HOT TOPICS FROM DOJ TO OIG TO CMS

Lynn M. Barrett, Esq., CHC, CCP
Barrett Law, PA
lynn@blhealthlaw.com

Health Ethics Trust
Washington Executive Course
May 2022

Agenda

1. Department of Justice
   - Corporate Compliance Program Guidance
     - Certain Enforcement Actions
   - Individual Accountability
     - Certain Enforcement Actions
   - Pandemic-Related Fraud
     - Certain Enforcement Actions
   - Cyber-Fraud & Cyber Security

2. Office of Inspector General (OIG) Hot Topics
   - 2022 OIG Advisory Opinions
   - OIG Advisory Opinion Changes
   - OIG Self-Disclosure Protocol

Agenda

3. **CMS Hot Topics**
   - ❑ Telehealth
   - ❑ Open Payments
   - ❑ Certain Surveys & Audits

4. **Board Roles & Responsibilities**
   - ❑ Cases
   - ❑ Responsibility for Cybersecurity?

Department of Justice "Hot Topics"

- Corporate Compliance Program Guidance
- Individual Accountability
- Pandemic-Related Fraud
- Cyber-Fraud & Cyber-Security

A Brief Look at Prior DOJ Guidance

- 2017 – DOJ Fraud Section publishes Evaluation of Corporate Compliance Programs (ECCP) containing import topics and sample questions it uses when evaluating the effectiveness of corporate compliance programs

- DOJ's "Principles of Federal Prosecution of Business Organizations" include "Filip Factors"

  - One factor is the existence and effectiveness of the corporation's pre-exiting compliance program as well as remedial efforts to implement an effective corporate compliance program or to improve an existing one.

A Brief Look at the 2019 Changes

- 11 Sections:
  1. Analysis and Remediation of Underlying Conduct
  2. Senior and Middle Management
  3. Autonomy and Resources
  4. Policies and Procedures
  5. Risk Assessment
  6. Training and Communications
  7. Confidential Reporting and Investigation
  8. Incentives and Disciplinary Measures
  9. Continuous Improvement, Periodic Testing and Review
  10. Third Party Management
  11. Mergers & Acquisitions

A Brief Look at the 2019 Changes

- Expands DOJ Guidance to beyond the Fraud Section to DOJ's entire criminal division
- Focuses on 3 areas of corporate compliance:
  - Risk assessments – CCP must be proportionate to identified risks
  - Culture of compliance - Entities must demonstrate financial, practical and philosophical support for compliance
  - Continuous compliance program improvement – Entities should continually review, reassess and improve their CCP
- Effect on False Claims Act (FCA) Guidance

A Brief Look at the 2019 Changes

- There are 3 Fundamental Questions prosecutors must ask when evaluating the effectiveness of a Corporate Compliance Program (CCP):
  - (1) Is the compliance program well designed?
  - (2) Is the compliance program being implemented effectively?
  - (3) Does the compliance program work in practice?

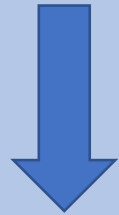
The 2020 Changes

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

The 2020 Changes

- Is the program being implemented effectively?



- Is the program adequately resourced and empowered to function effectively?

The 2020 Changes

- There are <u>3 Fundamental Questions</u> prosecutors must ask when evaluating the effectiveness of a Corporate Compliance Program (CCP):
  - (1) Is the compliance program well designed?
  - (2) Is the program adequately resources and empowered to function effectively?
  - (3) Does the compliance program work in practice?

The 2020 Guidance: Question 1

Step 1: Risk Assessment

✓ Design
✓ Comprehensiveness
✓ Accessibility
✓ Responsibility for Operational Integration
✓ Gatekeepers

Best Practice: Coordinated surveys/questionnaires
Compliance committee

The 2020 Guidance: Question 1

Step 2: Policies & Procedures

- ✓ Design
- ✓ Comprehensiveness
- ✓ Accessibility
- ✓ Responsibility for Operational Integration
- ✓ Gatekeepers

This Photo by Unknown Author is licensed under CC BY

Best Practice: Code of Conduct
Readability
Accessible
Searchable

The 2020 Guidance: Question 1

Step 3: Training and Communication

- ✓ Risk-Based Training
- ✓ Form/Content/Effectiveness of Training
- ✓ Communications about Misconduct
- ✓ Availability of Guidance

Best Practice:

Frequency
Short reminders
Real life scenarios/case studies
On-going tests

The 2020 Guidance: Question 1

Step 4: Confidential Reporting & Investigation Process

- ✓ Effectiveness of the Reporting Mechanism
- ✓ Properly Scoped Investigations by Qualified Personnel
- ✓ Investigation Response
- ✓ Resources and Tracking of Results

Best Practice: Coordination & cooperation
Qualified personnel
Tracking/Turn-around
If legal – Upjohn warnings

The 2020 Guidance: Question 1

Step 5 : Third Party Management

- ✓ Risk-Based and Integrated Processes
- ✓ Appropriate Controls
- ✓ Management of Relationships
- ✓ Real Actions & Consequences

Best Practice: Due diligence
Contract provisions

Enforcement Action: Billing Company

FOR IMMEDIATE RELEASE Tuesday, October 14, 2014

Radiology Billing Company To Pay $1.95 Million To Resolve False Claims Act Allegations

ATLANTA - The United States Attorney's Office announced that it has reached a settlement with Medical Business Service, Inc. (MBS), which agreed to pay $1.95 million to settle claims that it violated the False Claims Act by fraudulently changing diagnosis codes on claims to Medicare and Medicaid, in order to get the rejected claims paid on behalf of radiologists. MBS was located in Florida, with an office in Duluth, Ga.

"Billing companies provide a key check-point to combat medical billing fraud. Consequently, they will be examined with the same scrutiny as healthcare providers," said United States Attorney Sally Quillian Yates.

J. Britt Johnson, Special Agent in Charge, FBI Atlanta Field Office, stated: "Federal funds designated for use through the Medicare and Medicaid programs are much needed but limited. When those funds are not used as intended, the system does not work as intended and people suffer. The FBI will continue to work with its various law enforcement partners in dedicating significant investigative resources toward ensuring that these federally funded healthcare based programs are not abused."

"The health care providers who contracted with MBS placed their trust in the company to correctly process claims and not submit fraudulent information to the Medicare and Medicaid programs," said Derrick L. Jackson, Special Agent in Charge of the U.S. Department of Health and Human Services, Office of Inspector General in Atlanta. "The lack of compliance and oversight by MBS placed all these providers at risk. Billing services such as MBS have no less of a duty to ensure truthful information on claims than do the providers who use these services."

Enforcement Action: Management Company

FOR IMMEDIATE RELEASE Thursday, April 8, 2021

South Carolina's Largest Urgent Care Provider and its Management Company to Pay $22.5 Million to Settle False Claims Act Allegations

Columbia, South Carolina --- Acting United States Attorney for the District of South Carolina M. Rhett DeHart announced today that Doctors Care, P.A. ("Doctors Care") – South Carolina's largest urgent care provider network – and its management company, UCI Medical Affiliates of South Carolina, Inc. ("UCI"), will pay $22.5 million to resolve civil allegations of healthcare fraud in violation of the False Claims Act.

The case began with a whistleblower complaint alleging that Doctors Care, UCI, and UCI Medical Affiliates, Inc. (a related holding company), falsely certified that certain urgent care visits were performed by providers who were credentialed to bill Medicaid, Medicare, and TRICARE for medical services. Whereas, the services were performed by non-credentialed providers, according to the complaint.

Federal health insurance companies require physicians and midlevel providers to apply for and receive approval to bill any services to the insurer. This approval is known as a provider's "billing credentials." Providers are obligated to renew these billing credentials periodically and must obtain new credentials with new employment.

As early as 2013 and continuing to 2018, it is alleged that UCI was unable to secure and maintain necessary billing credentials for most Doctors Care providers. UCI knew that federal insurance programs would deny claims submitted with the billing number of a provider who had not yet received their billing credentials. But instead of solving its credentialing problem – or holding claims while a temporary solution could be found – UCI allegedly submitted the claims falsely, "linking" the uncredentialed rendering providers to credentialed billing providers in order to get the claims paid.

With each "linked" bill, it is alleged that UCI knowingly submitted a false claim for payment. Evidence obtained in support of the allegations includes emails memorializing UCI's "linking" scheme and well-organized "cheat sheets," as employees called them, which UCI used to keep track of properly-credentialed billing providers whose names could be substituted on uncredentialed providers' bills.

The 2020 Guidance: Question 1

Step 5 : Mergers & Acquisitions

- ✓ Due Diligence Process
- ✓ Integration in the M&A Process
- ✓ Processes Connecting Due Diligence to Implementation

Best Practice: Due diligence
Contract provisions
Indemnification
Reps & warranties

Enforcement Actions: Private Equity

From August 2009 to the present, MassHealth and its contracted managed care entities paid SBMHC more than $123 million for outpatient services including mental health counseling, such as psychiatric diagnostic evaluations and psychotherapy. The AG's Office estimates that a significant portion of that $123 million was based on fraudulent claims for services rendered by unlicensed, unqualified, and unsupervised staff to more than 30,000 MassHealth members.

The complaint was filed in U.S. District Court against SBMHC and Peter J. Scanlon, who founded and owned the company until April 2012. The complaint also names H.I.G. Growth Partners, LLC and H.I.G. Capital, LLC (collectively, HIG), which created Community Intervention Services (CIS) to acquire SBMHC from Scanlon, as well as co-founder and CEO of CIS, Kevin P. Sheehan.

The AG's Office alleges that HIG, CIS, Scanlon, and Sheehan knew that SBMHC was providing services in violation of regulatory requirements and did not bring SMBHC operations into compliance or make any attempts to repay the money owed to MassHealth, as required by law. HIG allegedly cited the large profit margins as a reason to acquire the company.

Enforcement Actions: Private Equity

Massachusetts alleged that C.I.S. and the H.I.G. fund and sponsor became aware via pre-acquisition due diligence that the mental health centers were using unlicensed and inadequately supervised personnel. It further alleged that after the acquisition, the Director of Clinical Services of the mental health chain informed multiple C.I.S. executives that the mental health centers were using unlicensed and unsupervised personnel, and that the problem increased as the private equity owners pressed for growth in the business. Subsequently, "tiger teams" formed by the mental health chain investigated and reported to the C.I.S. Board on the licensure and supervision problems, and recommended to the C.I.S. Board that the mental health centers hire a "substantial number" of "qualified supervisors" in order to satisfy Massachusetts regulations.

According to the Complaint, the C.I.S. Board took no action to ensure the portfolio company corrected the staffing problems and considered the tiger teams to be an "enormous waste of time." In addition, Massachusetts alleged that the C.I.S. Board was "heavily involved in the operational decisions of [the mental health centers], including approving contracts, strategic planning, budgeting, and earnings issues." Finally, Massachusetts alleged that the H.I.G. defendants knew of these compliance issues because certain H.I.G. executives learned about them by serving on the Board of C.I.S.

https://www.faegredrinker.com/-/media/files/insights/pubs/2020/wsl_august20.pdf

Enforcement Actions: Private Equity

THE TIMELNE

Date	Event
9/9/2015	Yates memo released (PDF) outlining Justice Department's commitment to holding individuals accountable for wrongdoing.
? 4/29/2016	DOJ intervenes in Fortress et al. One of the first examples of DOJ including private equity firm as defendant in False Claims Act lawsuit against healthcare company.
? 5/5/2016	DOJ reaches $8.9 million settlement with Fortress Investment Group and Holiday Acquisition Corp.
? 12/15/2017	DOJ intervenes in part and declines to intervene in part in Medrano and Lopez v. Diabetic Care Rx case.
? 1/9/2018	Massachusetts attorney general intervenes in Martino-Fleming v. South Bay Mental Health Center et al.
? 9/18/2019	DOJ reaches $21.4 million settlement with private equity firm Riordan, Lewis & Haden and other defendants in Medrano v. Diabetic Care Rx case.
? 11/19/2020	DOJ intervenes in Johnson et al. v. Therakos case, reaches $11.5 million settlement with private equity firm The Gores Group and Johnson & Johnson subsidiary Medical Device Business Services. Of the $11.5 million, Gores agreed to pay $1.5 million.
? 7/21/2021	DOJ reaches $15.3 million settlement to resolve kickback and false billing allegations with Alliance Family of Companies. Of that, private investment firm Ancor Holdings will pay about $1.8 million.
? 10/14/2021	Massachusetts attorney general reaches $25 million settlement with private equity firm H.I.G. Capital, H.I.G. Growth Partners and two executives for their roles in Martino-Fleming case.

Source: Modern Healthcare research

Modern Healthcare Nov. 16, 2021

THE CASES

- U.S. et al. v. Fortress Investment Group et al. / 13-cv-00314 MO
  Click to view this case's details. You can also hover or touch the ? tooltip for a shorter summary.
- U.S. ex rel. Medrano and Lopez v. Diabetic Care Rx d/b/a Patient Care America, et al. / 15-cv-62617
  Click to view this case's details. You can also hover or touch the ? tooltip for a shorter summary.
- U.S. and the Commonwealth of Massachusetts ex rel. Martino-Fleming v. South Bay Mental Health Center; Community Intervention Services; H.I.G. Growth Partners; H.I.G. Capital; Peter J. Scanlon; and Kevin P. Sheehan / 15-CV-13065-PBS
  Click to view this case's details. You can also hover or touch the ? tooltip for a shorter summary.
- U.S. ex rel. Johnson et al. v. Therakos et al. / 12-cv-1454
  Click to view this case's details. You can also hover or touch the ? tooltip for a shorter summary.
- Six qui tam lawsuits, including U.S. ex rel. Mandalapu et al. v. Alliance Family of Companies et al. / 4:17-cv-00740
  Click to view this case's details. You can also hover or touch the ? tooltip for a shorter summary.

https://www.modernhealthcare.com/government/justice-departments-new-way-fight-healthcare-fraud-sue-private-equity

The 2020 Guidance: Question 2

A. <u>Commitment by Senior and Middle Management</u>

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law at all levels of the company. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.

The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. *See* U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company's "*governing authority* shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of it; "[*h*]*igh-level personnel* … shall ensure that the organization has an effective compliance and ethics program" (emphasis added)).

The 2020 Guidance: Question 2

B. <u>Autonomy and Resources</u>

Effective implementation also requires those charged with a compliance program's day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. "A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization." Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, "a small organization may [rely on] less formality and fewer resources." *Id.* Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

The 2020 Guidance: Question 2

C. <u>Incentives and Disciplinary Measures</u>

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear disciplinary procedures in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) ("the organization's compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct").

By way of example, some companies have found that publicizing disciplinary actions internally, where appropriate and possible, can have valuable deterrent effects. At the same time, some companies have also found that providing positive incentives – personnel promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership – have driven compliance. Some companies have even made compliance a significant metric for management bonuses and/or have made working on compliance a means of career advancement.

The 2020 Guidance: Question 3

III. <u>Does the Corporation's Compliance Program Work in Practice?</u>

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision." JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. *See* U.S.S.G. § 8B2.1(a) ("[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct"). Indeed, "[t]he Department recognizes that no compliance program can ever prevent all criminal activity by a corporation's employees." JM 9-28.800. Of course, if a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor should view the occurrence as a strong indicator that the compliance program was working effectively.

The 2020 Guidance: Question 3

A. Continuous Improvement, Periodic Testing, and Review

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47-120(2)(c) (looking to "[t]he auditing of the compliance program to assure its effectiveness"). Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

The 2020 Guidance: Question 3

B. Investigation of Misconduct

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken.

The 2020 Guidance: Question 3

C. <u>Analysis and Remediation of Any Underlying Misconduct</u>

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47.120(3)(c) ("to receive full credit for timely and appropriate remediation" under the FCPA Corporate Enforcement Policy, a company should demonstrate "a root cause analysis" and, where appropriate, "remediation to address the root causes").

The Yates Memo

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

September 9, 2015

MEMORANDUM FOR THE ASSISTANT ATTORNEY GENERAL, ANTITRUST DIVISION
THE ASSISTANT ATTORNEY GENERAL, CIVIL DIVISION
THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
THE ASSISTANT ATTORNEY GENERAL, ENVIRONMENT AND NATURAL RESOURCES DIVISION
THE ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION
THE ASSISTANT ATTORNEY GENERAL, TAX DIVISION
THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR, EXECUTIVE OFFICE FOR UNITED STATES TRUSTEES
ALL UNITED STATES ATTORNEYS

FROM: Sally Quillian Yates
Deputy Attorney General

SUBJECT: Individual Accountability for Corporate Wrongdoing

The Yates Memo

1. To be eligible for any cooperation credit, corporations must provide to the Department all relevant facts about the individuals involved in corporate misconduct.

2. Both criminal and civil corporate investigations should focus on individuals from the inception of the investigation.

3. Criminal and civil attorneys handling corporate investigations should be in routine communication with one another.

4. Absent extraordinary circumstances, no corporate resolution will provide protection from criminal or civil liability for any individuals.

5. Corporate cases should not be resolved without a clear plan to resolve related individual cases before the statute of limitations expires and declinations as to individuals in such cases must be memorialized.

6. Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.

The Yates Memo

Deputy Attorney General Rosenstein:

“investigations should not be delayed merely to collect information about individuals whose involvement was not substantial, and who are not likely to be prosecuted.”

“a company must identify all wrongdoing by senior officials, including members of senior management or the board of directors, if it wants to earn any credit for cooperation.”

“If a corporation wants to earn maximum credit, it must identify every individual person who was substantially involved in or responsible for the misconduct.”

DOJ Criminal Division Guidance

JUSTICE NEWS

Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime

Washington, DC ~ Thursday, October 28, 2021

Remarks as Prepared for Delivery

Thank you, Ray, for that introduction, and thank you all for having me today. I'm sorry that I am not able to be there in person but appreciate the ability to join you virtually.

I have three priorities for my time with you. First, I want to describe three new actions that the department is taking today to strengthen the way we respond to corporate crime. Second, I want to look forward and tell you about some areas we will be studying over the next months, with an eye to making additional changes to help further invigorate the department's efforts to combat corporate crime. But before both of those, I want to set the scene by discussing trends, as well as the Attorney General's and my enforcement priorities, when it comes to corporate crime.

We can all agree the department's enforcement activities in the white-collar space ebb and flow due to a variety of factors — some internal to the department and some external. When I started as a newly minted AUSA, it was an active time for enforcement against corporate crime — one that witnessed the prosecutions of executives at WorldCom, Qwest Communications, Adelphia, Tyco and Enron. I've experienced how — when given the right resources and support

https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute

DOJ Criminal Division Guidance

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

October 28, 2021

MEMORANDUM FOR ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
ACTING ASSISTANT ATTORNEY GENERAL, CIVIL DIVISION
ACTING ASSISTANT ATTORNEY GENERAL, ANTITRUST DIVISION
ASSISTANT ATTORNEY GENERAL, ENVIRONMENT AND NATURAL RESOURCES DIVISION
ACTING ASSISTANT ATTORNEY GENERAL, TAX DIVISION
ACTING ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
DIRECTOR, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS
ALL UNITED STATES ATTORNEYS

FROM: THE DEPUTY ATTORNEY GENERAL

SUBJECT: Corporate Crime Advisory Group and Initial Revisions to Corporate Criminal Enforcement Policies[1]

https://www.justice.gov/dag/page/file/1445106/download

Enforcement Action: Yates in Action

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE | Tuesday, April 12, 2022

Physician Partners of America to Pay $24.5 Million to Settle Allegations of Unnecessary Testing, Improper Remuneration to Physicians and a False Statement in Connection with COVID-19 Relief Funds

Physician Partners of America LLC (PPOA), headquartered in Tampa, Florida, its founder, Rodolfo Gari, and its former chief medical officer, Dr. Abraham Rivera, have agreed to pay $24.5 million to resolve allegations that they violated the False Claims Act by billing federal healthcare programs for unnecessary medical testing and services, paying unlawful remuneration to its physician employees and making a false statement in connection with a loan obtained through the Small Business Administration's (SBA) Paycheck Protection Program (PPP). Certain PPOA affiliated entities are jointly and severally liable for the settlement amount, including the Florida Pain Relief Group, the Texas Pain Relief Group, Physician Partners of America CRNA Holdings LLC, Medical Tox Labs LLC and Medical DNA Labs LLC.

The United States alleged that PPOA caused the submission of claims for medically unnecessary urine drug testing (UDT), by requiring its physician employees to order multiple tests at the same time without determining whether any testing was reasonable and necessary, or even reviewing the results of initial testing (presumptive UDT) to determine whether additional testing (definitive UDT) was warranted. PPOA's affiliated toxicology lab then billed federal healthcare programs for the highest-level UDT. In addition, PPOA incentivized its physician employees to order presumptive UDT by paying them 40% of the profits from such testing in violation of the Stark Law, which prohibits physicians from referring patients to receive "designated health services" payable to Medicare or Medicaid from entities with which the physician or an immediate family member has a financial relationship, unless an exception applies.

The United States further alleged that PPOA required patients to submit to genetic and psychological testing before the patients were seen by physicians, without making any determination as to whether the testing was reasonable and necessary, and then billed federal healthcare programs for the tests.

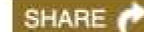
/1445106/download

Enforcement Action: Yates in Action

Department of Justice

U.S. Attorney's Office

Eastern District of Texas



FOR IMMEDIATE RELEASE Thursday, January 20, 2022

Seven Texas Doctors and a Hospital CEO Agree to Pay over $1.1 Million to Settle Kickback Allegations

Hospital CEO Excluded from Federal Healthcare Programs for Three Years

SHERMAN, Texas – Seven Texas doctors and a hospital executive have agreed to pay a total of $1,106,449 to resolve False Claims Act allegations involving illegal remuneration in violation of the Anti-Kickback Statute and Stark Law, and to cooperate with the Department's investigations of and litigation against other parties, announced Eastern District of Texas U.S. Attorney Brit Featherston today.

"Paying kickbacks to physicians distorts the medical decision-making process, corrupts our healthcare system, and increases the cost of healthcare funded by the taxpayer," said U.S. Attorney Brit Featherston. "Laboratories, marketers, and physicians cannot immunize their conduct by attempting to disguise the kickbacks as some sort of investment arrangement. Our office is committed to looking through the disguise and putting an end to any arrangement where the purpose is to improperly influence medical decision making through the payment of kickbacks."

The Anti-Kickback Statute prohibits offering, paying, soliciting, or receiving remuneration to induce referrals of items or services covered by Medicare, Medicaid, and other federally funded programs. The Stark Law forbids a hospital or laboratory from billing Medicare for certain services referred by physicians that have a financial relationship with the hospital or laboratory. The Anti-Kickback Statute and the Stark Law are intended to ensure that medical providers' judgments are not compromised by improper financial incentives and are instead based on the best interests of their patients.

page/file/1445106/download

Enforcement Action: Yates in Action

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Monday, April 4, 2022

Justice Department Files False Claims Act Complaint Against Two Laboratory CEOs, One Hospital CEO and Others Across Texas, New York, and Pennsylvania

The Justice Department has filed a complaint against two laboratory CEOs, one hospital CEO and other individuals and entities, alleging False Claims Act violations based on patient referrals in violation of the Anti-Kickback Statute and the Stark Law, as well as claims otherwise improperly billed to federal healthcare programs for laboratory testing.

According to the United States' complaint, laboratory executives and employees at True Health Diagnostics LLC (THD) and Boston Heart Diagnostics Corporation (BHD) allegedly conspired with small Texas hospitals, including Rockdale Hospital dba Little River Healthcare (LRH), to pay doctors to induce referrals to the hospitals for laboratory testing, which was then performed by BHD or THD. The complaint alleges that the hospitals paid a portion of their laboratory profits to recruiters, who in turn kicked back those funds to the referring doctors. The recruiters allegedly set up companies known as management service organizations (MSOs) to make payments to referring doctors that were disguised as investment returns but were actually based on, and offered in exchange for, the doctors' referrals. As alleged in the complaint, BHD and THD executives and sales force employees leveraged the MSO kickbacks to doctors to increase referrals and, in turn, their bonuses and commissions. The complaint alleges that laboratory tests resulting from this referral scheme were billed to various federal health care programs, and that the claims not only were tainted by improper inducements but, in many cases, also involved tests that were not reasonable and necessary. In addition, the complaint alleges that, to increase reimbursement, LRH falsely billed the laboratory tests as hospital outpatient services.

"The Department of Justice is committed to holding accountable individuals and entities who commit and profit from healthcare fraud," said Principal Deputy Assistant Attorney General Brian M. Boynton, head of the Justice Department's Civil Division. "We will continue to pursue those who enter into unlawful financial arrangements that waste taxpayer dollars, improperly influence healthcare providers' medical judgments and subject patients to unnecessary testing or other services."

e/1445106/download

DOJ Criminal Division Guidance

Attorney General Merrick B. Garland Delivers Remarks to the ABA Institute on White Collar Crime

Washington, DC ~ Thursday, March 3, 2022

As the Deputy Attorney General noted, I have made it clear that the Department's first priority in corporate criminal cases is to prosecute the individuals who commit and profit from corporate malfeasance.

It is our first priority because corporations only act through individuals.

It is our first priority because penalties imposed on individual wrongdoers are felt by those wrongdoers, rather than by shareholders or inanimate organizations.

It is our first priority because – as everyone who has counseled individual corporate officers know – the prospect of personal liability has an uncanny ability to focus the mind. That prospect is the best deterrent to corporate crime. And deterrence – after all – is what we are after.

But most important, the prosecution of individuals is our first priority because it is essential to Americans' trust in the rule of law. As I said a moment ago: the rule of law requires that there not be one rule for the powerful and another for the powerless; one rule for the rich and another for the poor.

When people see individuals walk while their companies pay the fines, they cannot help but think that essential principle has been violated.

Corporate Compliance & Enforcement

Assistant Attorney General Kenneth A. Polite Jr. Delivers Remarks at NYU Law's Program on Corporate Compliance and Enforcement (PCCE)

New York, NY ~ Friday, March 25, 2022

Remarks as Prepared for Delivery

I have been fortunate in my career to have served as a prosecutor, as a defense attorney, and to work as a chief compliance officer of a Fortune 500 company. The detection and prevention of criminal conduct has been a constant across these three roles. Perhaps the most challenging of the three roles has been serving in compliance.

I know the resource challenges. The challenges you have accessing data. The relationship challenges. The silo-ing of your function. You are called upon to be a resource for information, an enforcer of law and policy, and somehow the primary architect of your company's ethical culture. I have seen first-hand how a strong compliance program can ward off misconduct and empower ethical employees. Although I am the head of the Criminal Division, I believe that enforcement, while a critical tool, is not our only one. I believe that the number of prosecutions we bring is not necessarily the most accurate measure of our success.

Having served in these three positions, I know that your compliance role is perhaps the most impactful, because you have a direct role in utilizing the most effective tool in addressing crime – you are trying to prevent it in the first place. That is why we closely evaluate corporate compliance programs during our corporate investigations and after our corporate resolutions, and give significant credit to companies that build strong controls to detect and prevent misconduct.

Today, I want to describe in detail about how we evaluate corporate compliance programs to ensure that companies are designing and implementing effective compliance systems and controls, creating a culture of compliance, and promoting ethical values. As our Evaluation of Corporate Compliance Programs guidance makes clear, we expect an effective corporate compliance program to be much more than a company's policies, procedures, and internal controls. We expect companies to implement compliance programs that: (1) are well designed, (2) are adequately resourced and empowered to function effectively, and (3) work in practice.

Corporate Compliance & Enforcement

First, when we say that we expect a company's compliance program to be well designed, we closely examine the company's process for assessing risk and building a program that is tailored to manage its specific risk profile. We want to see whether the company has implemented policies and procedures that are designed to address the key risk areas identified in its risk assessments, and that those policies and procedures are easily accessible and understandable to the company's employees and business partners. We want to know how the company is training employees, management, and third-parties on the risk areas and responsibilities applicable to those individuals. Policies, training, and other processes should address relevant high-risk elements of the company's business model, such as third-party relationships or mergers and acquisitions. We want to see that the company has established a process for reporting violations of law or company policy that encourages employees to speak up without fear of retaliation, and that those reports are taken seriously, appropriately documented, investigated, and—if substantiated—remediated.

Second, when we are evaluating whether a compliance program is adequately resourced and empowered to function effectively, we want to know more than dollars, headcount, and reporting lines. We will review the qualifications and expertise of key compliance personnel and other gatekeeper roles. We want to know if compliance officers have adequate access to and engagement with the business, management, and the board of directors. We seek to understand whether and how a company has taken steps to ensure that compliance has adequate stature within the company and is promoted as a resource. A company's commitment to promoting compliance and ethical values at all levels—from the chief executive on down to middle and lower-level managers—is critical.

Third, we want to see evidence that the compliance program is working in practice. We look at whether the company is continuously testing the effectiveness of its compliance program, and improving and updating the program to ensure that it is sustainable and adapting to changing risks. We want to know that a company can identify compliance gaps or violations of policy or law. Equally importantly, we want to see how the company addresses the root causes of these gaps or violations and finds ways to improve its controls and prevent recurrence of issues. We want to see examples of compliance success stories—the discipline of poor behavior, the rewarding of positive behavior, the transactions that were rejected due to compliance risk, positive trends in whistleblower reporting, and the partnerships that have developed between compliance officers and the business. We are also interested in how a company measures and tests its culture—at all levels of seniority and throughout its operations—and how it uses the data from that testing to embed and continuously improve its ethical culture.

Corporate Compliance & Enforcement

There is a separate question of whether a company is demonstrating an ethical culture in practice. Do employees feel empowered to bring issues and questions to the management's attention? Are managers and compliance officers providing ethical advice to salespeople even though such advice may mean loss of business? Just as we use data analytics to detect and combat criminal schemes, we urge corporations to consider what data analytic tools they can use to monitor compliance with laws and policies within their operations and to ferret out wrongdoing when it occurs.

Corporate Compliance & Enforcement

Additional considerations:

- Consider requiring the CCO and CEO to certify that the CP is reasonably designed and implemented to detect and prevent violations of the law and is functioning effectively, and attest that all compliance reports submitted during the term of the resolution (guilty plea, deferred prosecution, non-prosecution) are "true, accurate, and complete reports."
  - Requires CCO input - meant to EMPOWER CCOs within the corporate entity and improve their position
  - Leaders must take ownership

- Failure to comply with compliance obligations could result in penalties from extension of resolution term to seeking corporate conviction

CMPs & The 8th Amendment

CMPs were adjusted in December 2021:

- For DOJ Penalties after 12/31/21:
  - Min: $11,803
  - Max: 23,607

- Excessive Fines:
  - Yates v. Pinellas:
    - $755.54 in damages for 214 false claims
    - $1,179,266 in penalties
    - 8th Amendment problem??

DOJ on Pandemic Fraud

Attorney General Merrick B. Garland Addresses American Bar Association National Institute on White Collar Crime

DOJ on Pandemic Fraud

In that regard, the President's FY22 budget seeks increases for the Justice Department's corporate criminal enforcement efforts. These increases extend to our 94 U.S. Attorneys' Offices, as well as to the Criminal, Antitrust, Tax, and Environment Divisions.

They include an additional $36.5 million for the U.S. Attorneys' Offices and the Criminal Division to bolster efforts to combat pandemic-related fraud.

These additional funds will allow the Department to hire 120 additional attorneys to execute that important mission. And this is on top of 34 attorneys the Criminal Division's Fraud Section hired in 2021.

The FY22 budget also seeks $325 million to fund more than 900 FBI agents to support the FBI's White Collar-Crime Program.

We are also bolstering our resources by adding force-multipliers to our prosecutors and agents. I want to highlight three of those force-multipliers.

As the President also noted in his address, I will soon be naming a chief prosecutor to lead specialized teams dedicated to combatting pandemic fraud. This will build on the existing work of the COVID-19 Fraud Enforcement Task Force that I established last May.

That task force, led by the Deputy Attorney General, includes nearly 30 agencies that administer and oversee pandemic relief funding, including the Labor Department, the Treasury Department, the Small Business Administration, the U.S. Postal Inspection Service, and the Pandemic Response Accountability Committee.

The Justice Department is also working more closely than ever with Inspectors General across the federal government to identify perpetrators of health care fraud, procurement fraud, and every other kind of government-program fraud.

DOJ on Pandemic Fraud

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, March 10, 2022

Justice Department Announces Director for COVID-19 Fraud Enforcement

Criminal and Civil Enforcement Actions Alleging Fraud Related to Over $8 Billion in Pandemic Relief

Today, the Justice Department announced the appointment of a Director for COVID-19 Fraud Enforcement to lead the department's criminal and civil enforcement efforts to combat COVID-19 related fraud, along with the latest results of criminal and civil enforcement actions that include alleged fraud related to over $8 billion in pandemic relief.

Effective immediately, Associate Deputy Attorney General Kevin Chambers will serve as the Director for COVID-19 Fraud Enforcement. Mr. Chambers will lead Justice Department efforts that to date have resulted in criminal charges against over 1,000 defendants with alleged losses exceeding $1.1 billion; the seizure of over $1 billion in Economic Injury Disaster Loan proceeds; and over 240 civil investigations into more than 1,800 individuals and entities for alleged misconduct in connection with pandemic relief loans totaling more than $6 billion.

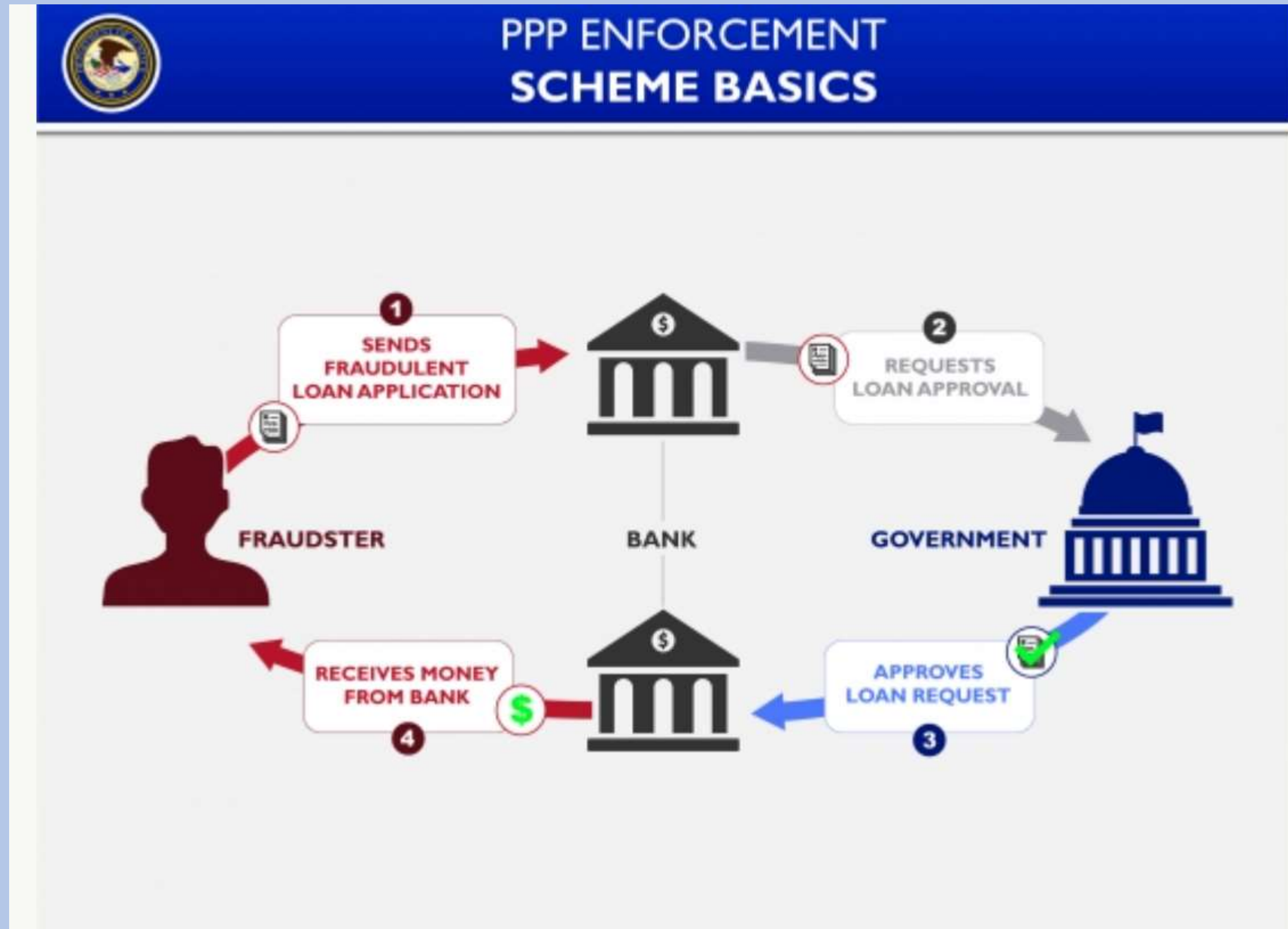
"The Justice Department remains committed to using every available federal tool — including criminal, civil, and administrative actions — to combat and prevent COVID-19 related fraud," said Attorney General Merrick B. Garland. "We will continue to hold accountable those who seek to exploit the pandemic for personal gain, to protect vulnerable populations, and to safeguard the integrity of taxpayer-funded programs."

DOJ on Pandemic Fraud

Fact Sheet: Combatting COVID-19 Fraud

In May 2021, the Attorney General established the COVID-19 Fraud Enforcement Task Force to marshal the resources of the Department of Justice in partnership with agencies across government to enhance efforts to combat and prevent pandemic-related fraud. The task force bolsters efforts to investigate and prosecute the most culpable domestic and international criminal actors and assists agencies tasked with administering relief programs to prevent fraud by, among other methods, augmenting and incorporating existing coordination mechanisms, identifying resources and techniques to uncover fraudulent actors and their schemes, and sharing and harnessing information and insights gained from prior enforcement efforts.

Pandemic Fraud



Pandemic Fraud

- Capitalized on scarcity to peddle fake vaccines and sell millions of counterfeit N95 masks and other personal protective equipment to health care facilities desperate to protect frontline workers

- Inflated payrolls to obtain loans larger than they were eligible to receive.

- Used shell companies and received assistance that they unlawfully diverted

- Set up operations to submit identical loan applications in the names of multiple companies.

- Fraudulently misrepresented the products or services they sold to the federal government.

What To Do??

Areas to perform risk assessments:

- ✓ Potential false certifications
- ✓ Labs
  - ✓ Respiratory panels
  - ✓ COVID testing
  - ✓ HRSA reimbursement
- ✓ Marketing
  - ✓ Collection entities looking for labs

PRF Reporting

>PRF Reporting

- Deadlines correspond to payment periods
- $10,000 +
- Healthcare related expenses/lost revenue attributable to COVID-19

>Period 1 reporting was extended – no signal of similar extension for Period 2

> Period 2 reporting (July 1- Dec 31, 2021) ended March 31, 2022; payments due April 30, 2022

> Demand Letters

Cyber-Fraud

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, October 6, 2021

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced today the launch of the department's Civil Cyber-Fraud Initiative, which will combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it," said Deputy Attorney General Monaco. "Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust."

Cyber-Fraud

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE | Tuesday, March 8, 2022

Medical Services Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan

First Settlement by the Department of Justice of a Civil Cyber-Fraud Case Under the Department's Civil Cyber-Fraud Initiative

Comprehensive Health Services LLC (CHS), located in Cape Canaveral, Florida, has agreed to pay $930,000 to resolve allegations that it violated the False Claims Act by falsely representing to the State Department and the Air Force that it complied with contract requirements relating to the provision of medical services at State Department and Air Force facilities in Iraq and Afghanistan. This is the Department of Justice's first resolution of a False Claims Act case involving cyber fraud since the launch of the department's Civil Cyber-Fraud Initiative, which aims to combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

Cyber- Security

Shown Here:
Introduced in House (09/30/2021)

117TH CONGRESS
1ST SESSION

H. R. 5440

To amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 30, 2021

Ms. CLARKE of New York (for herself, Mr. KATKO, Mr. THOMPSON of Mississippi, and Mr. GARBARINO) introduced the following bill; which was referred to the Committee on Homeland Security

---

A BILL

To amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

Cyber-Security

Organizations operating in critical infrastructure sectors must:

- Report "substantial" cyber incidents to the Cybersecurity and Infrastructure Security Agency ("CISA") within 72 hours after the entity “reasonably believes” the incident occurred.
- Provide reports to CISA of substantial new or different information that becomes available until the incident has concluded and been fully mitigated and resolved.
- Report ransom payments to CISA within 24 hours after making the ransom payment.
- Preserve data related to cyber incidents or ransom payments in accordance with procedures to be established by CISA

Cyber-Security

OCR Quarter 1 2022 Cybersecurity Newsletter

Defending Against Common Cyber-Attacks

Throughout 2020 and 2021, hackers have targeted the health care industry seeking unauthorized access to valuable electronic protected health information (ePHI). The number of breaches of unsecured ePHI reported to the U.S Department of Health and Human Service's Office for Civil Rights (OCR) affecting 500 or more individuals due to hacking or IT incidents increased 45% from 2019 to 2020.[1] Further, the number of breaches due to hacking or IT incidents accounted for 66% of all breaches affecting 500 or more individuals reported to OCR in 2020.[2]

Although some attacks may be sophisticated and exploit previously unknown vulnerabilities (*i.e.*, zero-day attack), most cyber-attacks could be prevented or substantially mitigated if HIPAA covered entities and business associates ("regulated entities") implemented HIPAA Security Rule requirements to address the most common types of attacks, such as phishing emails,[3] exploitation of known vulnerabilities, and weak authentication protocols. If an attack is successful, the attacker often will encrypt a regulated entity's ePHI to hold it for ransom, or exfiltrate the data for future purposes including identify theft or blackmail. Cyber-attacks are especially critical in the health care sector as attacks on ePHI can disrupt the provision of health care services to patients. This newsletter explores preventative steps regulated entities can take to protect against some of the more common, and often successful, cyber-attack techniques.

Cyber-Security

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3: Analyst Note

April 18, 2022 TLP: White Report: 202204181300

Hive Ransomware

Executive Summary

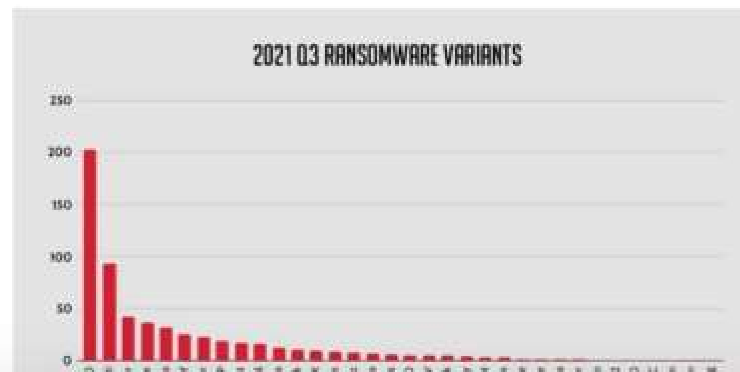
Hive is an exceptionally aggressive, financially-motivated ransomware group known to maintain sophisticated capabilities who have historically targeted healthcare organizations frequently. HC3 recommends the Healthcare and Public Health (HPH) Sector be aware of their operations and apply appropriate cybersecurity principles and practices found in this document in defending their infrastructure and data against compromise.

Report

The Hive ransomware group has been known to be operational since June of 2021 but in that time has been very aggressive in targeting the US health sector. One report covering the third quarter of 2021 – just months after they began operating – ranks them as the fourth most active ransomware operators in the cybercriminal ecosystem (see figure 1). Another report noted the observation of 355 companies in Hive's first 100 days of operation.

Their operations include the following features:

- They conduct double extortion (data theft prior to encryption) and support this with their data leak site which is accessible on the dark web
- They operate via the ransomware as a service (RaaS) model, which involves them focusing on development and operations of the ransomware and other



What to Do???

- ✓ Get back to HITECH Basics
  - ✓NIST Framework
- ✓Work closely with IT
- ✓Phishing exercises for all
- ✓Train and train again
- ✓Polices & Procedures

Office of Inspector General "Hot Topics"

- 2022 Advisory Opinions
- OIG Self-Disclosure Protocol
- OIG Guidance on Advisory Opinions

OIG 2022 Advisory Opinions

- **AO 22-01 (Jan. 19, 2022**) Regarding the proposed expansion of discount programs for low-income individuals.
- **AO 22-02 (Feb 9, 2022**) Regarding a proposed arrangement between Requestor and two individuals, pursuant to which Requestor and the individuals would reduce and subsidize certain costs incurred by qualifying patients of Requestor's children's hospital.
- **AO 22-03 (Feb. 14, 2022)** Regarding Requestors' proposal to pay salaries to, and nurse aide certification program tuition costs on behalf of, new employees who Requestors have hired to work as certified nurse aides for Requestors' home health agencies.
- **AO 22-04 (March 2,2022**) Regarding a program through which Requestor provides certain individuals access to digital contingency management and related tools to treat substance use disorders, where the Program is funded by customers, which could include individuals' health care providers or suppliers.
- **AO 22-05 (March 16, 2022)** Regarding the proposed subsidization of certain Medicare cost-sharing obligations in the context of a clinical trial.

OIG 2022 Advisory Opinions

- **AO 22-06 (April 11, 2022**) Regarding the provision of free genetic testing and genetic counseling services to individuals who meet specified clinical criteria.

- **AO 22-07 (April 25, 2022**) Regarding an arrangement whereby certain physicians have an ownership interest in a medical device company that manufactures products that may be ordered by the physician owners and a physician spouse of one of the physician owners.

- **AO 22-08 (April 27, 2022)** Regarding an arrangement whereby certain existing patients of Requestor use limited-use smartphones that Requestor loaned to such patients to facilitate access to telehealth services.

- **AO 22-09 (April 28,2022**) Regarding a proposed arrangement pursuant to which Requestor would compensate hospitals for certain specimen collection services for laboratory tests furnished by Requestor.

- **AO 22-10 (May 2, 2022)** Regarding (i) a modification to OIG Advisory Opinion 15-14, issued to the requestor on November 13, 2015, to include within the scope of that opinion, the requestor's proposal to provide financial assistance for certain past magnetic resonance imaging tests; and (ii) a second arrangement regarding the distribution of certain cooling and mobility items, ancillary to the arrangement addressed in OIG Advisory Opinion 15-14.

OIG Self Disclosure Protocol

UPDATED

OIG's Health Care Fraud Self-Disclosure Protocol

Note: This notice, issued on April 17, 2013, and amended on November 8, 2021, updates and renames the Provider Self-Disclosure Protocol.

OIG Advisory Opinions

DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20201

OIG Enforcement Policy Statement Regarding OIG's Assessment of Advisory Opinion Requests

January 6, 2022 (Updated January 13, 2022)

Pursuant to section 1128D of the Social Security Act (the Act), the Department of Health and Human Services (HHS), through the Office of Inspector General (OIG), publishes advisory opinions regarding the application of the Federal anti-kickback statute and safe harbor provisions, as well as OIG's administrative sanction authorities, to requesting parties' proposed or existing arrangements. More specifically, in consultation with the Department of Justice (DOJ) OIG issues written advisory opinions to requesting parties with regard to: (1) what constitutes prohibited remuneration under the Federal anti-kickback statute;[1] (2) whether an arrangement or proposed arrangement satisfies the criteria in section 1128B(b)(3) of the Act, or established by regulation (i.e., safe harbors),[2] for activities that do not result in prohibited remuneration; (3) what constitutes an inducement to reduce or limit services to Medicare or Medicaid program beneficiaries under section 1128A(b) of the Act; and (4) whether an activity or proposed activity constitutes grounds for the imposition of sanctions under section 1128, 1128A, or 1128B of the Act.

OIG's advisory opinion regulations at 42 C.F.R. Part 1008 contain the specific procedures for the submission of requests by individuals or entities for advisory opinions to—and the issuance of advisory opinions by—OIG. In a final rule entitled "Procedures Regarding the Submission of Advisory Opinion Requests to, and the Issuance of Advisory Opinions by, OIG," published on OIG's website on January 6, 2022 (the Final Rule),[3] OIG revised its advisory opinion regulations to remove a procedural provision that precluded the acceptance of an advisory opinion request and/or issuance of an advisory opinion when the same or substantially the same course of action is under investigation or is the subject of a proceeding involving HHS or another governmental

DHHS & CMS "Hot Topics"

- Telehealth
- Sunshine Act Reporting
- Surveys/Audits
- Medicare Advantge

Telehealth

Consolidated Appropriations Act of 2022:

- Medicare waivers will continue to apply for 151 days following the end of the PHE, including:
  - ✓ Originating site can include beneficiary's home
  - ✓ Eligible Practitioners include PT, OT speech & audiologists
  - ✓ Mental Health providers do not need to see patients in person before providing behavioral health services
  - ✓ Audio-only
  - ✓ FQHCs

Sunshine Act Reporting

- ✓ Due date March 31, 2022
- ✓ Physicians, APPs teaching hospitals
  - ➢ APPs as new recipients
- ✓ CY 2021
- ✓ 4 new categories
  - ➢ Debt forgiveness
  - ➢ Long-term medical supply or device loan
  - ➢ Acquisitions
  - ➢ Compensation for serving as faculty or as speaker for a Medical Education Program
- ✓ Disputing reports may occur until May 15. 2022

Audits & More Audits

Announced or Revised	Agency	Title	Component	Report Number(s)
January 2022	Administration for Children and Families	Audit of the Administration for Children and Families Awarding and Monitoring of an Unaccompanied Children Program Sole Source Contract to Deloitte Consulting LLP	Office of Audit Services	W-00-22-20029
January 2022	Health Resources and Services Administration	Hospital's Compliance With the Provider Relief Fund Balance Billing Requirement for Out - of - Network Patients	Office of Audit Services	W-00-22-35878
January 2022	Centers for Medicare and Medicaid Services	Nationwide Review of Hospice Beneficiary Eligibility	Office of Audit Services	W-00-22-35883
January 2022	Centers for Medicare and Medicaid Services	Followup Audit on CMS's Use of Medicare Data To Identify Instances of Potential Abuse or Neglect	Office of Audit Services	W-00-22-35882
January 2022	Centers for Medicare and Medicaid Services	Medicare Administrative Contractor Cost Report Oversight - Contract Review	Office of Audit Services	W-00-22-35881
January 2022	CMS, FDA	Mandatory Review of HHS Agencies' Annual Accounting of National Drug Control Program Funds	Office of Audit Services	W-00-22-52312
January 2022	OS	OIG DATA Act Audit and Data Completeness & Accuracy (2022)	Office of Audit Services	W-00-22-41021

Audits & More Audits

Hospital's Compliance With the Provider Relief Fund Balance Billing Requirement for Out - of - Network Patients

The Coronavirus Aid, Relief, and Economic Security (CARES) Act, Paycheck Protection and Health Care Enhancement Act, and Consolidated Appropriations Act, 2021, appropriated a combined $178 billion in relief funds to hospitals and other health care providers. This funding, known as the Provider Relief Fund (PRF), is administered by the Department of Health and Human Services (HHS), Health Resources and Services Administration (HRSA) and is intended to reimburse eligible health care providers for health care-related expenses or lost revenue attributable to COVID-19 and to ensure that Americans could get testing and treatment for COVID-19. Under the PRF terms and conditions, hospitals are eligible for PRF distribution payments if they attest to specific requirements, including a requirement that providers, such as hospitals, must not pursue the collection of out-of-pocket payments from presumptive or actual COVID - 19 patients in excess of what the patients otherwise would have been required to pay if the care had been provided by in-network providers. We refer to this limitation on balance billing, commonly referred to as "surprise billing," as the "balance billing requirement." We will perform a nationwide audit to determine whether hospitals that received PRF payments and attested to the associated terms and conditions complied with the balance billing requirement for COVID - 19 inpatients. We will assess how bills were calculated for out-of-network patients admitted for COVID-19 treatment, review supporting documentation for compliance, and assess procedural controls and monitoring to ensure compliance with the balance billing requirement.

Audits & More Audits

Nationwide Review of Hospice Beneficiary Eligibility

Hospice care can provide comfort to beneficiaries, families, and caregivers at the end of beneficiaries' lives. To be eligible for hospice care, they must be entitled to Medicare Part A and be certified as being terminally ill. The certification of terminal illness for hospice benefits shall be based on the clinical judgment of the hospice medical director or physician member of the interdisciplinary group, and the beneficiaries' attending physician, if they have one, regarding the normal course of their illness. OAS has performed several compliance audits of individual hospice providers in recent years, and each of those audit reports identified findings related to beneficiary eligibility. We will perform a nationwide review of hospice eligibility, focusing on those hospice beneficiaries that haven't had an inpatient hospital stay or an emergency room visit in certain periods prior to their start of hospice care.

Audits & More Audits

US Department of Labor announces enforcement,
effort for focused inspections in hospitals, nursing care facilities treating COVID-19 patients

WASHINGTON – For two years, millions of the nation's healthcare workers have been battling the coronavirus. Many have endangered themselves as they care for those who contract COVID-19 while working in high-risk settings that expose themselves and their families.

As the nation moves to the next phase of the pandemic, the U.S. Department of Labor recognizes the need to prepare for any new variants that may emerge and provide healthcare workers the protections they deserve.

The Department's Occupational Safety and Health Administration today announced an enforcement memorandum for a short-term increase in highly focused inspections directed at hospitals and skilled nursing care facilities that treat or handle COVID-19 patients.

OSHA's goal is to expand its presence to ensure continued mitigation to control the spread of COVID-19 and future variants of the SARS-CoV-2 virus, and protect the health and safety of healthcare workers at heightened risk for contracting the virus.

"We are using available tools while we finalize a healthcare standard," said Assistant Secretary of Labor for Occupational Safety and Health Doug Parker. "We want to be ahead of any future events in healthcare."

The agency will be initiating focused inspections to emphasize monitoring for current and future readiness to protect workers from COVID-19. Follow-up inspections will be conducted at sites that were previously issued citations, as well as where complaints were received but the agency did not conduct in-person inspections.

OSHA intends to expand its presence in targeted high-hazard healthcare facilities during a three-month period from March 9, 2022 to June 9, 2022. Through this focused enforcement initiative, the agency will verify and assess hospital and skilled nursing care employers' compliance actions taken, including their readiness to address any ongoing or future COVID-19 surges.

Medicare Advantage

Fact sheet

CY 2023 Medicare Advantage and Part D Final Rule (CMS-4192-F)

Apr 29, 2022 | Affordable Care Act

Share

CMS is issuing a final rule that advances CMS' strategic vision of expanding access to affordable health care and improving health equity in Medicare Advantage (MA) and Part D through lower out-of-pocket prescription drug costs and improved consumer protections.

An increasing number of Medicare beneficiaries receive services through MA and Part D plans. Over 27 million beneficiaries are enrolled in MA plans (including plans that offer Part D prescription drug coverage), and approximately 24 million beneficiaries are enrolled in standalone Part D plans. Additionally, an increasing number of beneficiaries who are dually eligible for both Medicare and Medicaid are enrolled in MA plans, Medicaid managed care, or both. About 4.1 million dually eligible beneficiaries currently receive their Medicare services through MA dual eligible special needs plans (D-SNPs).

Medicare Advantage

Press release

CMS Issues New Policies to Provide Greater Transparency for Medicare Advantage and Part D Plans

Apr 29, 2022 | Affordable Care Act

Share

Updated measures for 2023 will advance equity and increase access to affordable care

Today, the Centers for Medicare & Medicaid Services (CMS) issued a final rule for the Medicare Advantage (MA) and Part D prescription drug programs that will improve experiences for dually eligible beneficiaries and provide greater transparency for the MA and Part D programs. The measures set forth in the Contract Year 2023 MA and Part D Policy and Technical Changes final rule build on the agency's strategic pillars to be a responsible steward of public programs, as it continues to expand access to quality, affordable care and advance health equity for people with Medicare and Medicaid.

Certain Enforcement Actions: Medicare Advantage

Case 3:13-cv-03891-EMC Document 110 Filed 10/25/21 Page 1 of 96

1 SARAH E. HARRINGTON
Deputy Assistant Attorney General
2
STEPHANIE M. HINDS (CABN 154284)
3 Acting United States Attorney
4 MICHELLE LO (NYBN 4325163)
Chief, Civil Division
5
SHIWON CHOE (CABN 320041)
6 BENJAMIN WOLINSKY (CABN 305410)
Assistant United States Attorneys
7
450 Golden Gate Avenue, Box 36055
8 San Francisco, California 94102-3495
Telephone: (415) 436-7200
9 Facsimile: (415) 436-6748
shiwon.choe@usdoj.gov
10 benjamin.wolinsky@usdoj.gov

11 JAMIE ANN YAVELBERG
PATRICIA L. HANOWER
12 ARTHUR S. DI DIO
GARY R. DYAL
13 LAURIE A. OBEREMBT
United States Department of Justice
14 Civil Division
Commercial Litigation Branch
15
Attorneys for the United States of America
16

17 UNITED STATES DISTRICT COURT

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Friday, July 30, 2021

Government Intervenes in False Claims Act Lawsuits Against Kaiser Permanente Affiliates for Submitting Inaccurate Diagnosis Codes to the Medicare Advantage Program

The United States has intervened in six complaints alleging that members of the Kaiser Permanente consortium violated the False Claims Act by submitting inaccurate diagnosis codes for its Medicare Advantage Plan enrollees in order to receive higher reimbursements.

The Kaiser Permanente consortium members (collectively Kaiser) are Kaiser Foundation Health Plan Inc., Kaiser Foundation Health Plan of Colorado, The Permanente Medical Group Inc., Southern California Permanente Medical Group Inc. and Colorado Permanente Medical Group P.C. Kaiser is headquartered in Oakland, California.

"Medicare's managed care program relies on the accuracy of information submitted by health care providers and plans to

Certain Enforcement Actions: Medicare Advantage

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA EX REL.TERESA ROSS, Plaintiff, v. INDEPENDENT HEALTH ASSOCIATION, INDEPENDENT HEALTH CORPORATION, DxID LLC, & BETSY GAFFNEY, Defendants.	CASE NO. 12-CV-0299(S)

UNITED STATES' COMPLAINT IN INTERVENTION

The United States of America ("United States" or "Government") brings this action against Defendants Independent Health Association ("IHA") and Independent Health Corporation ("IHC") (collectively "IH"), DxID LLC ("DxID"), and Betsy Gaffney ("Gaffney") (collectively, "Defendants"), to recover treble damages and civil penalties for their violations of the False Claims Act ("FCA"), 31 U.S.C. §§ 3729–3733, and damages and

2. Specifically, Defendants (1) knowingly submitted or caused to be submitted thousands of unsupported diagnosis codes to CMS, (2) knowingly used or caused to be used false records or statements to submit the unsupported diagnosis codes, (3) knowingly retained overpayments resulting from the submission of these unsupported diagnosis codes, and (4) conspired with the other defendants to violate the FCA from no later than January 1, 2011 through at least January 31, 2017.

3. Defendant IH is a MA Organization ("MAO") that contracted with CMS to provide MA health plans to beneficiaries enrolled in Medicare Part C in New York State. Generally, under the MA Program, CMS pays insurers, like IH, on a per member per month ("PMPM") or capitated basis. CMS calculates and increases payments to insurers, like IH, pursuant to a risk adjustment system, in which payment increases are based, in part, on the health status of the plan's members. Thus, CMS pays more for sicker members and for members who have conditions that are costlier to manage than for healthier members. Therefore, the submission of diagnosis codes directly affects the amount of payments to MAOs like IH.

Board of Directors

Role & Responsibilities

A Board's Role and Responsibilities

The Board has 3 broad duties:

- The Duty of Care
- The Duty of Loyalty
- The Duty of Obedience to Purpose

Caremark:

"a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and . . . failure to do so under some circumstances may . . . render a director liable for losses caused by non-compliance with applicable legal standards."

A Board's Role and Responsibilities

"But is important that the board exercise a good faith judgement that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility."

"And obviously too, no rationally designed information and reporting system will remove the possibility that the corporation will violate laws or regulations or that senior officers or directors may nevertheless sometimes be misled or otherwise fail reasonably to detect acts material to the corporation's compliance with the law."

A Board’s Role and Responsibilities

Director shall perform his or her duties, including duties as a member of any committee of the board upon which the director may serve:

- In good faith;
- In a manner that is in the best interest of the corporation;
- Based on information sought and provided to his or her; and
- With such care, including reasonable inquiry, as an ordinarily prudent person in a like position would use under similar circumstances

A Board's Role and Responsibilities

Marchand:

"... the board had no committee overseeing food safety, no full board-level process to address food safety issues, and no protocol by which the board was expected to be advised of food safety reports and developments. Consistent with this dearth of any board-level effort at monitoring, the complaint pleads particular facts supporting an inference that during a crucial period when yellow and red flags about food safety were presented to management, there was no equivalent reporting to the board and the board was not presented with any material information about food safety."

A Board's Role and Responsibilities

Boeing:

"A 737 MAX airplane manufactured by The Boeing Company…crashed in October 2018, killing everyone onboard; a second one crashed in March 2019, to the same result. Those tragedies have led to numerous investigations and proceedings in multiple regulatory and judicial arenas to find out what went wrong and who is responsible. Those investigations have revealed that the 737 MAX tended to pitch up due to its engine placement; that a new software program designed to adjust the plane downward depended on a single faulty sensor and therefore activated too readily; and that the software program was insufficiently explained to pilots and regulators. In both crashes, the software directed the plane down. The primary victims of the crashes are, of course, the deceased, their families, and their loved ones. While it may seem callous in the face of their losses, corporate law recognizes another set of victims: Boeing as an enterprise, and its stockholders."

A Board's Role and Responsibilities

Corporate Integrity Agreements

"Board Compliance Obligations. The Board of Provider shall be responsible for the review and oversight of matters related to compliance with Federal health care program requirements and the obligations of this CIA. The Board must include independent (i.e., non-employee and non-executive) members. The Board shall, at a minimum, be responsible for the following: a. meeting at least quarterly to review and oversee Provider's compliance program, including but not limited to the performance of the Compliance Officer and Compliance Committee; b. submitting to the OIG a description of the documents and other materials it reviewed, as well as any additional steps taken, such as the engagement of an independent advisor or other third party resources, in its oversight of the compliance program and in support of making the resolution below during each Reporting Period;…"

Any Questions/Thoughts/Comments

Lynn Barrett, Esq., CCP, CHC
lynn@blhealthlaw.com

Comments encouraged!