, and facilitate communication shut off of in-use medical devices until, e.g., a vulnerability mitigating patch can be implemented.

Reporting obligations to various agencies of the federal and state governments, and mechanisms for addressing any FDA-mandated action, should be contained in the incident response plan that is prepared and in place ahead of any hack.

Plan of Action

Medical device hacks can have serious and wide ranging repercussions: they can endanger patient lives, result in data breaches, materially affect stock prices, sour investor relationships, scuttle on-going transactions, and tarnish a device manufacturer's reputation. Hackers may also attempt to use their ability to hack a device to extract a ransom in exchange for not harming patients relying upon the device, for providing information about how the hack is performed, or for containing or preventing a data breach.

To prepare for a possible intrusion, companies whose devices may be subject to hacking should develop an incident response plan. Companies should also create a culture that encourages and enables timely reporting, evaluation and escalation of reports of a possible hack, regardless of the source. This can be achieved, for example, through comprehensive training of personnel and putting into place appropriate internal reporting mechanisms and structures.

Companies should also consider reviewing existing internal compliance policies, including those related to whistleblowing, to ensure these are designed to appropriately identify and address reports of information technology and cybersecurity issues. For example, whistleblowers and "white hat" hackers should have appropriate avenues to report potential cyber vulnerabilities.

Incident Response Plan and Team

The discovery of a hack is, at a minimum, unsettling for any company. Senior managers are faced with making decisions, under extreme time pressures, which can significantly impact the business.

In making these decisions, senior managers must be able to adjust in response to unfolding events and new information. Manufacturers may also have obligations to notify various government agencies such as the FDA and the U.S. Department of Health and Human Services, as well as affected individuals and their caregivers.[13]

Managing this effort can be complicated and uncertain; and being prepared is a significant factor in mitigating costs and damages associated with a hack. A key factor in security incident preparedness is developing an incident response plan. Supporting the centrality and importance of an incident response plan, research conducted by the Ponemon Institute shows that failure to have an incident response plan and team in place is a leading factor that can increase the incident costs and damages.[14]

Companies should, therefore, draft, implement and regularly test their incident response plans.[15] Incident response plans typically include detailed instructions for:

1. Identifying and preparing the members of the incident response team. This includes determining, in advance, what roles and responsibilities key decisions makers will have in the event of a hack;

2. Putting communication trees (e.g., phone trees) in place, and pressure testing the communication trees to ensure timely access to key decisions makers in the event of a hack;

3. Cultivating good working relationships with law enforcement and relevant governmental agencies before any hack occurs (the first time law enforcement meets your team should not be after a hack occurs);

4. Understanding, implementing and updating protective mechanisms required by different laws;

5. Identifying suspected incidents;

6. Responding to suspected hacks from an information technology perspective;

7. Bringing in outside legal and forensics experts — legal should be involved from the start;

8. Documenting a hack;

9. Mitigating damage from a hack;

10. Reporting response efforts to senior management;

11. Assessing legal and business risks from a security incident;

12. Determining breach notification obligations under applicable law and contracts. This includes state and federal government and agency reporting requirements, and their associated time frames, as well has having a detailed plan for notifying health care providers and their patients; and

13. If a ransom is demanded, deciding in advance the company's policy on ransom payment, keeping in mind that in some situations, the general policy may need to be adapted to meet incident specifics.[16]

Having and following an incident response plan helps an organization methodically take the proper steps while responding to an incident. Organizations with a plan will be able to more quickly assess the incident so that they can respond in timely, cost-efficient and effective manner.

Intellectual Property Considerations

Timely fixing or patching over the hack is of paramount importance. But, the ability to make hardware or software modifications that mitigate a hacking vulnerability may not simply be a technical problem. Any fix to a device's hardware or software should also not violate intellectual property to which the medical device manufacturer does not have rights. Thus, medical device manufacturers should maximize patent claim scope, strategically leverage licenses and be aware of the relevant patent landscapes so as to create a "buffer" that allows for modifications that could be reasonably foreseeable in response to a hack.

Other Considerations

A medical device hack (or the possibility of a hack) raises diverse considerations beyond those discussed above. While it is not possible to address all of these, we point out three relevant examples as catalysts for further thought.

First, if a medical device manufacturer is involved in a transaction to sell the company, the medical device manufacturer should be careful in ensuring proper disclosure regarding the features and limitations of the medical device and proactively addressing any cybersecurity vulnerabilities to limit post-closing issues. The medical device manufacturer should also carefully consider how risk — in the form of indemnification — should be allocated after the deal closes

Second, disclosure of a hack may put downward pressure on a medical device company's stock. To protect against hostile takeover at a vulnerable point, companies may want to consider implementing appropriate protective actions.

Finally, one way to minimize fallout from a hack is to control the narrative which includes providing thoughtful responses, such as planned changes to address vulnerabilities. Strategic, clear, timely and honest public relations can help a company weather a hack. Any proposed communication, however, should be evaluated in light of the potential for the communication to be used in a future investor or patient lawsuit.

Conclusion

With the growth of medical devices that communicate wirelessly, share data and can be adjusted or turned off remotely, the threat, reach and potential fallout of hacking will grow. Medical device manufacturers should proactively take steps to minimize the possibility of hacking, and have structures in place, including an incident response plan, to deal with a hack should it occur.

David M. Hoffmeister is a partner at Wilson Sonsini Goodrich & Rosati PC in Palo Alto, California. Vern Norviel is a partner in Wilson Sonsini's San Francisco, San Diego and Boston offices. Mark C. Solakian and Louis D. Lieto are partners in Wilson Sonsini's Boston office. Lydia Parnes is a partner in Wilson Sonsini's Washington, D.C., office.

Lawrence J. Perrone and Charles J. Andres are associates in Wilson Sonsini's Washington, D.C., office. Wendell Bartnick is an associate in Wilson Sonsini's Austin, Texas, office. Jennifer Fang, Prashant Girinath and Jake D. Gatof are associates in Wilson Sonsini's Boston office.

[1] See http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/.

[2] Id.

[3] See http://www.bloomberg.com/news/articles/2016-08-25/carson-block-takes-on-st-jude-medical-with-claim-of-hack-risk.

[4] Id.

[5] See http://www.reuters.com/article/us-st-jude-medical-cyber-idUSKCN11129K.

[6] The HHS regulations implementing the privacy and data security provisions of HIPAA are at 45 C.F.R. §§ 160, 164.

[7] The protocol HHS uses in HIPAA compliance audits is available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/.

[8] For example, in January 2016, the FTC investigated and settled a case against Henry Schein Practice Solutions Inc., for its alleged failure to provide industry-standard encryption of patient information despite advertising that it did so. In re Henry Schein Practice Solutions Inc., No. C-4575 (May 20, 2016).

[9] While the SEC engaging in the regulation of cyber or security events may seem odd, it is not. That the underlying facts of such securities violations related to a cyberattack or security vulnerability in a medical device likely do not undermine such authority. See Securities Act of 1933 (Securities Act), Sections 19 & 20, 15 U.S.C. §§ 77s, 77t; Securities Act of 1934 (Exchange Act), Section 21, 15 U.S.C. § 78u.

[10] Earlier this year, the SEC hired Chris Hetner as SEC's first Senior Advisor to the Chair for Cybersecurity Policy.

[11] See "Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff," FDA, (Jan. 22, 2016), available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

[12] Manufacturers regulated by the FDA may be required to report certain vulnerabilities under 21 C.F.R. parts 803, 806, and 1004.

[13] FTC v. Wyndham Worldwide Corp., 12-CV-1365 (D. Ariz. 2012) (Complaint).

[14] "Cost of a Data Breach Study: United States," Ponemon Institute (June 2016).

[15] HIPAA requires regulated companies to have an incident response plan. HHS recently reached a settlement with the University of Mississippi Medical Center imposing a monetary penalty of $2.75 million for HIPAA violations including a failure to implement policies and procedures to address security incidents and a failure to properly notify individuals affected by a data breach.

[16] Although this article does not deal with device design and manufacturing issues per se, companies should also consider taking steps to minimize the possibility of a device being hacked by: limiting the communication range of the device, using handshake protocols, making use of sophisticated encryption software, and allowing for external communication with the device to be shut off.

In addition, the U.S. Food and Drug Administration has provided draft guidance to medical device manufacturers to address premarket concerns that networked medical devices may be vulnerable to cybersecurity threats that pose safety and effectiveness risks. See "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," FDA, (Oct. 22, 2014), available at: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

While not legally binding, medical device companies are nevertheless strongly encouraged to follow the FDA's guidance, which among other things, promotes the benefits of collaboration on and sharing of cyber risk information and intelligence with the medical device community through participation in an information sharing analysis organization.

The guidance also recommends using the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, and evaluating premarket risk by:

- Identifying assets, threats and vulnerabilities;

- Assessing the impact of these threats and vulnerabilities on the device functionality and end users/patients;

- Assessing the likelihood of a threat and of a vulnerability being exploited;

- Determining risk levels and suitable mitigation strategies; and

- Assessing residual risk and risk acceptance criteria.