GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(RESEARCH ARTICLE)

Check for updates

Pandemic profiteering at a time of crisis: Using python to detect fraud in covid-19 testing and treatment payments

Isaac Asamoah Amponsah *

Public Administration, School of Public Management and Policy, University of Illinois Springfield, United States of America.

GSC Advanced Research and Reviews, 2024, 19(02), 208–218

Publication history: Received on 10 April 2024; revised on 18 May 2024; accepted on 20 May 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.19.2.0183

Abstract

During the pandemic, the Centre for Medicare and Medicaid Services (CMS) introduced blanket waivers and rule flexibilities to address rising COVID-19 cases. This included expanding telehealth services to urban areas and waiving certain reporting requirements, along with various testing options such as surveillance testing, school and workplace testing, self-tests, and testing in more inpatient settings such as nursing homes. The federal and state governments also covered COVID-19 testing, vaccination and treatment for the uninsured population, creating opportunities for fraud and unnecessary testing, double billing, kickbacks, and deceased billing, mainly for monetary gain, by unscrupulous healthcare providers. Using Python programming, the study adopted an unsupervised learning approach by employing Isolation Forest to detect healthcare providers who were anomalies in the payment for COVID-19, treatment and vaccination by the Health Resources and Services Administration (HRSA). Additionally, using official search enquiry into official U.S. government websites such as the FBI, USDOJ, and HHS-OIG, this study identified eight (8) fraud, waste and abuse schemes related to laboratory testing and treatment. The isolation forest algorithm, set at a 5% contamination level, identified 1,890 healthcare providers (7.64% of total claims) as being anomalies. These results support the recommendations given to the HRSA by the Office of Inspector General of the Department of Health and Human Services (HHS-OIG), emphasizing the need for identifying and addressing improper payments. Protecting public health resources requires preventing fraud in the healthcare industry. Strong education programs for healthcare workers are crucial, as are vigilant oversight and collaboration between federal and state agencies. Additionally, this study emphasizes how crucial it is to use official government resources—such as the FBI, HHS-OIG, USDOJ, and CDC—to efficiently detect and prevent fraudulent activities. In the wake of information asymmetry, calls for private–public partnerships are needed to address fraud, waste and abuse in the healthcare industry.

Keywords: Medical Information; Anomaly Detection; COVID-19 Testing; Fraud; Waste and Abuse; Healthcare Fraud.

1. Introduction

When lives were in jeopardy due to a global crisis, some people seemingly saw opportunity, while others saw despair. Through pandemic profiteering, whereby laboratories capitalized on sorrow for their own benefit, potentially billing for the spirits of the afflicted and nonexistent people, my research uncovers a potentially unsettling reality. Coronavirus disease 2019 (COVID-19) was named by the World Health Organization (WHO) on February 11, 2020, because of the illness caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) infection. Compared to other countries in the world, the United States reported the most COVID-19 cases and fatalities in 2020 (WHO, 2020). During the course of the year, there were three pandemic waves: (1) a spring outbreak in a small number of primarily urban areas following the introduction of the virus; (2) a summer wave that primarily affected the southern half of the country; and (3) an autumn–winter wave that persisted until the spring of 2021 (El-Shabasy et al., 2022). On January 20, the same day South Korea reported its first COVID-19 case, Washington state confirmed the first case in the U.S. through a serological test (Holshue et al., 2020). Twelve weeks later, on April 11, the U.S. surpassed Italy in reported COVID-19

* Corresponding author: Isaac Asamoah Amponsah.

deaths, reaching approximately 24,000, while South Korea had 10,450 deaths (Bergquist et al., 2020). By August 9, 2020, the global total number of COVID-19 cases had reached 5.04 million, with 162,919 deaths.

As of the CMS publication dated December 15, 2021, health expenditures experienced the greatest growth rate since 2002, owing to the impact of the COVID-19 pandemic. According to the same publication, federal spending on public health ($114.9 billion), which included funding for COVID-19 testing, vaccine development, and health facility preparedness; financial assistance to providers to compensate for lost revenue through the Provider Relief Fund ($122 billion in 2020); and the Paycheck Protection Program ($53 billion in 2020), were the main drivers of the rapid increase in health care spending in response to the pandemic. Consequently, in 2020, the federal government's growth in health care spending grew by 36.0% (CMS, 2021).

In response to the increasing COVID-19 cases and death tolls, the Centers for Medicare & Medicaid Services (CMS) issued numerous blanket waivers and flexible rules during the Public Health Emergency. During national emergencies, CMS can provide blanket waivers under Sections 1135 or 1812(f) of the Social Security Act to help beneficiaries access care. When such a waiver is issued, providers do not need to apply for a separate 1135 waiver (CMS, 2022). These waivers included extending telehealth services to both rural and urban areas, eliminating verbal order requirements (42 CFR §482.23, §482.24, and §485.635(d)(3)), and easing intensive care unit reporting obligations (42 CFR §482.13(g)(1)(i)-(ii)). CMS also waived the mandate for hospitals to furnish advance directive policy information, simplifying care delivery. Additionally, parts of 42 CFR 483.10 were waived to facilitate the segregation of nursing home residents by COVID-19 status, overriding usual regulations concerning room preferences, notifications, and transfer refusals. Specifically, CMS allowed healthcare providers to offer telehealth services across state lines, reimbursed telehealth visits at the same rate as in-person visits and expanded the types of services covered under telehealth to include emergency department visits, initial nursing facility and discharge visits, and home visits (CMS, 2020a). Other waivers included the three-day hospital stay requirement before transferring to a skilled nursing facility, relaxing supervision requirements for certain services, and allowing hospitals to provide services in non-traditional settings such as temporary expansion sites (CMS, 2020b; AAMC, 2020). While essential for maintaining healthcare access, these changes also increased the potential for fraud, waste, and abuse. For instance, the expanded telehealth coverage and reimbursement could lead to overbilling or billing for non-existent services. Similarly, relaxing supervision and location requirements might result in inadequate oversight and improper billing for services provided in non-compliant settings (Covington & Burling LLP, 2023). CMS also introduced flexibilities for COVID-19 testing, including surveillance testing in schools and workplaces, self-tests, drive-through testing, community-based testing, and testing in nursing homes. The lack of oversight for SARS-CoV-2 surveillance testing using pooled sampling protocols, which did not require facilities to be CLIA-certified, allowed for potential fraud. Government insurance programs like Medicaid and Medicare often covered these COVID-19 tests, leading to schemes involving unnecessary tests such as billing for respiratory pathogen tests and genetic tests in addition to COVID-19 tests (USDOJ, 2022). These additional tests usually had little or no impact on confirming the presence of COVID-19 antibodies.

Federal and state officials, such as the Federal Bureau of Investigations (FBI), issued public alerts about coronavirus testing frauds that preyed on the country's overburdened testing infrastructure and left Americans with false test results, erroneous medical bills, and expensive at-home tests (FBI, 2020; HHS-OIG, 2023; USDOJ, 2023). The FBI and HHS-OIG collaborated in investigating a case involving fraudulent billing practices targeting the HRSA Uninsured Program by a provider group allegedly involved in a $36 million health care fraud scheme (USDOJ, 2024). It's important to note that an indictment merely represents allegations, and all providers are presumed innocent until proven guilty in a court of law. According to a HHS-OIG report, HRSA improperly made payments to providers under the COVID-19 Uninsured Program (UIP) for individuals who had health insurance coverage and for services unrelated to COVID-19. The OIG audit found that HRSA disbursed nearly $784 million in improper payments out of $4.2 billion, affecting approximately 3.7 million patients out of 19.2 million. The OIG recommended that HRSA recover $294,294 identified in the audit and conduct further reviews to recover additional improper payments. Furthermore, the OIG advised HRSA to enhance verification processes and ensure the reliability of data sources for future similar programs (HHS-OIG, 2023).

1.1. Fraud schemes in covid-19 testing.

An official search of the U.S. Government website revealed a number of fraudulent cases related to COVID-19 testing and treatment. This deep search included federal agency websites such as the Department of Healthcare and Human Services – Office of Inspector General (HHS-OIG), the Federal Bureau of Investigations (FBI), the United States Department of Justice (USDOJ), the Centers for Medicare and Medicaid Services (CMS), the Food and Drugs Authority (FDA) and the Centers for Disease Control (CDC).

42 U.S.C. § 1320a-7b(b) contains the Anti-Kickback Statute (AKS), a criminal statute that forbids the exchange of "remuneration" to influence patient referrals or business development under Federal healthcare programs. This encompasses a variety of noncash types of compensation as well as Medicare and Medicaid services. Both parties are subject to the AKS when giving or receiving kickbacks, and a key factor in assessing responsibility is intent. Rewarding people who recommend businesses is appropriate in certain sectors. However, it is illegal to pay for referrals under Federal Health Care Programs (HHS-OIG, 2024). Kickback and collusion schemes in the laboratory and COVID-19 testing and treatment might involve two or more labs or providers having large numbers of shared members or seeing the same members on the same date of service for the same procedure codes. Collusion schemes are common among laboratories that share the same or a close geographic location. If 50% of Lab A's members are also seen by Lab B, there could be a possibility of kickback or collusion between these two labs that might warrant further investigation, such as requesting and reviewing medical records. Kickbacks or collusions might also violate physician self-referral, often known as stark law (Social Security Act 42 U.S.C 1395nn). Kickbacks in COVID-19 testing can also arise between healthcare professionals and individuals. In an enforcement action against a Mercer County man and his conspirators, the United States attorney Philip R. Sellinger stated that "clinical laboratories and health care professionals are on notice: paying kickbacks to steer tests to a lab may break the law" (USDOJ, 2023). The conspirators demanded payments in return for supplying COVID-19 test samples to MetPath Laboratories, a clinical laboratory in Parsippany, New Jersey. MetPath paid bribes for COVID-19 test sample referrals, which were subsequently billed to Medicare and other health care benefit programs.

Billing for services not rendered, including stealing social security and phantom billing of state insurance programs, is another fraudulent scheme. Providers sometimes use social media platforms, fake websites, or click baits to entice members to sign up for services they end up not receiving. The providers then use these social security numbers to bill Medicare, Medicaid, and private insurance for services they did not render. A public alert on potential identity theft to charge Medicare and Medicaid for services not rendered was issued by HHS-OIG throughout the pandemic. These con artists put beneficiaries at risk of harm by using COVID-19-related needs and services for their own financial gain. Medical identity theft and fraudulent billing of federal health care programs are two possible uses for gathering personal information (HHS-OIG, 2023). Al-Qahtani and Cresci (2022) coined the term "scamdemic" to describe the surge in cyber-attacks, amidst increasing covid-19 cases, during the global pandemic, which was exacerbated mainly by the widespread shift to remote work. Bad actors employed phishing, vishing, smishing, and pharming schemes—where pharming redirects users from legitimate websites including social media pages, to fraudulent ones—to steal personal information and fraudulently bill Medicare and Medicaid for fictitious COVID-19 tests. Vishing, or voice phishing, uses telephony, robocalls, and voice over IP, while phishing typically exploits emails and websites, and smishing targets victims through SMS text messages. An Atlanta based provider was sentenced to 27 years in prison for orchestrating a $463 million Medicare fraud scheme through LabSolutions LLC, involving fraudulent genetic tests procured via kickbacks and bribes from patient brokers and telemedicine companies, in violation of Medicare regulations and anti-kickback statutes (USDOJ, 2023). This provider's actions exemplify the intersection of modern fraud tactics like phishing (via telemarketing calls), vishing (utilizing telemedicine companies), and smishing (through deceptive marketing to Medicare beneficiaries), highlighting the sophistication and harm of such schemes. Instances of billing for services not rendered can manifest when two labs or providers submit claims for the same patients on the same service date, using the same procedure codes. In such cases, while one provider may have rendered the service, the other may have fraudulently billed Medicare and Medicaid without providing the service. Moreover, billing for services not rendered can extend to situations where a lab or provider performs a COVID-19 test, but the patient never receives the results. Anomalies such as sudden surges or spikes in claims volume within a short timeframe or an unusually high number of tests performed in a single day may also be indicative of instances of billing for services that were never actually provided.

Upcoding is one of the most common fraud schemes. Upcoding in COVID-19 testing and treatment involves billing for a higher CPT code than the code actually performed. Examples of upcoding in COVID-19 testing schemes include billing for the add-on high-throughput technology codes and performing the test with simple technology. On October 15, 2020, the CMS announced that effective January 1, 2021, Medicare would be paying $100 for laboratories that perform COVID-19 tests using high-throughput technology and provide COVID-19 test results within two calendar days (CMS, 2021). For providers who continue to perform COVID-19 tests using simple laboratory technology and providers who produce COVID-19 results in more than two calendar days, Medicare will be paying only $75. The rationale for this policy modification was to increase the accuracy of the COVID-19 results and to expedite the COVID-19 test results. The add-on COVID test code was U0005 when performed via high throughput within two calendar days. If a lab performs a COVID-19 test with simple technology or produces results in more than two calendar days and bills Medicare using the U0005 add-on code, the provider or lab has upcoded her services. The correct procedure billing code is U0003 for 75$. Adding the U0005 code means that the lab or provider has charged an extra 25$ for using high-throughput technology within 2 calendar days for a service for which he used simple technology. Labs or providers also billing in-lab codes for

COVID self-tests or over-the-counter tests also represent upcoding. Between April 4, 2022, and May 11, 2023, Medicare Part b paid for over-the-counter tests.

Excessive COVID-19 testing is usually linked to the overutilization of COVID-19 tests, such as billing a member for more than 10 COVID-19 tests in a week. Unusual spikes and increases in Covid test billing can also represent services not rendered in some circumstances. The detection of excessive COVID-19 can be usually done through outlier detection in comparison to that of peers. Repetitive testing of the same members can also represent excessive COVID-19 testing. If a laboratory performs an antigen test and then a PCR test on the same member on multiple occasions, this could also represent excessive COVID-19 testing mainly targeted at state insurance programs for more money. Excessive testing is usually observed during mass testing in community-based programs, testing in nursing homes and schools, and workplace testing. The frequency of carrying out these tests is usually excessive. An inappropriate number of services provided to recipients is one way to detect excessive COVID-19. For example, if a provider bill 50 COVID tests for 2 members in a week, the service-to-recipient ratio will be 25 (50/2). Twenty-five tests in a week for a member might indicate excessive testing. Provider peer comparisons are also a useful way of detecting excessive tests billed by a laboratory in relation to other laboratories.

Duplicate billing can be evidenced when a visit is billed more than once. For example, billing an office visit and a telehealth visit for the same member on the same date of service. Duplicate billing in COVID-19 testing can occur when a lab bills two separate COVID-19 testing codes for the same tests and for the same member and date of service. When a lab or provider collects a single specimen and bills Medicare or Medicaid more than once using the specimen collection code G2023, this could be considered duplicate billing. When a laboratory performs an antigen test and charges more than once for the test, it could be indicative of susceptible duplicate billing. Duplicate billing is also evident when two providers bill the same members on the same date of service for the same procedure code or COVID-19 test. Shared members between two providers billing on the same date of service can also represent susceptive double billing. Billing of respiratory pathogen panel test (RPP) together with covid -19 tests could also be evidence of double billing, especially in instances where performing the RPP test has no significant outcome of the results of the covid-19 tests.

The Division of Clinical Laboratory Improvement and Quality within the Center for Medicate and Medicaid Services regulates the laboratory through the provision of a Clinical Laboratory Improvement Amendment (CLIA). CLIA ensures that laboratories are operating in accordance with acceptable quality standards (CMS, 2005). A laboratory registered with CMS as a certificate of waiver lab bills for a procedure code such as U0005 could be considered a violation against policy and a fraud, waste, or abuse scheme in COVID-19 testing because the U0005 code is a high-throughput code and not a simple technology code. Another FWA in COVID-19 testing related to CLIA is labs or providers with expired CLIA certification billing Medicare and Medicaid. A CLIA certification is good for 2 years and subject to renewal. The CMS maintains a website for checking the type and validity of a CLIA certificate just by entering the name of the lab or their CLIA number. During the public health emergency, the absence of oversight on surveillance pooled sampling for SARS-CoV-2 testing created vulnerabilities for potential fraud, waste, and abuse. Without CLIA certification requirements for facilities conducting this type of testing, there's limited control over result accuracy and reporting, leaving room for bad actors to exploit the system by submitting false claims for reimbursement through government insurance programs like Medicaid and Medicare. Additionally, the lack of oversight increases the risk of false negative or false positive results, further exacerbating the potential for misuse and fraudulent billing practices.

One rare scheme in COVID-19 testing is when providers bill the same member on the same date of service for administering different variants of COVID-19. Some of the COVID-19 vaccine brands approved by the FDA include Pfizer-BioNTech, Moderna, and Novavax (CDC, 2024). The CMS also provided additional guidance and payments for administering the COVID-19 vaccine in patients' homes. This leaves room for fraudulent waste and abuse where a lab bills for COVID-19 vaccine administration in patients' homes even though it was performed in the laboratory or during an office visit. When administering COVID-19 vaccines in Medicare patients' homes, providers use the HCPCS level II code M0201, receiving an additional $36 payment (CMS, 2023). Throughout the public health emergency, the Office of Inspector General, department Health and Human Services, continued to warn the public on avoiding purchasing or creating fake COVID-19 vaccination cards, as scams offering to sell them are prevalent. HHS-OIG admonished the public to only obtain valid proof of vaccination from legitimate providers, and be cautious of sharing personal, medical, or financial information to prevent fraud (HHS-OIG, 2023).

Postmortem billing basically involves billing COVID tests recipients who are dead. According to Rozen (2023), some unscrupulous fraudsters billed Medicare and Medicaid to send COVID-19 test kits to deceased people, which led the USDOJ to determine the breadth of this scheme. A way to catch this fraudulent scheme using data analytics might be to run the date of service when the COVID-19 test was performed against the date of death database. A case in which any COVID-19 test was performed after the date of death might indicate suspected billing. The Centers for Disease Control's

Coronavirus Disease Death Data and Reporting as well as the National Death Index might be useful databases. Post-mortem billing of COVID tests, particularly in self-tests, may occur due to the practice of pharmacies and laboratories routinely sending tests to recipients' homes on a weekly basis without verifying their vital status or address changes. While patients are typically responsible for ordering self-tests, if pharmacies operate on a recurring test delivery plan, tests might continue to be supplied even after the patient's demise. This lack of verification poses significant risks for erroneous billing and potential misuse of healthcare resources.

2. Methodology and data analysis

There are numerous data mining strategies available for detecting healthcare fraud, waste and abuse. Generally, unsupervised, supervised or combined methods have been used by experts to detect healthcare fraud. To identify outliers in healthcare fraud, Massi et al. (2020) employed an unsupervised clustering technique on administrative databases. To construct a health model that automatically identifies fraudulent cases from Saudi Arabian health insurance claims, Nabrawi & Alanazi (2023) employed supervised machine and deep learning analysis techniques such as random forest, logistic regression, and artificial neural networks to construct a predictive analytic model.

A review of the literature reveals that specific approaches employed to identify possible healthcare fraud include link analysis (using neural networks to detect interrelationships among two or more providers—to catch possible shared members and potential kickback schemes); rule-based audits (such as desk audits to identify providers who do not have the right certification type to perform a particular type of test but are paid for those tests); outlier detection (usually providers who receive higher reimbursement in relation to their peers or procedure code or an inappropriate number of services to recipients); predictive modeling; and time-dependent billing (such as providers billing improbable hours per day—more than 24 hours in a day for a time-dependent procedure code).

This study aimed to detect providers who might be outliers in claims reimbursement data paid to health facilities and providers by the Health Resources and Services Administration (HRSA) for COVID-19 testing, vaccine administration and COVID-19 treatment for the uninsured population between February 4, 2020, and March 2022. To achieve this anomaly detection method, this study employs an unsupervised learning method using isolation forest, first at a 5% contamination level and then at a 1% contamination level, to detect extreme outliers. Payment for claims reimbursement for the uninsured population was made by the HRSA through the Covid-19 Coverage Assistance Fund (CAF) and other funds such as the Provider Relief Fund. To be eligible for reimbursement, the provider must ensure that the patient or recipient has no Medicare, Medicaid, or any private insurance. The provider must also be willing to be paid the current Medicare fee – for – service rates (to avoid balance billing). To identify anomalies in the payment of COVID-19 testing, vaccination and treatment claims, the study uses anonymized identifiers such as Provider 1, Provider 2, Provider 3, etc., to maintain confidentiality and prevent any potential HIPAA violations. This approach ensures that the identities of the healthcare providers remain protected. The analysis focuses on the volume of claims paid, identifying outliers whose claimed volumes appear unusually high, potentially indicating the need for further review. It is important to note that detecting outliers does not automatically mean the perpetration of fraud. Identifying red flags means that claims payments to those providers need further investigation. Further investigations might include record reviews, interviewing recipients, procedural code analysis, and identifying interrelated or shared members among these providers (link analysis).

3. Data analysis

3.1. Description of the dataset and statistics

There are a total of 50,244 healthcare providers who received claim reimbursement from HRSA for providing COVID-19 testing, vaccination, and treatment to the uninsured population. Of these 50,244 providers, 24,792 are unique or distinct. The total number of claims paid over the period spanning from February 2020 to March 2022 is more than 18 billion (18,784,822,233) claims paid to these providers from 55 states. It is worth noting that some of these providers who were paid claims reimbursement were located outside of the United States, such as in Guyana.

The map chart below shows the city location and frequency of times providers were paid for providing COVID-19, COVID-19 and COVID-19 treatment for the uninsured population between February 2020 and March 2022. This map chart was constructed from the latitudinal and longitudinal information (geo-referenced information) provided in the claims data reimbursement data found on the Centers for Disease Control (CDC) website. From this map chart, providers located between San Antonio and Houston were paid 2339 frequency times between February 4, 2020, and March 2022, 2020, for providing COVID-19 testing, vaccination and treatment for the uninsured population.

Column Name	Description	Type
Provider Name	Provider name associated with the billing TIN to whom the payment was issued.	Plain Text
State		Plain Text
City		Plain Text
Claims Paid for Testing	Uninsured claims paid for Testing	Number
Claims Paid for Treatment	Uninsured claims paid for Treatment	Number
Claims Paid for Vaccine	Uninsured claims paid for Vaccine	Number
Georeferenced Column	Point derived from City and State	Point

Figure 1 Dataset Fields

Table 1 Summary Level Information from Dataset

Parameter	Statistic
Number of States	55
Total Paid Providers	50,244
Total Unique Paid Providers	24,792
Total Paid Claims for Covid Testing	11,362,068,129
Total Paid Claims for Covid Vaccines	1,617,170,645
Total Paid claims for Covid treatment	5,805,583,459
Total Paid Claims	18,784,822,233

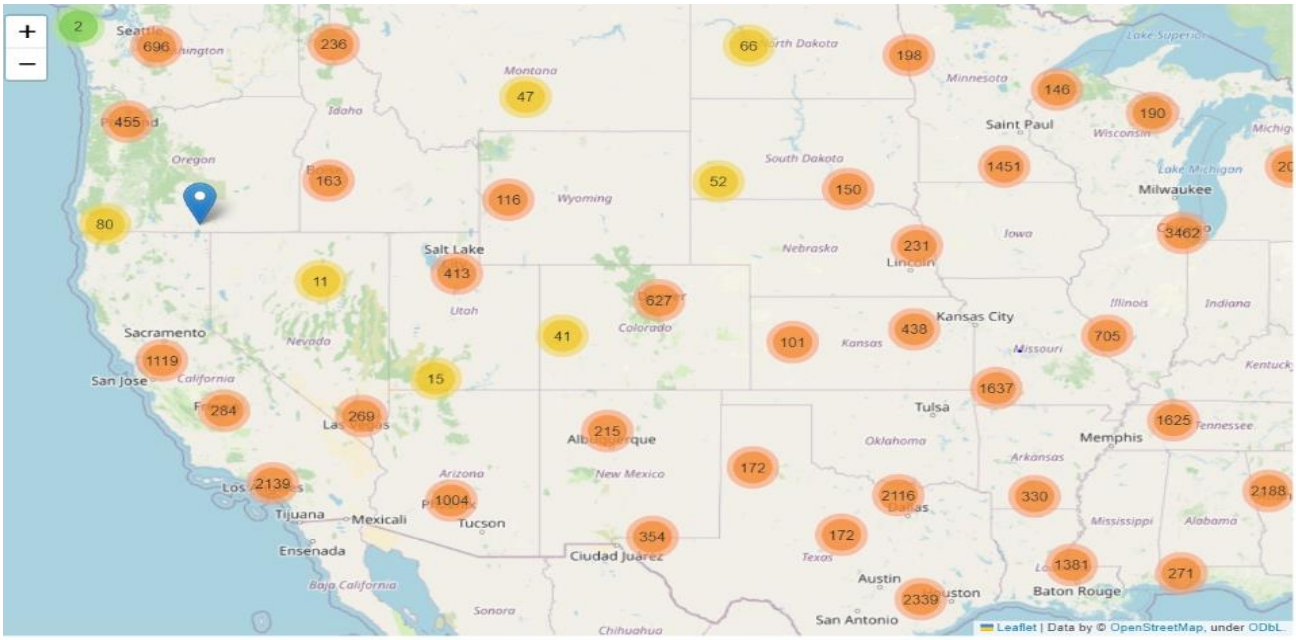


Figure 2 Frequency of Payments based on Provider City Located

Source: Centers for Disease Control and Prevention (CDC) - Claims Reimbursement to Health Care Providers and Facilities COVID-19 Data. Available at Link.

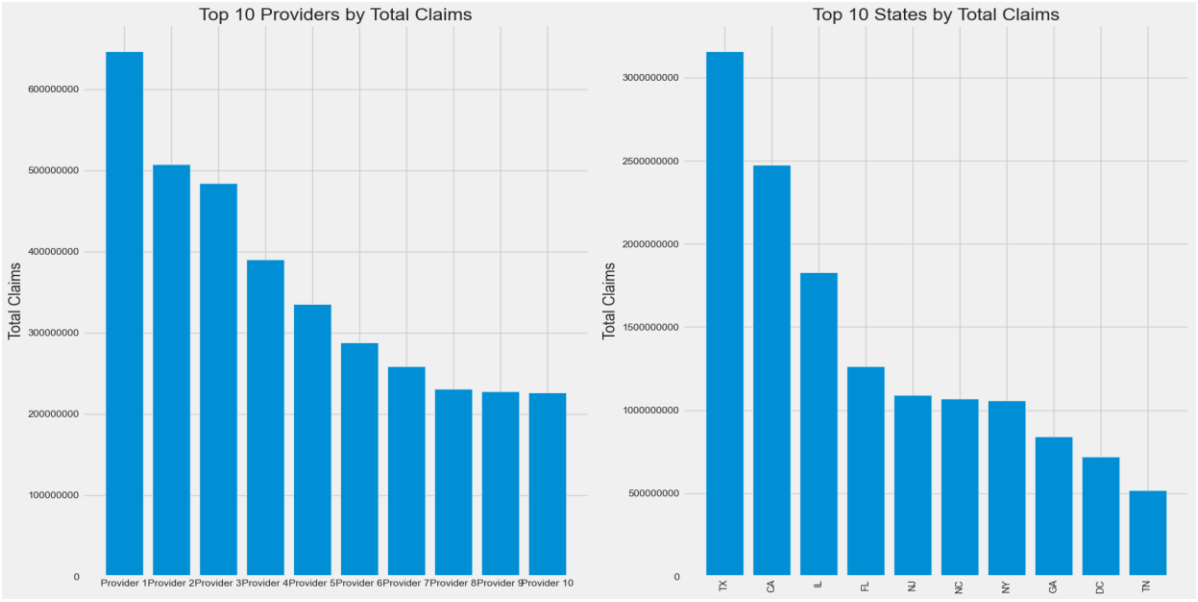


Figure 3 Top 10 Providers and States by Total Claims Paid

Table 2 TOP 10 Providers based on Total Claims Paid – Tabular Representation

Provider name	**Total claims paid**
Provider 1	646,140,450
Provider 2	507,386,938
Provider 3	484,273,848
Provider 4	390,459,241
Provider 5	334,978,320
Provider 6	288,067,592
Provider 7	258,721,942
Provider 8	230,669,547
Provider 9	227,691,475
Provider 10	226,616,685
Grand Total	3,595,006,038

Table 3 Top 10 States based on Total Claims Paid – Tabular Representation

State	Total claims paid
TX	3,155,980,164
CA	2,476,068,809
IL	1,828,846,889
FL	1,263,421,953
NJ	1,089,381,037
NC	1,068,332,131
NY	1,057,754,828

GA	842,556,358
DC	720,286,528
TN	518,850,701
Grand Total	14,021,479,398

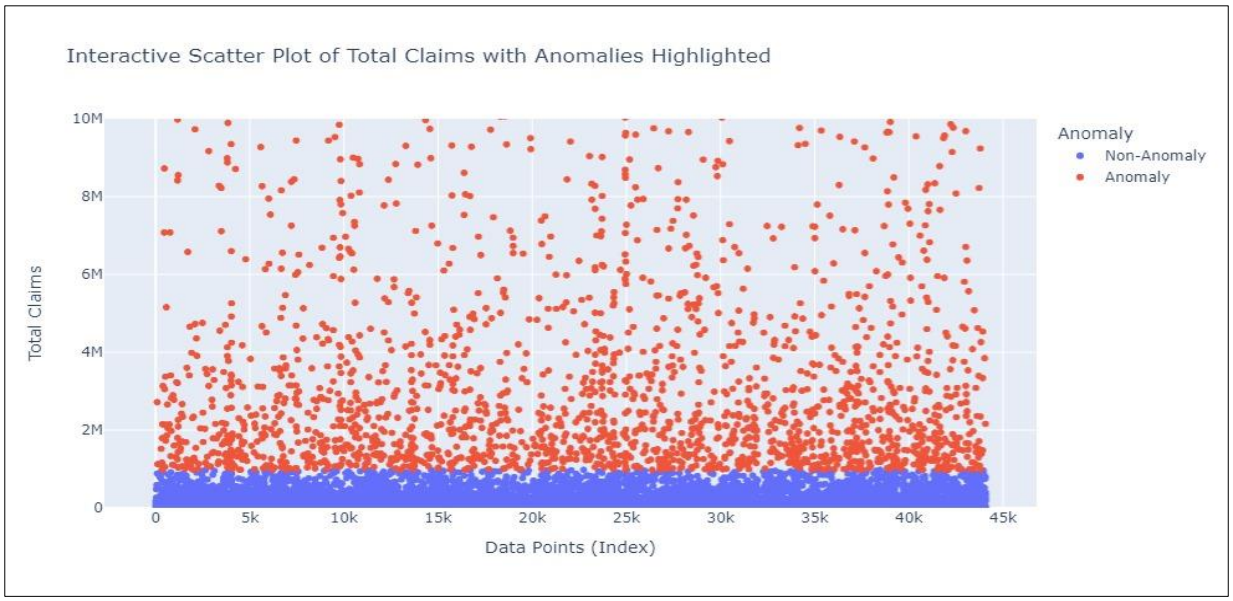
Source: Centers for Disease Control and Prevention (CDC) - Claims Reimbursement to Health Care Providers and Facilities COVID-19 Data. Available at Link.

The bar chart and tables above show the top 10 providers based on total claims paid by the HRSA for COVID-19, COVID-19 treatment, vaccination and treatment for the uninsured population. The top provider (Provider 1) was paid 646,140,450 claims over the period, followed by 507,386,938 in total claims for Provider 2. On a state level, providers located in Texas were the number 1 with the highest number of paid claims for COVID-19 testing, COVID-19 vaccination, and COVID-19 treatment for the uninsured population. Providers in TX were paid more than 3B claims (3,155,980,164), followed by those in California (2,476,068,809). Illinois follows with close to 2B claims (1,828,846,889).

3.2. Anomaly detection with isolation forest

The isolation forest (iForest) algorithm is a tree-based algorithm that isolates anomalies by randomly selecting a feature and a random split value. It creates a tree structure and measures how many splits are required to isolate a data point. Anomalies require fewer splits to be isolated, making them stand out. iForest is effective at identifying anomalies because it separates them from the majority of normal data points in fewer steps. In the context of total claims, iForest can identify providers with unusually high or low claims compared to the majority. Unusually high claims payments might signal that those services were not actually rendered and might need further review.

The objective of this analysis is to identify providers with unusually high claims reimbursement, which are considered anomalies in the context of COVID-19 claims. This study employs the isolation forest algorithm for this purpose. The providers flagged as having anomalies according to the isolation forest algorithm are candidates for further investigation. These providers may have received significantly higher or lower reimbursements than expected based on the total claims patterns of the majority.



Source: Centers for Disease Control and Prevention (CDC) - Claims Reimbursement to Health Care Providers and Facilities COVID-19 Data. Available at Link.

Figure 4 Anomaly Providers detected at 5% contamination level

4. Results and discussion

The isolation forest algorithm, with a contamination level of 5%, identified 1,890 healthcare providers, representing 7.64% of the total claims, as anomalies. Providers classified as having anomalies had an average total claim amount of

7,543,562.66. The highest anomaly claim amounted to 646,137,850.00. Among the anomalies, the highest claim was attributed to "Claims Paid for Testing," with an amount of 586,931,650.00.

4.1. Interpretation

The isolation forest algorithm identified a small percentage of providers (7.64%) as being anomalies. These provider anomalies exhibited a wide range of total claims paid, with some providers receiving exceptionally high reimbursements. Among the anomalies, claims paid for testing had the highest individual claim, contributing to the high total claims paid.

To further drill down the identified outliers associated with the 5% contamination, we reduced the contamination level from 5% to 1% and found a total of 350 providers out of the total unique providers of 24,792, as shown below.

Source: Centers for Disease Control and Prevention (CDC) - Claims Reimbursement to Health Care Providers and Facilities COVID-19 Data. Available at Link.

Figure 5 Anomaly Providers detected at a 1% contamination level.

5. Conclusion

Protecting public health resources and protecting the integrity of testing programs require the identification of various fraudulent schemes in COVID-19 testing. It is clear that bad actors may try to take advantage of the system for financial gain, whether through kickback and collusion schemes, upcoding, or postmortem billing. The detection and prevention of fraudulent operations depend heavily on vigilant oversight, education, and cooperation between federal and state agencies. Wholesale blanket waivers might provide an opportunity for perpetrators to milk the system in times of crisis.

Recommendation

Protecting the validity of COVID-19 testing requires the application of a complex strategy. This involves performing routine, in-depth audits of provider claims using cutting-edge analytics to identify anomalies and possible fraud. Furthermore, it is critical to establish thorough education programs for healthcare professionals, providing instruction on how to handle complex billing situations and guarantee compliance. Additionally, improving the detection and punishment of fraudulent providers is crucial for protecting public health resources and maintaining the integrity of healthcare programs such as the COVID-19 testing program. To do this, federal, state, and law enforcement agencies must work more closely together. To stop unauthorized testing, strict control measures must be implemented, including adherence to Clinical Laboratory Improvement Amendment (CLIA) standards. Regulations should be strictly enforced, including licensing and credentialing of providers, conducting background checks during provider enrollment, excluding bad actors from federal and state healthcare programs, and conducting on-site visits. Additionally, there should be regular reporting requirements and verification processes to ensure recipients actually receive the services

billed for. This verification could include sending explanation of benefits statements, making phone calls, and sending letters to patients.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. IET information security, 16(5), 324–345. https://doi.org/10.1049/ise2.12073

[2] Association of American Medical Colleges (2020). CMS issues additional waivers for flexibility during COVID. https://www.aamc.org/advocacy-policy/washington-highlights/cms-issues-additional-waivers-flexibility-during-covid

[3] Bergquist, S., Otten, T., & Sarich, N. (2020). COVID-19 pandemic in the United States. Health policy and technology, 9(4), 623-638.

[4] Centers for Disease Control and Prevention (2022). "Claims Reimbursement to Health Care Providers and Facilities for Testing, Treatment, and Vaccine Administration of the Uninsured | Data | Centers for Disease Control and Prevention." Data.cdc.gov, 3 Mar. 2022, data.cdc.gov/Administrative/Claims-Reimbursement-to-Health-Care-Providers-and-/rksx-33p3/about_data. Accessed 14 Jan. 2024.

[5] Centers for Disease Control and Prevention. "Overview of COVID-19 Vaccines." Centers for Disease Control and Prevention, 12 Jan. 2024, www.cdc.gov/coronavirus/2019-ncov/vaccines/different-vaccines/overview-COVID-19-vaccines.html. Accessed 23 May 2024.

[6] Centers for Medicare & Medicaid Services. (2005). [Types of CLIA Certificates]. Retrieved from TYPES OF CLIA CERTIFICATES (cms.gov)

[7] Centers for Medicare & Medicaid Services. (2022). *COVID-19 emergency declaration blanket waivers for health care providers*. https://www.cms.gov/files/document/covid-19-emergency-declaration-waivers.pdf. Accessed 23 May 2024.

[8] Centers for Medicare and Medicaid Services (2020a). COVID-19 frequently asked questions (FAQs) on Medicare fee-for-service (FFS) billing. https://www.cms.gov/files/document/03092020-covid-19-faqs-508.pdf

[9] Centers for Medicare and Medicaid Services (2020b). Physicians and other clinicians: CMS flexibilities to fight COVID-19. https://www.cms.gov/files/document/physicians-and-other-clinicians-cms-flexibilities-fight-covid-19.pdf

[10] Centers for Medicare and Medicaid Services (2023). "In-Home Vaccine Administration: Additional Payment." www.cms.gov/medicare/coverage/preventive-services/home-vaccine-administration-additional-payment. Accessed 23 May 2024.

[11] Centers for Medicare & Medicaid Services. (February, 2021). National Health Spending in 2020 Increases Due to Impact of COVID-19 Pandemic. Retrieved from National Health Spending in 2020 Increases due to Impact of COVID-19 Pandemic | CMS

[12] Centers for Medicare & Medicaid Services. (October, 2021). CMS Changes Medicare Payment to Support Faster COVID-19 Diagnostic Testing. Retrieved from https://www.cms.gov/newsroom/press-releases/cms-changes-medicare-payment-support-faster-covid-19-diagnostic-testing

[13] Covington & Burling LLP. (2023). CMS proposes changes to Medicare telehealth policies, including increased payment rates. https://www.cov.com/en/news-and-insights/insights/2023/07/cms-proposes-changes-to-medicare-telehealth-policies-including-increased-payment-rates.

[14] Department of Health and Human Services, Office of Inspector General. (February, 2023). Fraud Alert: COVID-19 Scams. Retrieved from https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-covid-19-scams/

[15] El-Shabasy, R. M., Nayel, M. A., Taher, M. M., Abdelmonem, R., & Shoueir, K. R. (2022). Three waves changes, new variant strains, and vaccination effect against COVID-19 pandemic. International Journal of Biological Macromolecules, 204, 161-168.

[16] Federal Bureau of Investigation. (June, 2022). FBI Warns of Potential Fraud in Antibody Testing for COVID-19. Retrieved from https://www.fbi.gov/news/press-releases/fbi-warns-of-potential-fraud-in-antibody-testing-for-covid-19

[17] Holshue, M. L., DeBolt, C., Lindquist, S., Lofy, K. H., Wiesman, J., Bruce, H., ... & Pillai, S. K. (2020). First case of 2019 novel coronavirus in the United States. *New England journal of medicine*, *382*(10), 929-936.

[18] Massi, M. C., Ieva, F., & Lettieri, E. (2020). Data mining application to healthcare fraud detection: a two-step unsupervised clustering method for outlier detection with administrative databases. BMC medical informatics and decision making, 20, 1-11.

[19] Nabrawi, E., & Alanazi, A. (2023). Fraud Detection in Healthcare Insurance Claims Using Machine Learning. Risks, 11(9), 160.

[20] Office of Public Affairs, United States Department of Justice. (2023, August 18). Lab owner sentenced for $463M genetic testing scheme [Press release]. Retrieved May 23, 2024, from https://www.justice.gov/opa/pr/lab-owner-sentenced-463m-genetic-testing-scheme

[21] Office of Public Affairs, United States Department of Justice (2024). " Laboratory Owners Charged in $36M COVID-19 Testing Fraud Scheme | United States Department of Justice." Www.justice.gov, www.justice.gov/opa/pr/laboratory-owners-charged-36m-covid-19-testing-fraud-scheme. Accessed 23 May 2024.

[22] Rozen, C. (2023, June 12). DOJ probing COVID test fraud including kits sent to dead people. Bloomberg Law. https://news.bloomberglaw.com/health-law-and-business/doj-probing-covid-test-fraud-including-kits-sent-to-dead-people

[23] U.S. Department of Health & Human Services, Office of Inspector General. (2024). Fraud & Abuse Laws. Retrieved from https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws/

[24] U.S. Department of Health and Human Services, Office of Inspector General. (2023, July). *HRSA made COVID-19 uninsured program payments to providers on behalf of individuals who had health insurance coverage and for services unrelated to COVID-19* (Report No. A-02-21-01013). https://oig.hhs.gov/oas/reports/region2/A022101013.asp

[25] U.S. Department of Health & Human Services, Office of Inspector General. (February,2023). Fraud Alert: COVID-19 Scams. Retrieved from https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-covid-19-scams/

[26] U.S. Department of Justice, U.S. Attorney's Office, District of New Jersey. (August, 2023). Mercer County Man Admits to Soliciting Kickbacks in COVID-19 Testing Kickback Conspiracy. Retrieved from https://www.justice.gov/usao-nj/pr/mercer-county-man-admits-soliciting-kickbacks-covid-19-testing-kickback-conspiracy

[27] U.S. Department of Justice. (February, 2023). Lab Billing Company Settles False Claims Act Allegations Relating to Unnecessary Respiratory Tests. Retrieved from Office of Public Affairs | Lab Billing Company Settles False Claims Act Allegations Relating to Unnecessary Respiratory Panels Run on Seniors Receiving COVID-19 Tests | United States Department of Justice

[28] U.S. Department of Justice. (January, 2022). Lab Owner Pleads Guilty in $69 Million Genetic Testing, COVID-19 Testing Fraud Scheme. Retrieved from https://www.justice.gov/opa/pr/lab-owner-pleads-guilty-69-million-genetic-testing-covid-19-testing-fraud-scheme

[29] U.S. Department of Justice. (2023). Justice Department Announces Nationwide Coordinated Law Enforcement Action to Combat COVID-19. Retrieved from Office of Public Affairs | Justice Department Announces Nationwide Coordinated Law Enforcement Action to Combat COVID-19 Health Care Fraud | United States Department of Justice

[30] World Health Organization. (2020). Naming the coronavirus disease (COVID-19) and the virus that causes it. World Health Organization. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it