Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

October 24, 2019

FEATURED AUTHORS:

Linn Foster Freedman
Deborah A. George
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Privacy
Enforcement + Litigation
HIPAA
New + Now
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

CYBERSECURITY

Hackers Eavesdrop and Obtain Sensitive Data of Users Through Home Smart Assistants

Although Amazon and Google respond to reports of vulnerabilities in popular home smart assistants Alexa and Google Home, hackers continually work hard to exploit any vulnerabilities in order to listen to users' every word to obtain sensitive information that can be used in future attacks. *Read more*

Philadelphia DPH Breach Exposes Hepatitis Patients' Data

A reporter from the *Philadelphia Inquirer* discovered that sensitive data of hepatitis patients were accessible online through a Philadelphia Department of Public Health (DPH) website tool without the need for a password. The Inquirer was able to access the data of some 23,000 patients who had contracted Hepatitis C. The vulnerable data included the patient's name, gender, address, test results and some Social Security numbers. *Read more*

HIPAA

Jackson Health System Fined $2.15 Million by OCR

The Office for Civil Rights (OCR) announced on October 23, 2019 that Jackson Health System (Jackson), a not-for-profit hospital system comprised of six hospitals, urgent care centers, nursing facilities, and primary care and specialty services based in Miami, Florida, has waived its right to a hearing and did not contest the findings set forth in the OCR's Notice of Proposed Determination (NPD), and has agreed to pay the full civil monetary penalty assessed by OCR. This unusual step means that Jackson will pay the full fine of $2.15 million. *Read more*

ENFORCEMENT + LITIGATION

HHS Proposes Changes to Permit Donation of Cybersecurity Technology

On October 17, 2019, the Department of Health and Human Services (HHS) published proposed rules to update the regulatory Anti-Kickback Statute (AKS) safe-harbors and exceptions to the Physician Self-Referral (PSR) Law, known commonly as the Stark Law (AKS proposed rule

available here; PSR proposed rule available here). In an earlier blog post, we described each of the proposed rules. Among the proposed changes are a new safe harbor/exception that would generally permit entities to donate certain cybersecurity technology and related services to physicians, subject to compliance with the conditions described below. In the preamble to each proposed rule, the HHS Office of Inspector General (OIG) (which published the AKS proposed rule) and the Centers for Medicare and Medicaid Services (CMS) (which published the PSR proposed rule) noted that cyber-attacks in the health care industry are on the rise and cybersecurity technology can be cost-prohibitive for some providers. Both OIG and CMS stated their hope that the proposed rules will improve overall cybersecurity in the health care industry and reduce instances of data breaches resulting from cyber-attacks. *Read more*

DATA PRIVACY

FTC Settles First Case Involving Stalkerware

Would you hand over your smartphone, including your call history, text messages, photos, GPS locations, and browser history to your employer? To your significant other? How about to a random stranger? I'm guessing your answer is an overwhelming "No" to each of these questions.

Stalkerware and stalking apps do just that. Both are spyware that secretly monitors your smart phone. In its first case against the developer of a stalkerware app, the Federal trade Commission (FTC) recently announced a settlement with Retina-X Studios, LLC. Retina-X developed several apps (MobileSpy, PhoneSheriff and TeenShield) that shared detailed information about a user's smartphone activities. *Read more*

NEW + NOW

Compliance: Keeping Up with Rapidly Changing Privacy and Security Laws

The pace at which data privacy and security laws are changing continues to move at warp speed. Back in the day, I would keep track of all privacy and security bills in state legislatures and Congress; about 10 years ago, I stopped that practice because many were never enacted.

Now, however, state laws are being enacted at a rapid pace, and it is challenging to keep up, even when it is your job to do so. We spend a lot of time staying on top of newly enacted laws for our clients, but compliance officers/personnel are being overwhelmed with the complexity of being aware of, and complying with, new laws, many of which are obscure. *Read more*

PRIVACY TIP #213

The Jumbo Privacy App

The Jumbo Privacy app, available in the App Store, is all about providing consumers with a way to audit their privacy and learn whether and how

their information might have been compromised. This week's tip includes a review of why you may want to use it. *Read more*