Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Aviation and Petrochemical Industries Subject to Hacking by Iran

Hackers working on behalf of the Iranian government have been targeting the aviation and petrochemical industries in the United States, Saudi Arabia, and South Korea since 2013, according to a report released by FireEye last week. *Read more*

SEC Hacked!

The Securities and Exchange Commission (SEC) has admitted it was the victim of a cyber attack in 2016 that exposed information that may have been used for insider trading. The hack involved the SEC's filing database, known as EDGAR. The admission was on the heels of a Government and Accountability Office report in July warning the SEC that it had not fully implemented an intrusion detection capability in its system. *Read more*

Security Vulnerabilities Identified in Wireless Syringe Infusion Pumps

The U.S. Department of Homeland Security (DHS) recently issued a warning that Smiths Medical Medfusion 4000 wireless syringe infusion pumps contain a security vulnerability that can be exploited by hackers to alter the performance of the medical devices.

The devices are used to infuse small doses of medication to patients in acute care settings. Eight different vulnerabilities have been identified in pump versions 1.1, 1.5, and 1.6. According to DHS, hackers can exploit the vulnerabilities remotely, causing harm to patients, and can be used to gain access to other health care information technology systems if they are not segmented on the health care organization's network.

Smiths Medical is working with the DHS to resolve the flaws in its new version, which will be released in January 2018. Until then, Smiths

September 28, 2017

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan
Matthew W. Rizzini

FEATURED TOPICS:

Cybersecurity
Drones
HIPAA
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

recommends the following: *Read more*

HIPAA

Second Largest Business Associate Breach in 2017

Cornerstone Business & Management Solutions, a medical supply company in Nebraska, has notified 21,856 individuals and the Office for Civil Rights that while performing a routine review of system logs, it discovered a suspicious account on its server downloading personal information of patients using its medical devices, including names, addresses, dates of birth, and insurance information.

According to the OCR website, this is the second largest breach from a hacking incident in 2017. *Read more*

DRONES

Consortiq Software System Demonstrates Security for UAS is Possible

Unmanned aerial systems (UAS or drones) security has become a hot topic not only in the United States but also in countries around the world. As more UAS hit the skies, increasing the potential for hackers to intercept data being transferred from drones to servers or other devices on the ground or to carry out hostile takeovers of the drones as they attempt to complete a mission. However, Consortiq's security software for UAS, known as CQNet, could be the start of one solution in this area. *Read more*

City of Newton's Drone Ordinance Overturned by Federal Judge

Last week, a federal judge in Massachusetts ruled that the City of Newton's drone ordinance, which attempted to regulate drone flights in the airspace over Newton, could not be enforced by the municipality because it is preempted by federal law. In Decembet 2016, the city passed an ordinance that required drone operators to register their drones, banned unmanned drone flights under 400 feet, and banned flights over private and public property without permission from the landowner. *Read more*

PRIVACY TIP #107

Medical Marijuana Privacy

As more and more state laws allow the use of marijuana for medical conditions, and dispensaries are opening to provide users with access to marijuana for medical purposes (and recreational use), patients are questioning and becoming concerned about the protection of their privacy when purchasing marijuana in dispensaries. The concern is that federal law still outlaws marijuana, as do many states, and many employers conduct drug monitoring and may access and use data in the employment setting to terminate employees.

In response to these concerns, many states are enacting laws to protect the privacy of consumers who frequent marijuana dispensaries. For instance, Massachusetts does not require retailers to record customer information. Oregon does not allow marijuana retailers to record, retain, or transfer personal information of customers of marijuana retailers.

Many ask whether HIPAA applies to medical marijuana dispensaries. The answer is that it depends on whether the dispensary is a covered entity under HIPAA—that is, whether it is billing or submitting a "covered transaction" that falls under the regulatory rubric of HIPAA. If the dispensary receives cash for the marijuana, it is probably not covered by HIPAA, and therefore, consumers' personal and health information is not protected by the HIPAA Privacy and Security Rules. Nonetheless, some state laws protect the privacy of consumers' health information.

Although some dispensaries hold themselves out as being "HIPAA compliant" and provide patients who frequent the dispensary a Notice of Privacy Practices, which is required by HIPAA, in general, consumers should assume that a medical dispensary is not following HIPAA and that their health information can be and is being shared, and monetized as with any other business.

If you visit a marijuana dispensary (or any other retail establishment,) paying cash is always the best way to protect your privacy. Otherwise, your personal information will be collected, used, transmitted, and stored in the dispensary's system and in the cloud, all of which have risks that have been discussed before in this blog.