CARLTON FIELDS

# Could Your Medical Device Be a Hacker’s Gateway into a Hospital Network?

HEALTH CARE | PHARMACEUTICALS AND MEDICAL DEVICES | TECHNOLOGY | HEALTH CARE | CYBERSECURITY AND PRIVACY | PHARMACEUTICALS AND MEDICAL DEVICES | DECEMBER 23, 2015

This has been a big year for health care data breaches. In January, the data of 80 million Anthem members was compromised; in March, a cyberattack exposed the data of 11.2 million Premera BlueCross BlueShield members and business affiliates; and in May, the data of 1.1 million CareFirst BlueCross BlueShield members met the same fate. Hackers’ methods of accessing health care networks are becoming more creative, and include infiltration through medical devices.

Six years ago, for the first time, the number of “things” connected to the Internet surpassed the number of people, according to a January 2015 Federal Trade Commission report, “Internet of Things: Privacy & Security in a Connected World.“ Experts estimate that by the end of 2015, there will be 25 billion connected devices— and that by 2020, there will be 50 billion. While these devices can significantly improve the lives and health of consumers worldwide, they also pose sizable risks.

Hospital networks are prime targets for hackers because many contain vast amounts of highly personalized and confidential data, and **hackers have developed new methods of breaching hospital networks through hospital patients’ medical devices.** In June 2015, TrapX, a firm specializing in deception-based cybersecurity defense, released a report that found attackers targeted and compromised radiology picture archive and communications systems and blood gas analyzers to gain access to the hospital networks. The TrapX report even suggested that an attacker could remotely hack a hospital drug pump and modify the amount of medication to a fatal dose.

Both the Food and Drug Administration and the FTC have provided guidance on cybersecurity in medical devices. In late 2014, the FDA issued final guidance calling for manufacturers to consider cybersecurity risks in designing and developing medical devices. Shortly thereafter, the FTC issued guidance on best practices for privacy and security protection, including guidance on the design, deployment, and management of medical devices.

Everyone involved in the development and maintenance of medical devices must be aware of the applicable cybersecurity risks, and take appropriate safeguards to ensure patient safety and privacy. These include the device developers, the providers who maintain them, and the consumers who use them. Compliance with the nonmandatory guidance and best practices issued by the FTC and FDA offer a good starting point.

Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.