AN A.S. PRATT PUBLICATION
MAY 2018
VOL. 4 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 4 | MAY 2018

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [107] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2018–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

The Government's Use of Data Analytics to Identify Healthcare Fraud

By Merle M. DeLancey, Jr.*

Although data analytics has been around for years, only over the last decade has the government appeared to become better at using it to detect potential fraud. This article discusses the use of data analytics in connection with investigations involving home health agencies, physician referrals, retail pharmacies, the distribution of opioids, and more.

No one knows exactly how much fraudulent conduct costs the United States' healthcare system. Some suggest it may cost Medicare, Medicaid, and private insurers $100 billion each year. Regardless of the exact amount, everyone agrees that the fraudulent activities result in more expensive healthcare and possibly the deprivation of healthcare for some.

The Department of Justice ("DOJ") and agency inspectors general have recovered billions of dollars based upon demonstrated or alleged healthcare fraud. These cases and investigations, however, have generally been limited to a specific company or class of providers. Government investigators have struggled for years with how to identify fraudulent practices in government healthcare programs involving large volumes of claims.

Since 1990, the Government Accountability Office ("GAO") has designated Medicare a high-risk program because of its size, complexity, and susceptibility to mismanagement and improper payments. The Centers for Medicare & Medicaid Services ("CMS") estimates Medicare contractors process 4.6 million claims per day. Medicaid, the Department of Veterans Affairs ("VA"), and Department of Defense also process millions of claims. Data analytics appears to be a game changer in terms of the government's investigation of fraudulent activities relating to these large volume of claims healthcare programs.

DATA ANALYTICS: WHAT IS IT?

Although data analytics has been around for years, only over the last decade has the government appeared to become better at using it to detect potential fraud. Data analytics is the collection and organization of information in a way that raises red flags. Simply put, data analytics allows investigators to pore through hundreds of millions of claims and other transactions to identify anomalies and outliers. Anomalies and outliers are suspicious claims which warrant additional review. While data

* Merle M. DeLancey, Jr., is a partner at Blank Rome LLP representing clients contracting with federal and state governments, primarily in the healthcare industry, involved in a broad spectrum of government contracting issues and litigation. Resident in the firm's Washington, D.C., office, he may be contacted at mdelancey@blankrome.com.

analytics may not catch every fraudulent practice, it can identify the most egregious. Significantly, the outliers or suspicious claims are not evidence of fraud, but they are a good predictor of providers who will be subject to a federal investigation.

Data analytics has been used to ferret out fraud in a variety of areas of the healthcare system. To date, it has most commonly been used in connection with Medicare investigations involving home health agencies, physician referrals, retail pharmacies, and, most recently, the distribution of opioids.

Home Health Agencies

In June 2016, the Department of Health and Human Services- Office of Inspector General ("HHS-OIG") reported finding over 500 home health agencies ("HHA") and 4,500 physicians were outliers on multiple characteristics commonly found in OIG-investigated cases of home health fraud. Further, the OIG identified 27 geographic areas in 12 states as hotspots for characteristics commonly found in OIG-investigated cases of home health fraud. Specifically, the OIG identified five distinct characteristics common to HHA fraud cases:

- High percentage of episodes in which the beneficiary had no recent visits with the supervising physician;
- High percentage of episodes that were not preceded by a hospital or nursing home stay;
- High percentage of episodes with a primary diagnosis of diabetes or hypertension;
- High percentage of beneficiaries with claims from multiple HHAs; and
- High percentage of beneficiaries with multiple home health readmissions in a short period of time.

Based upon a review of millions of claims, the OIG then identified HHAs and supervising physicians that were statistical outliers with regard to the above characteristics in comparison to their peers nationally. The OIG used a similar outlier approach when identifying so-called "hotspots."

Anti-Kickback Schemes

Data analytics provides fast access to claims data and also allows investigators to identify patients who were referred to a particular doctor or healthcare provider by another physician or provider. Again, while this information itself does not demonstrate fraudulent practices, it is used to uncover illegal kickback schemes such as those involving patient brokers.

Retail Pharmacies

The national prescription drug market is approximately $129 billion annually. Unsurprisingly, such a large market attracts unscrupulous providers. In 2012, the OIG examined billing records of pharmacies participating in the Medicare Part D

program. Of the then 59,000 retail pharmacies that billed the government under the Part D program, investigators identified 2,600 pharmacies that, in their view, had questionable billing. Investigators examined factors such as the total amount billed to Medicare, the amount billed per beneficiary, the number of prescriptions written per prescriber, and the percentage of prescriptions for various types of drugs. Based upon these metrics, problem pharmacies were identified for further investigation based upon anomalous conduct when compared to that of other participating pharmacies.

Opioid Distribution

DOJ recently announced the Opioid Fraud and Abuse Detection Unit that will use data analytics to combat opioid fraud. The new unit will focus specifically on illegal opioid distribution and will use fraud data to track down people who may be contributing to opioid addiction. This is the first time DOJ has used data analytics in fraud prevention, both specifically related to the opioid crisis and in broader prevention efforts.

OTHER FEDERAL HEALTHCARE PROGRAMS

Because Medicaid is a shared federal/state program, the use of data analytics has been less frequent. Under Medicaid, each state pays claims; thus, there is no uniform system of data collection. As a result, even if a fraudulent provider is identified in one state, there is nothing to prevent the provider from moving its illegal operations to another state. But states are working, individually and collectively, to address these data problems. Currently, approximately 35 states have agreed to submit their Medicaid transaction data to a national database. In addition, California, New York, Massachusetts, and Utah have implemented or have publicly announced their intention to implement data analytics programs.

The Department of Veterans Affairs and CMS recently announced plans to share data and best practices on fraud prevention and detection, including allowing the VA to take advantage of CMS's use of data analytics to detect fraud.

WHAT SHOULD PROVIDERS DO?

It is clear, the use of data analytics is here to stay. For example, in November 2017, the HHS-OIG issued a request for information seeking industry input on data analytics and data visualization tools. These tools include a possible cloud-based solution able to handle large volumes of claims and other data and the ability to develop visualizations and dashboards to allow stakeholders to easily identify patterns or anomalies in such data. Further, in its fiscal year 2019 budget request, the HHS-OIG requested approximately $23 million in additional funding for fraud programs that historically have relied heavily on the use of data analytics.

As a result, healthcare providers need to incorporate data analytics into their compliance programs. Providers should look for trends and aberrant behavior on a monthly basis. The specifics will depend upon the provider's service area. Retail pharmacies will want to analyze the amount billed per beneficiary, the number of prescriptions written per prescriber, and the percentage of prescriptions for various types of drugs. Home health agencies should review claims involving patients that have not had recent visits with the supervising physician, that were not preceded by a hospital or nursing home stay, and patients with multiple home health readmissions in a short period of time. Physician practices will want to review beneficiary referral metrics and trends in the type and number of procedure claims to federal healthcare programs.