Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

[4,229 Psychiatric Patients' Records Hacked]

Bangor Health Center, a psychiatric practice located in Bangor Maine, has notified 4,229 patients that a hacker from Moldova has accessed their psychiatric records, including names, addresses, Social Security numbers, telephone numbers, diagnoses, and doctors' notes. *Read more*

HIPAA

[OCR Settles First Case With Wireless Provider for $2.5 Million]

Touted as the first Office for Civil Rights (OCR) settlement with a wireless health services provider, the OCR announced on April 24, 2017, that it has settled alleged HIPAA violations with CardioNet, based in Pennsylvania, for $2.5 million. CardioNet self-reported a data beach in January of 2012, stating that an unencrypted laptop of one of its employees was stolen from a vehicle parked outside the employee's home. *Read more*

[The Center for Children's Digestive Health Settles with OCR for $31,000]

The Office for Civil Rights (OCR) has announced that it entered into a settlement with The Center for Children's Digestive Health (CCDH) for $31,000. CCDH is a small for-profit health care provider with seven locations in Illinois. *Read more*

[HIPAA Refresher for Workplace Wellness Programs]

Now more than ever, workplace wellness programs are becoming increasingly popular among employers. A common concern many employers have is how to design a meaningful workplace program

April 27, 2017

FEATURED AUTHORS:

Pamela H. Del Negro
Linn Foster Freedman
Virginia E. McGarrity
Kathleen M. Porter
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Data Privacy
Drones
Enforcement + Litigation
HIPAA
International Privacy
Privacy Tips

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

intended to improve the health of participating employees while complying with HIPAA's privacy and security rules. Although employers are not covered entities, HIPAA may apply to an employer's workplace program if it is part of the group health plan. In a blog post last year, OCR Director Jocelyn Samuels sought to further explain how employers can use health data collected for wellness program purposes and what measures are necessary to protect health information under HIPAA. *Read more*

ENFORCEMENT + LITIGATION

Class Action Initiated Against Telehealth Provider for Disclosure of Sensitive Information

A class action was filed in Fort Lauderdale, Florida this week against a national telehealth provider, MDLive Inc. (MDLive) for its mobile app's alleged secret capture of screenshots containing sensitive patient information without restricting access to medical providers who have a legitimate need to view the information. The lawsuit was filed by Utah resident Joan Richards, who is seeking class certification of a class that she estimates will include thousands of other MDLive users and more than $5 million in damages. *Read more*

DATA BREACH

Eight Thousand Clients Affected by Data Breach at Two Massachusetts Accounting Firms

Recently, two Massachusetts accounting firms each notified the Office of the Massachusetts Attorney General and the Office of Consumer Affairs and Business Regulation of data breach incidents at their firms, resulting in the unauthorized access of their respective clients' names, addresses, and Social Security numbers. *Read more*

1.3 Million K-12 Students' Data Potentially Exposed

We often comment how no industry is immune from data breaches. That would include educational institutions and their vendors, as this story reminds us. Schoolzilla, a student data warehouse platform based in California, was alerted by security researcher Chris Vickery this month that while he was scanning the Internet for Amazon S3 buckets, (which is a misconfiguration in Amazon cloud storage devices), he came across a storage device that included a database containing the personal information, including some Social Security numbers and test scores, of 1.3 million K-12 students in the United

States. *Read more*

DATA PRIVACY

Facebook's New Software Suggests Passwords May One Day Be Obsolete

Facebook says that someday 'the password' will be a distant memory. For now, passwords are certainly necessary; however, Facebook has released a beta version of its Delegated Account Recovery software—a new way for social networks to be the backup security key when online consumers forget their password on different, non-Facebook, websites and services. Facebook says its new method is more secure than the typical password reset via an email or code to a mobile device. *Read more*

DRONES

Police Foundation Releases New Infographic and Tips for Law Enforcement Agencies' Use of Drones

The Police Foundation, a non-profit organization for policing across the United States, recently released a new infographic for law enforcement agencies seeking to establish a program for small unmanned aircraft systems (UAS or drones). The infographic, "UAS and Public Safety" [accessible here], includes an overview of operational, training, and legal and regulatory compliance considerations for law enforcement agencies interested in implementing UAS for public safety purposes. It also highlights key recommendations for law enforcement agencies related to community engagement before launching UAS to the skies. *Read more*

INTERNATIONAL PRIVACY LAWS

General Data Protection Regulation (GPDR) Series Part #1: Introduction and Overview

The General Data Protection Regulation (GPDR) (EU) 2016/679 of April 27, 2016, which goes into effect in May 2018, will introduce major changes to the law on the processing of personal data in the European Union. Over the next twelve months, several European Union law firms we work very closely with will join us in providing you with more information on the GDPR. Different themes will be tackled month by month to help you prepare for the GDPR deadline.

Part #1 of this GDPR Series is brought to you by FIDAL, a French law

firm. Subsequent blog entries in this series will be brought to you by the law firms of Graf von Westphalen (Germany), Mills & Reeve (United Kingdom) and VanBenthem & Keulen (Netherlands) as well as Robinson & Cole (United States).

GDPR Effective Date and Geographical Scope of Application

The GDPR will apply as of May 25, 2018. It provides a single set of very innovative rules directly applicable in the entire European Union (EU), without the need for national implementing measures—which means that any personal data processing ongoing at this date shall be in compliance with the GDPR. This leaves one year for companies to ensure compliance with the GDPR. The GDPR provides for a scope of application wider than processing undertaken in EU countries. *Read more*

PRIVACY TIPS

#84 - Utility Company Imposters Scaring and Scamming Vulnerable Consumers

A new but old scam is on the rise and is reportedly hitting droves of unwary and vulnerable consumers. The frequency of this scam has increased now that tax season is over, and W2 scams are difficult to succeed this time of year. The criminals are always trying to find ways to make money, and sometimes old scams still work.

Similar to the scam where criminals call consumers pretending to be from the IRS and scaring people into sending them money because they believe it is the IRS and that they are behind on taxes (the IRS will NEVER call you on the phone), in this scam, the criminals call pretending to be from the utility company and threaten to shut off your electricity and power. Losing your electricity is a scary thought, so it has been quite successful.

The caller says you must wire money quickly or use a prepaid card and tries to pressure the consumer into believing the money must be paid that day or the power will be shut off. This is not how utility companies work, so if you get a call like this, get the person's name and number and tell them you will call them back.

Contact the utility company through the phone number provided on your bill. You can call the company to check on your account, and to verify that you are up to date or behind, and if you are behind, at least you know you are talking to the right people and not a scam artist.

Utility companies do not shut off your electricity just like that. If you are behind on your bill, try to work with the company to enter into a payment plan, but make sure you are working with the company

directly and not some random person who calls you on the phone.

Never wire money or pay from a prepaid card to anyone over the phone if they have called you. Make sure you are working with the company itself to work out any details of payment. Be suspicious of anyone calling on the telephone asking for money. It is unusual and suspicious and probably a scam.

#85 - OIG Warns Consumers of Phone Call Scams by OIG Imposters

Phone call scams are on the rise. In addition to scam artists posing as employees of utility companies (see blog post-Privacy Tip #84), the Office of the Inspector General (OIG) has issued a warning to consumers about a phone scam involving imposters of its agency.

The imposters call consumers saying they are from the OIG and that the consumer is eligible to receive a federal grant because they paid their taxes on time. The callers have spoofed the OIG 800 number to make the call look legitimate. The 800 number (1-800-447-8477) is the actual OIG hotline number to report potential fraud. The gall of these people.

The scammers sound official and tell the consumer they must verify their identity so they can quality for the grant. They ask the consumer to verify their personal information, including Social Security number and bank account number. They are advised that they need to pay a processing fee, and give payment information over the phone.

The criminals not only scam consumers into paying the fee, but because they are getting all of the consumer's personal information, they can then open up credit card accounts and get into people's bank accounts.

The OIG says it does not make unsolicited telephone calls to consumers, and reminds consumers not to give their personal information, including their Social Security number or bank account number, to anyone over the phone.