

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks



CYBERSECURITY

[OCR Issues Checklist for Responding to Cyber-Attack](#)

The Office for Civil Rights (OCR) recently released guidance entitled "[My Entity Just Experienced a Cyber-attack! What Do We Do Now?](#)" The checklist is a practical tool for health care entities and outlines several steps to take following a cyber-attack. Of course, there are more steps before, during, and after a cyber-attack and these are the bare minimum; nonetheless, any time guidance is issued by OCR it is worth a read. [Read more](#)

[Companies Using IoT Being Hit with Security Breaches](#)

A new survey released by Altman Vilandrie & Company, which surveyed 400 IT personnel who have purchased Internet of Things (IoT) security products, shows that 46 percent of companies that buy IoT security admitted they have experienced an IoT-related security intrusion or breach within the last two years, representing hundreds of millions of dollars. [Read more](#)

DATA BREACH

[Medicaid Documents Thrown in Dumpster](#)

The North Dakota Department of Human Services has admitted that one of its employees threw Medicaid claim resolution worksheets into a dumpster instead of disposing of them in a secure on-site shredding receptacle. The result? The documents were found in the dumpster by a citizen who notified the department, who then notified almost 2,500 patients of the incident. [Read more](#)

ENFORCEMENT + LITIGATION

[Murder Arrest Warrant Weaves Web of Data Evidence in Fitbit,](#)

June 15, 2017

FEATURED AUTHORS:

[Nuala E. Droney](#)
[Linn Foster Freedman](#)
[Benjamin C. Jensen](#)
[Kathryn M. Rattigan](#)
[Norman H. Roos](#)

FEATURED TOPICS:

[Cybersecurity](#)
[Data Breach](#)
[Drones](#)
[Enforcement + Litigation](#)
[Privacy Tip](#)

VISIT + SHARE:

[Insider Blog](#)
[R+C website](#)
[Twitter](#)
[Facebook](#)
[LinkedIn](#)

Facebook, Alarm Systems, and More

The warrant that led to the arrest of a husband for the alleged murder of his wife weaves a web of electronic evidence. Based in large part on Fitbit fitness tracker data, Connecticut authorities have charged Richard Dabate with the murder of his wife, Connie. He also faces charges of tampering with evidence and making false statements. The [warrant](#) is a fascinating read. The prosecution claims that Mr. Dabate's interview with police following his wife's death on December 23, 2015, must be false, based on the timeline the data creates. Over 50 pages long, the data documents the investigators' attempts to track Mr. Dabate and his wife on the day of her death. It compares Mr. Dabate's version of the events to the electronic trail that he and his wife left on that day—using Fitbit information, various IP addresses, cell phone records, emails, Facebook data, and alarm system records. [Read more](#)

[New Nevada Law Recognizes Enforceability of Blockchain Transactions, Blocks Local Government Regulation and Taxation](#)

Senate Bill 398, unanimously passed by the Nevada legislature and signed into law by the governor on June 5, represents the most far-reaching state legislation to date concerning the use of blockchain technology. Blockchain is a decentralized database system that can be used to track and manage a broad range of digital transactions. Originally conceived as the technology underlying Bitcoin virtual currency, blockchain technology continues to expand into other applications, including “smart contracts.” [Read more](#)

[Reader's Digest Publisher Settles Case Alleging It Sold Subscribers' Personal Information for \\$8.2M](#)

In what is being considered the largest-ever settlement of alleged violations of Michigan's privacy law (the Michigan Preservation of Personal Privacy Act), the publisher of Reader's Digest has agreed to pay out \$8.2 million to settle a proposed class-action lawsuit brought by consumers who allege that the publisher sold subscribers' personal information to data brokers and other third parties. [Read more](#)

DRONES

[The State of the Drones: Unclear Laws and Anti-Drone Technology](#)

Over the past decade, since the Federal Aviation Administration (FAA) first permitted the use of drones for commercial and hobbyist purposes, after the 2012 directive of Congress for the FAA to come

up with a “comprehensive plan” for integrating drones into the National Airspace, drone use has grown substantially. However, with that growth has come concerns among lawmakers and regulators, at both the state and federal level, about privacy, smuggling, collisions with manned aircraft, safety, and national security, as well as private property owners looking to protect their privacy and property interests. That’s where anti-drone technology and systems come into play. From sophisticated technologies like jamming and control override systems to more amateur methods like net launchers or simply shooting a drone out of the sky, the law has yet to catch up with the state of technology—on either side. It has left the drone industry and property owners in a state of limbo. [Read more](#)

[NJ Law Restricting Drones Will Have to Be Rewritten](#)

The town of Garfield, New Jersey, has introduced new regulations related to hobbyist drone operation—or better yet, the nonoperation of drones above residences other than your own, commercial zones, roadways, government or public buildings, and specific property and parks that the city designates. Hobbyist drone operators may only fly their drones over their own residences. [Read more](#)

PRIVACY TIP #92

[Finally, HHS is Removing SSNs from Medicare Cards](#)

For those of you who know me, you know that I have been very frustrated with the federal and state governments for continuing to use Social Security numbers for eligibility, enrollment, and participation in Medicare and Medicaid. This includes listing individuals’ Social Security numbers on the Medicare and Medicaid cards.

The good news is that, finally, the Department of Health and Human Services (HHS) has figured out a way to SSNs from Medicare cards. The bad news is that the department won’t start sending new Medicare cards to beneficiaries until April 2018.

For Medicare recipients, the listing of your SSN on your Medicare card increases your risk for identity theft if your card or number is lost or stolen. Your Medicare card and any documents that have your Medicare number listed on them should be kept in a secure place and/or shredded when they are no longer needed. For those of you who care for seniors, take heed and assist your loved ones with protecting Medicare data. Scammers prey on seniors through the mail and over the telephone.

The FTC has listed some ways to avoid Medicare scams: between now and when the new Medicare cards are released:

- Is someone calling, claiming to be from Medicare, and asking for your Social Security number or bank information? Hang up. That's a scam. First, Medicare won't call you. Second, Medicare will never ask for your Social Security number or bank information.
- Is someone asking you to pay for your new card? That's a scam. Your new Medicare card is free.
- Is someone threatening to cancel your benefits if you don't give up information or money? Also a scam. New Medicare cards will be mailed out to you automatically. There won't be any changes to your benefits.

Updating Medicare cards so they don't list Social Security numbers is an important step in reducing the risk of identity theft for seniors.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP



© 2017 Robinson & Cole LLP. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission. This document should not be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.