Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

HIPAA

St. Joseph Health Settles with OCR for $2.14 Million

The Office for Civil Rights (OCR) has announced that it has entered into a $2.14 million settlement with St. Joseph Health, which operates hospitals and nursing homes in California, Texas, and New Mexico, for alleged HIPAA violations. St. Joseph Health notified the OCR on February 14, 2012, of a data breach involving the protected health information of 31,800 patients when one of its servers included a file-sharing application that used default settings and allowed access to the information through the Internet in 2011 and 2012. *Read more*

ENFORCEMENT + LITIGATION

Sixth Circuit: Substantial Risk of Harm and Mitigation Costs Sufficient to Confer Standing in Data Breach Case

On October 12, 2016, the U.S. Court of Appeals for the Sixth Circuit denied a petition for an *en banc* rehearing of its September 12 decision in *Galaria, et al. v. Nationwide Mutual Insurance Company* (Nos. 15-3386/3387). In that decision, a divided Sixth Circuit panel revived a suit against Nationwide arising from the 2012 theft by hackers of personal information of approximately 1.1 million individuals. *Read more*

CYBERSECURITY

Connecticut Governor Appoints State Cybersecurity Czar

Gov. Dannel P. Malloy recently appointed Arthur H. House as the state's first cybersecurity czar. House moves into the role after serving as the chairman of the Public Utilities Regulatory Authority for the past four years. *Read more*

October 20, 2016

FEATURED AUTHORS:

Kate E. Dion
Conor O. Duffy
Linn Foster Freedman
Edward Hadcock
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Enforcement + Litigation
Data Privacy
Drones
HIPAA
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

DATA PRIVACY

U.S. Department of Education Issues Guidance on Student Medical Records

On September 14, 2016, the Department of Education (DOE) issued a "Dear Colleague Letter" to provide guidance on the application of the Family Educational Rights and Privacy Act (FERPA) to the disclosure of student medical records in the context of litigation. *Read more*

Transatlantic Data Transfer: An Update

This article courtesy of guest blogger Edward Hadcock of Mills & Reeve LLP.

The EU-US Privacy Shield, designed to protect EU citizens' personal data when it is transferred to U.S. organizations, has now been in place for a couple of months. How is it shaping up? *Read more*

DRONES

NASA Announces Beyond Visual-Line-of-Sight UAS Test Flights

National Aeronautics and Space Administration (NASA) plans to fly unmanned aircraft systems (UAS; commonly known as drones) this month beyond the visual line of sight of their operators to test planning, tracking, and alerting capabilities of NASA's UAS traffic management (UTM) research platform. Two of the drones will fly beyond the visual line of sight, and the other three drones (if used) will fly in the same test airspace but will be separated by altitude (and remain within line of sight of their operators). NASA seeks to test the UTM's platform and its ability to track drone location. Before multiple commercial drones (and government drones for that matter) can start flying in the same areas—beyond a pilot's view—procedures must be in place to safely manage the drone traffic, to keep drones out of no-fly zones (or geo-fenced areas), and to alert drones of severe weather patterns or unplanned events in the airspace that change their plans. *Read more*

New Use for Drones on Australian Beaches

In Western Australia's southwest beaches, surveillance drones will hit the skies to increase swimmer safety by spotting sharks in the water. This project will take place over a three-month period (from November

to January) and will cost approximately $88,000. *Read more*

PRIVACY TIP #57

Do Chip Credit Cards Really Protect Me from Fraud?

There are a half a billion chip cards in the market right now. They have been touted to improve security and reduce credit card fraud. But do they?

According to a new report, both Visa and MasterCard have reported that the chip cards (also known as EMV) are working. Visa reports that it has seen a 47 percent decline in fraud, and MasterCard has seen a 54 percent reduction.

Nonetheless, only about a third of U.S. companies have implemented the EMV technology. This number should increase now that the credit card companies are making merchants responsible for any swiping fraud because old technology is being used.

However, online fraud continues to be a problem. It is reported that card not-present fraud (CNP) rose almost 50 percent last year alone. What is CNP fraud? It is when a criminal gets ahold of your credit card number and can buy things online and the goods are delivered electronically. The biggest items that are being purchased in CNP fraud are airline and other travel tickets, concert tickets, and digital gift cards. These items are easy to sell.

Criminals are also able to obtain individuals' personal information on the black market and open new credit cards in people's names without them ever knowing.

They will continue to find ways to commit fraud. What can you do to protect yourself? Use your EMV card. Frequently check your credit card and debit card balances. Check your credit report to see if any credit cards have been opened without your knowledge. But the best proactive strategy is to place a credit freeze on your account so no one can open an account in your name without your knowledge and authorization. You can contact any of the three credit bureaus to find out how to place a credit freeze on your account and the pros and cons of doing so.

In the meantime, the EMV "chip" cards are indeed chipping away at fraud. Use them and encourage your merchants to implement the technology so the number of businesses accepting EMV cards grows quickly to protect all of us from credit card fraud.