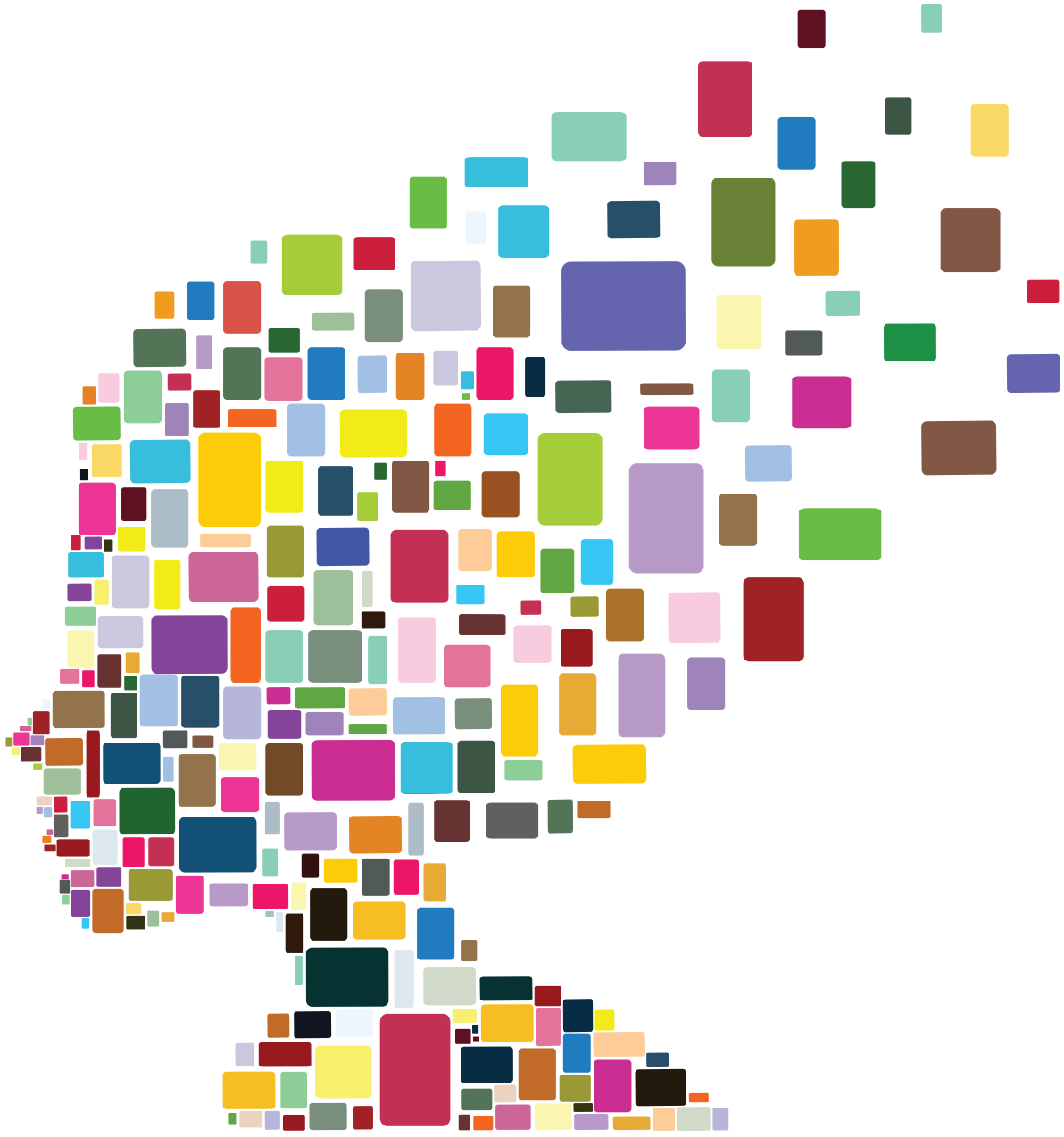
DATA INSIGHTS FOR BEST PRACTICE HEALTH CARE COMPLIANCE

UNDERSTANDING HOW DATA PROTECTS PATIENTS, YOUR ORGANIZATION, AND THE HEALTH CARE INDUSTRY



A VERISYS CORPORATION PUBLICATION

ABOUT VERISYS

Verisys Corporation wrote the book on health care data. Since 1992, Verisys has provided health care organizations with data and technology for best practice compliance.

Verisys' original and sustained mission is to provide a state-of-the-art, comprehensive technology platform of data, analytics, and services that deliver value to the full spectrum of stakeholders in the health care sector. Verisys' vision is to provide the tools that protect health care consumers by demanding competency and enforcing patient safety. This is the shared responsibility of all members of an organization and its affiliates. As stewards of provider data and credentials verification services, Verisys is dedicated to mitigating legal, financial, and regulatory risks for its clients and their end-users. Verisys prevents fraud, waste, and abuse in health care with accurate and timely data on persons, professionals, and businesses for contracting, privileging, employment, reimbursement, and referral validation. *Yes, we're the good guys.* The Verisys team handles millions of transactions annually across the health care sector including hospital systems, clinics, labs, pharmacies, pharmaceutical manufacturers, provider groups, dental practices, chiropractic practices, commercial and government payers, medical durable equipment and supplies manufacturers (DME), Medicaid enrollment, managed care organizations, medical malpractice carriers, background screening companies, and credentialing organizations. Verisys is one of only a few Credential Verification Organizations (CVO) both URAC Accredited and NCQA Certified (for 11 out of 11 verification services), as well as being current with ISO 9001:2015 and 27001 Certifications.

INTRODUCTION

HEALTH CARE COMPLIANCE AND BEYOND

When it comes to patient safety and quality outcomes, additional steps to assure complete provider and entity transparency not only prevent abuse to patients, but also keeps your organization and the entire health care system sustainable through the reduction of fraud, waste, and abuse.

Every organization lives by business rules that are designed to reduce risk by remaining in compliance with the regulatory requirements that govern health care. When in compliance with Federal and each state's regulations as well as standards of an organization in which you hold certification or accreditation, there is the feeling of wellbeing from checking all the boxes of compliance. However, to stay ahead of the curve of fraud schemes, patient abuse, as well as security risk, it behooves an organization to leverage an additional layer of data that may not be required by regulations and standards, but that will lend a deeper view and create a culture of complete transparency throughout an organization and its affiliates. History tells the story of regulations, acts, and laws that were created in an environment of desperation as a reaction to a situation that had gotten out of hand. Having to create a sustainable, effective, and longitudinal plan of risk prevention and mitigation of loss from a "Situation Room" standpoint does not always bring the big picture into play. Because of this historical trend, the fabric of the data point structure of regulatory compliance is a composite of reactions to catastrophic financial, national security, and public health events such as the Savings and Loan scandal, 9-11, the ongoing Opioid crisis and what will be the fallout of the current COVID-19 Pandemic. We herald prevention as the core of building and sustaining a healthy population. Yet we don't embrace prevention as a worthy concept for a sustainable health care system.

> *A true compliance program proves its value across the entire organization.*

THE CASE FOR A SOLID FOUNDATION OF DATA

Data points relative to credentialing and HR that sit in silos without assurance of a verified match of identity to a record can check off the compliance boxes required by the different departments, but does that practice truly execute on the desired spirit of compliance? Does that practice of compliance check off the risk box?

A true compliance program run by an empowered and unencumbered Compliance Officer creates an aggregated, verified 3-D picture of a provider, vendor, contractor, employee, partner, investor, and board member brings value across the entire organization.

The CFO may not want to delve into the many steps in the credentialing process, but a CFO will be very interested in how transparency across the entire array of engaged parties will save money through risk mitigation, freeing up resources by preventing the need for corporate integrity agreements, and driving better outcomes for a profit bump with greater ratios of reimbursement.

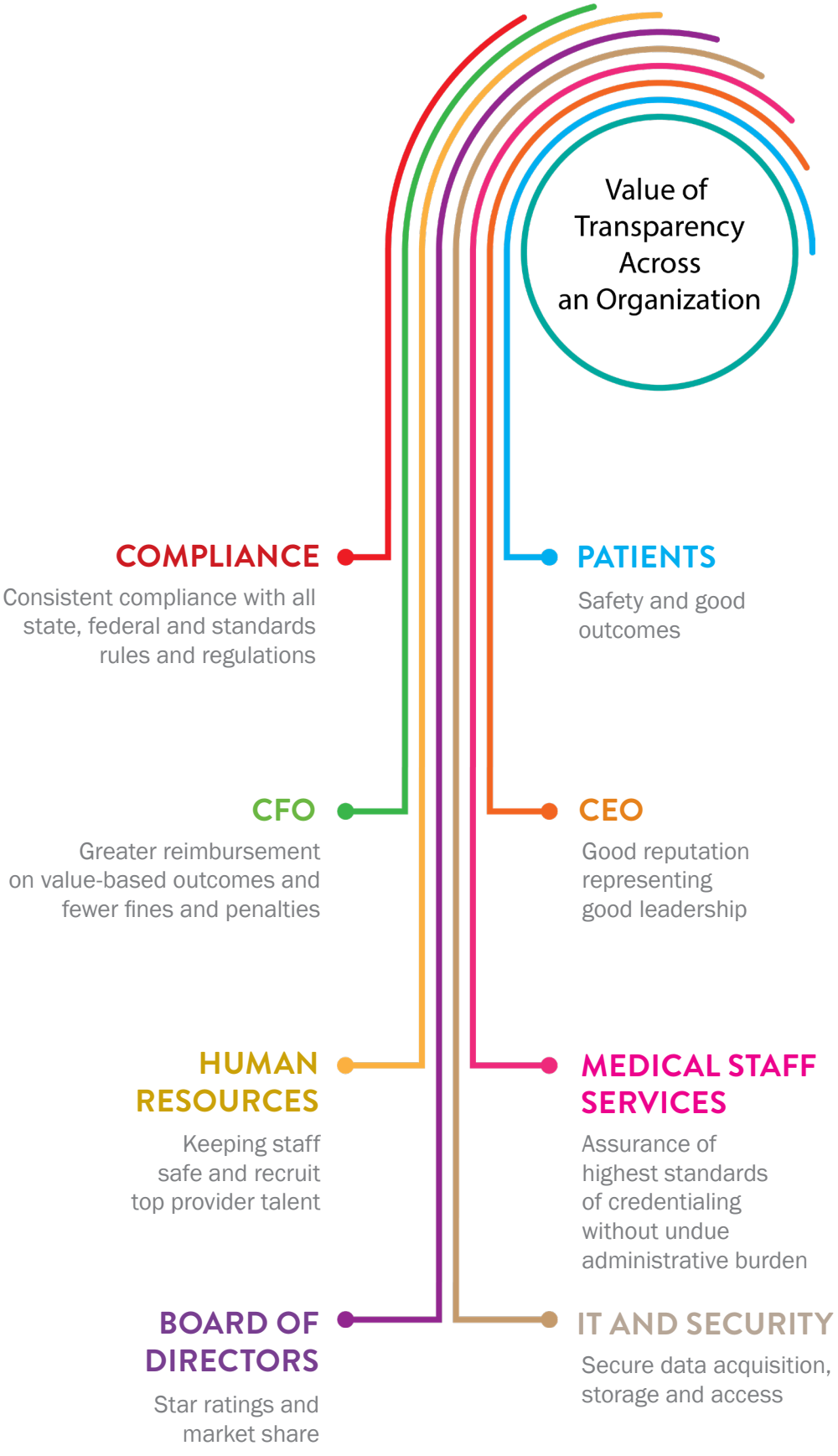
The Medical Staff Services Professionals may not have the view on the health care organization's financial operations, but this team will be interested in the efficiencies created with data automation and aggregation from a broad set of primary sources. So at the point of having credentialed a provider, their team can assure transparency that each credentialed provider is fully vetted, screened, verified and that continuous monitoring is attainable through the use of cloud-based digital automation.

Human Resource professionals want to assure that the entire workforce is safe from exposure to a co-worker, a provider, a vendor, or a board member who may have a background of violence, abuse, fraud, money laundering, or kickback schemes.

The IT and Security detail works tirelessly to sustain quality and security standards required by HIPAA, as well as inclusive to other regulatory and standard-setting frameworks. This team may have the least amount of influence regarding the choice of Credentialing Verification Organizations (CVOs) or data verification processes, yet they stand exposed to any violation of mandatory adherence.

The CEO and board members want their reputation and influence to be affiliated with a squeaky-clean organization. The C-Suite and Board don't necessarily engage in the nuts and bolts of compliance, screening, and organizational transparency, but their entire career path is at stake if short cuts are taken concerning security, compliance, workplace safety, and provider competence.

Understanding the value of each data set as well as the exponential value of aggregating and verifying data is critical to creating a culture of best practice compliance that plays the hand of a visionary, preventive trajectory, rather than operating from a frenetic, reactionary state.


Value of Transparency Across an Organization
COMPLIANCE
Consistent compliance with all state, federal and standards rules and regulations
CFO
Greater reimbursement on value-based outcomes and fewer fines and penalties
HUMAN RESOURCES
Keeping staff safe and recruit top provider talent
BOARD OF DIRECTORS
Star ratings and market share
PATIENTS
Safety and good outcomes
CEO
Good reputation representing good leadership
MEDICAL STAFF SERVICES
Assurance of highest standards of credentialing without undue administrative burden
IT AND SECURITY
Secure data acquisition, storage and access

OIG LEIE

Office of Inspector General's List of Excluded Individuals and Entities

When talking about data sets to check against, the first and most important database is the List of Excluded Individuals and Entities (LEIE) published by the U.S. Department of Health & Human Services (HHS) Office of Inspector General (OIG).

The LEIE is searchable online, updated monthly, and contains the current list of excluded individuals and entities. Health care organizations are required to check all new hires and contractors, as well as monitor regularly against the LEIE to assure there are no services or items provided by and/or reimbursed on behalf of an excluded individual or entity.

Plain and simple, if state or Federal reimbursement is sought on services provided by an excluded physician, other individual or entity, fines, and civil monetary penalties apply. Penalties can be up to $10,000 for each item of service provided during the period of exclusion, plus damages in the amount of three times the claim for each item or service. That can add up quickly and be followed by requirements stipulated in a Corporate Integrity Agreement.

Exclusion by the OIG from one entitlement program means exclusion from all HHS programs of which there are more than 100. Exclusions are either mandatory or permissive. It is mandatory for the OIG to exclude an individual or entity for committing felony crimes—Medicare or Medicaid fraud, or other felony offenses related to state or Federal health care programs; felony convictions related to controlled substances; or convictions for patient neglect or abuse. For permissive exclusions, the OIG has discretion on whether or not to exclude. The offenses related to permissive exclusions are on a misdemeanor level.

In many cases, it is not only providers who create cause for fines and penalties. Any employee of a health care organization or associate, affiliate, or vendor who provides items or services related to the care of an entitlement program beneficiary faces the same penalties as an excluded provider.

Examples of non-provider related fines and penalties in 2019:

A CHIROPRACTIC CLINIC ENTERED INTO A $10,000 SETTLEMENT AGREEMENT WITH OIG BECAUSE THE CLINIC HIRED A BILLING SPECIALIST WHO WAS EXCLUDED.

A $51,489.97 SETTLEMENT WAS ENTERED INTO BY A NURSING FACILITY BECAUSE IT EMPLOYED AN EXCLUDED INDIVIDUAL AS DIRECTOR OF INSERVICE EDUCATION.

A FAMILY PRACTICE ENTERED INTO A SETTLEMENT AGREEMENT OF $53,549.66 WITH THE OIG FOR HAVING HIRED AN EXCLUDED CODER.

AN ALZHEIMER'S CARE CENTER ENTERED INTO A $75,998.54 SETTLEMENT AGREEMENT FOR EMPLOYING A MEDICAL RECORDS COORDINATOR WHO WAS EXCLUDED.

A SKILLED NURSING FACILITY SETTLED FOR $171,047 ON BEHALF OF HIRING AN EXCLUDED INDIVIDUAL AS OFFICE MANAGER.

AN ASSISTED LIVING FACILITY SETTLED IN THE AMOUNT OF $96,020.92 FOR HIRING AN EXCLUDED INDIVIDUAL AS ADMISSIONS SPECIALIST.

THERE ARE MANY MORE MILLIONS IN PAYMENTS FOR SETTLEMENTS RELATED TO EXCLUDED PROVIDERS, BUT IT IS OFTEN OVERLOOKED TO CHECK EVERY EMPLOYEE AGAINST THE OIG LEIE.

SAM

General Services Administration's System For Award Management

While the Health and Human Services (HHS) Office of Inspector General (OIG) manages the List of Excluded Individuals and Entities (LEIE), The General Services Administration (GSA) administers the System for Award Management (SAM). Searching both data sets gives a broader view of the nature of an individual or entity in the screening and monitoring process.

THE DISTINCTION BETWEEN THE LEIE AND SAM:

The LEIE contains the identities of individuals and entities currently excluded by the OIG from participating in Federal health care programs.

SAM's list is inclusive of the OIG's LEIE and, additionally, contains debarment actions imposed by a broader list of federal agencies. SAM is designed as a consolidated list for federal procurement systems, and the Catalog of Federal Domestic Assistance that currently includes the Central Contractor Registry (CCR), Federal Agency Registration (Fedreg), Online Representations and Certifications Application (ORCA), and the Excluded Persons List System (EPLS).

SAM is the way a person or entity registers to do business with the Federal Government. U.S. registrants use a DUNS Number, Legal Business Name and Physical Address from the Dun & Bradstreet (D&B) record, the Taxpayer Identification Number (TIN), and Taxpayer Name associated with the TIN. A review of tax documents from the IRS, such as a 1099 or W-2 form is used to find the Taxpayer Name. Then bank routing information is used to set up the Electronic Funds Transfer (EFT). There is additional information needed for international registrants.

The SAM website is used to register to do business with the Federal Government as well as update, renew, and check your status. It is also where you search for registration, suspension, debarment, or exclusion status on an individual or entity. This is a free service to anyone.

Once registered, SAM has the authority to suspend or debar registrants to protect the Federal Government from fraud, waste, and abuse caused by contractors who act non-responsibly. Cases for suspensions and debarments are referred from a variety of sources, some voluntary and some mandatory.

Once suspended or debarred, the name is published on the SAM website and the effects of the suspension reach throughout the Executive Branch of the Federal Government for both procurement and non-procurement programs. Contracts shall not be awarded to a suspended or debarred individual or entity.

The causes for suspension or debarment are offenses that could be precursors to, or an actual felony offense warranting exclusion by the OIG. Screening and continuous monitoring against SAM provides an additional view for provider and entity transparency. As is true of all data collection and reporting systems, there are ways to avoid detection. Layering data points against a larger, more comprehensive, aggregated data platform is the best way to find those operating in the margins of exclusion, and those who are skillful in evading detection. Examples of violation of antitrust statutes are typically in the mergers and acquisitions category where there is a threat of reduced market competition. With health care spending constituting more than 17 percent of the gross domestic product, unbalanced market power can lead to price-fixing, group boycotts, bid-rigging, and other activities that benefit the institution at the cost of entitlement programs and the health care consumer.

U.S. FEDERAL AND STATES' ATTORNEYS GENERAL

Attorneys General sit at the top of legal activity and collect and publish data based on investigative and enforcement activity of many agencies.

The U.S. Attorney General (AG) is the chief law enforcement officer of the Federal government as the head of the Department of Justice (DOJ). The position is appointed by the President and sits within the Cabinet that also includes the Vice President and 15 of the President's top advisors.

The State Attorneys Generals are the primary legal officers for a respective state or territory advising and representing legislature and state agencies acting on behalf of the citizenry.

The DOJ is supervised by the U.S. Attorney General and oversees federal enforcement agencies such as the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Bureau of Prisons, the Office of Justice Programs, the U.S. Attorneys, and the U.S. Marshal's Service.

The data provided from the results of the investigative and enforcement activity of these agencies is a critical insight into those within the health care industry whether in a position of providing care directly to patients, or in proximity to patients via other services, and especially those in management or ownership of health organizations. It is an essential best practice to screen and monitor an entire organization's workforce to prevent and mitigate fraud and, especially, to assure patient safety and quality care.

Access to criminal data through this vast array of sources provides the first indicators of criminal activity. Information gathered from the respective AG's offices plays a critical role because in most cases, this data has not yet filtered down to the licensing boards, credentialing committees, or employers.

Only recently have some state AG agencies started to publish data electronically.

THE U.S. DEPARTMENT OF JUSTICE

The DOJ monitors, mitigates and prosecutes health plan fraud.

The U.S. Department of Justice (DOJ) was created by an act led by the Attorney General and passed by Congress in 1870 to handle federal law enforcement, criminal and civil prosecutions, and all the legal interests of the United States. It was tasked by Congress and President Bill Clinton in 1996 to combat fraud and abuse committed against all health plans, both public and private. This was done by the signing and implementation of the Health Insurance Portability and Accountability Act, HIPAA.

The goals of the program are to coordinate all levels of law enforcement to control health plan fraud; conduct investigations, audits, evaluations, and inspections with regard to health care delivery and payment; facilitate enforcement of all levels of health care statutes; provide industry guidance, alerts and safe harbors around fraud against health care; and, establish a national data bank of providers with adverse actions for centralized access. The program is funded by what is recovered from fraud investigations.

Health care fraud continues to be a growing problem across the United States with fraud schemes proliferating at a rate that is difficult to keep up with. New laws and government entities are continually created in a concerted effort to close the gap and pool resources to mitigate fraud, waste, and abuse in the health care system.

While there is no shortage of those who commit health care fraud, Federal efforts have resulted in substantial recoveries of funds. In Fiscal Year 2018, the DOJ recovered more than $2.8 billion, and in 2019 the DOJ recovered more than $3 billion in settlements and judgments from civil cases involving fraud and false claims against the government.

"The significant number of settlements and judgments obtained over the past year demonstrate the high priority this administration places on deterring fraud against the government and ensuring that citizens' tax dollars are well spent," said Jody Hunt, Assistant Attorney General of the DOJ's Civil Division.

Health systems and payers are vulnerable to fraud, waste, and abuse since the DOJ largely relies on whistle blowers to come forward with allegations against not only providers, but executive leadership, vendors, and all parties involved with the delivery of health care goods and services.

U.S. DEPARTMENT OF THE TREASURY

Health care fraud threatens U.S. economic stability.

The U.S. Department of the Treasury's primary function is to promote economic stability and prosperity as well as protect the financial security of the United States. Its purview reaches into the world economy both for reasons of financial opportunity as well as identifying national security and financial threats.

One of the data sets managed by the Treasury is the Office of Foreign Assets Control's (OFAC) list for Specially Designated Nationals And Blocked Persons (SDN). Anyone can search the SDN list to assure they are not doing business with a sanctioned person or entity and contributing to terrorism or money laundering.

The U.S. Treasury issues and enforces economic and trade sanctions according to U.S. national and foreign policy as an important part of sustaining our national security, and mitigating damage caused by terrorists, international drug traffickers, the proliferation of weapons of mass destruction, and other national threats.

The Treasury created the Financial Crimes Enforcement Network (FinCEN) that reports to the Under Secretary of the Office of Terrorism and Financial Intelligence in alignment with the Bank Secrecy Act (BSA). FinCEN coordinates with other law enforcement and task force entities to curb financial crimes across all industries such as mortgage loans, disaster recovery, and health care.

One of the initiatives focused on combating health care fraud was developing an advanced targeting process using analytics across local, state, and federal law enforcement. The Health Care Fraud Prevention and Enforcement Action Teams were the point agencies on behalf of the Treasury's Data.

FBI

Federal Bureau of Investigation

Health care spending reached more than $3.6 trillion in 2019 and accounted for 17.8 percent of the Gross Domestic Product (GDP) with a projected growth rate of 5.5 percent per year through 2027. Fraud, waste, and abuse divert some 10 percent of the total budget away from the care of patients, putting upwards of $360 billion in the hands of criminals. What is lost on health care fraud is more than half of the entire 2019 Department of Defense's discretionary budget of $686.1 billion.

With those kinds of numbers on the table, it is no wonder that the Federal Bureau of Investigation (FBI) considers health care fraud investigations a high priority. Through the Complex Financial Crime Program, the FBI has 56 field offices, and more than 350 satellite offices across the nation, with personnel dedicated to the investigation of health care fraud through coordinated initiatives, undercover operations, strike teams, and task forces. The Bureau lists its many priorities that include protecting the United States from terrorist attacks, foreign intelligence operations, espionage, cyberattack, public corruption, civil rights, violent crime, and major white-collar crime.

In its efforts to curb health care fraud, the Bureau partners with other Federal agencies along with various state Medicaid Fraud Control Units and other state and local agencies.

Through its involvement in the Healthcare Fraud Prevention Partnership (HFPP), a public-private fraud-fighting consortium made up of federal government, state agencies, law enforcement, private health insurance plans, and health care anti-fraud associations, the Bureau participates in data and information sharing.

In Fiscal Year 2018, FBI investigative efforts dismantled more than 207 health care schemes and disrupted more than 812 criminal operations by taking down criminal hierarchies and fraud organizations.

The U.S. Department of Justice published guidelines for screening persons working with vulnerable populations such as children, the elderly, and individuals with disabilities in need of support. While these guidelines were originally published in 1998, in the same time frame of the passing of the National Child Protection Act, and The Violent Crime and Law Enforcement Act, the relevance of protecting the vulnerable only increases in importance.

As patients in the health care system, everyone is vulnerable since it is a trust-based system, and patients rely on health care organizations to carefully screen and monitor not only providers, but executive leadership, vendors, and all parties that touch a patient throughout a lifetime of care.

DEA

The Drug Enforcement Administration

The DEA is the "Single Unified Command" on drug law enforcement. Checking against this important data set continues to rise in importance with one case in point—the current opioid crisis.

The DEA enforces the laws and regulations governing controlled substances and looks at organizations and involved individuals of organizations that grow, manufacture, or distribute controlled substances. It is also committed to supporting non-enforcement programs working to reduce the availability of controlled substances.

Health care providers must have a DEA number to prescribe controlled substances. From veterinarians to physicians, the DEA number, as a numerical identifier, is a way to track suspicious orders of controlled substances. A DEA number is not required by Federal law for non-controlled substance prescribing, yet some state laws require all licensed providers to register and obtain a DEA number in the event of reclassification, as well as for a secondary reason—ease in filing claims with insurance companies and order processing with pharmacies.

As with National Provider Identifier (NPI) numbers, the DEA number can be used to commit medical identity fraud in a variety of ways: 1) using a deceased provider's number, 2) illegally using the number of a provider, 3) illegally using the number of an entity as a prescribing physician, 4) applying for multiple numbers under assumed identities, or with aliases; and the list goes on.

As you can imagine, bad actors are counting on the fact that a simple name alteration will return "no results" on a name search, so using someone else's DEA or NPI number can fool those who rely on one database for identity and credentials verification.

Much like those who buy one ticket to a concert and then slip the same ticket to friends yet to gain entry, without a system that links one person to one ticket, fraud is relatively simple. When it comes to controlled substances and the way criminals have gamed the health care system, the DEA number is the hub of the wheel with the potential of greatly reducing the harm caused to patients by the perverse creation of addiction often resulting in overdose or death. The needless loss of life also comes with the loss of billions of dollars through improper reimbursements by Medicare and Medicaid diverting funds away from the very population that funded the system and are entitled to its benefits.

OFAC

Office of Foreign Assets Control

Adding OFAC screening and monitoring to a compliance program in the health care industry is important to the safety of patients through provider transparency, as well as preserving the integrity of reimbursements, and confirmation of the identities of all vendors and contractors of services, devices, and drugs.

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury issues and enforces economic and trade sanctions according to U.S. national and foreign policy. OFAC plays an important part in sustaining our national security by targeting and acting against terrorists, international drug traffickers, the proliferation of weapons of mass destruction, and other national threats.

OFAC publishes a searchable list of entities and individuals associated with hostile countries and regimes, as well as those engaged in, or associated with, actions that put the U.S. national security, foreign policy, or the economy at risk.

Anyone can search the list for Specially Designated Nationals And Blocked Persons (SDN), and two country-specific lists, the Consolidated Sanctions List combining seven lists, and the Other OFAC Sanctions Lists combining all lists plus two additional lists.

Blocking of assets and restricting trade and enterprise with those listed as sanctioned protects national security and the economy by preventing and mitigating money laundering and the funding and facilitation of terrorism. Every U.S. citizen, permanent resident aliens, foreign subsidiaries owned or controlled by U.S. individuals or entities must comply with OFAC regulations no matter where they are located. Fines for violation include civil monetary as well as criminal penalties and vary depending on the sanctions program. It is not unusual for combined fines to exceed several million dollars.

Understanding the use of aliases, and other techniques to verify that the search results are matched to the proper identity of the individual or entity when screening and monitoring against these lists, is a crucial element in data searches. Identity resolution when screening and monitoring is an essential part of compliance. When names are used in a siloed search without aggregating additional data points through algorithms, an error in identity either by having a no-results error or a mistaken positive result can be problematic.

HEAT

The Health Care Fraud Prevention and Enforcement Action Team is a valuable strike force created to combat health care fraud.

The Health Care Fraud Prevention and Enforcement Action Team, also known as the HEAT Strike Force, is a highly focused group of skilled investigators in collaboration with other federal, state, and local agencies specifically tasked with mitigating Medicare and Medicaid fraud. Two agencies responsible for investigating and prosecuting health care fraud, the Department of Health and Human Services (HHS) and the Department of Justice (DOJ) officially announced the creation of HEAT in 2009. The realization was that health care fraud against the Medicare and Medicaid programs was accelerating at such a pace that the solvency of the programs was being threatened. This threat puts millions of Medicare and Medicaid beneficiaries at risk of losing entitled benefits.

Preventing fraud has the most direct effect on maintaining and ensuring the integrity of the nation's largest health insurance program. The first Medicare Fraud Strike Force was created in 2007 in Miami-Dade County, FL as a collaboration and combination of resources including the DOJ's Criminal Division's Fraud Section, U.S. Attorney's Offices, HHS Office of Inspector General (OIG), along with state and local law enforcement agencies.

From that template, the makeup of today's HEAT Task Force includes agents from HHS-OIG and FBI, as well as Medicaid Fraud Control Units (MFCUs), local law enforcement, and oversight from the Office of the Medicaid Inspector General.

Strike Forces expanded with Los Angeles, CA in 2008; Detroit, MI, and Houston TX metro areas, plus Brooklyn, NY in 2009; Baton Rouge, LA, and Tampa, FL, in 2010; Chicago, IL, and Dallas, TX in 2011.

Other HEAT Strike Force locations formed since 2011 are Houston, TX; New Orleans, LA; Orlando, FL; Newark/Philadelphia; Washington, D.C.; and the Appalachian Region.

Those early years of deploying HEAT had a significant payoff. Between 2007 and 2011, the Fraud Strike Force operations charged 1,000 defendants in a collective amount of $2.3 billion in fraudulent billings. In 2010, an unprecedented $4 billion (up 56 percent, an increase of $1.4 billion over 2009) was returned to the Medicare Health Insurance Trust Fund, the U.S. Department of Treasury, and other Federal programs through targeting false claims and fraud committed against government health care programs.

Strike Force Statistics for 2019 as of May 31, 2019, are 2,208 criminal actions resulting in 2,829 indictments with investigative receivables of $3.48 billion. In April 2019.

HEAT and its supporting partners

successfully concluded what is coined, The Appalachian Regional Prescription Opioid Surge Takedown and was the largest prescription opioid enforcement operation in history. Over the past two years, more than 24,000 patients in the region received some 32 million pills from 350,000 illegal prescriptions of opioids and other dangerous narcotics by 60 individuals including 53 providers. Areas affected were West Virginia, Ohio, Kentucky, Alabama, and Tennessee.

Additionally, a DOJ press release mentions that from June 2018 to April 2019, the HHS excluded more than 2,000 individuals from participation in Medicare, Medicaid, and all other Federal health care programs. With all the work and effort by the OIG HHS to reach final exclusion status on providers, it is critical to check and continuously monitor against current and verified data since many fraudulent providers are skilled at schemes designed to hide an excluded status.

Prevention of fraudulent behavior averts a patient coming into contact with an abuser or being a victim of a fraud scheme. Prevention is done by screening and monitoring the health care workforce against data sources that reveal past fraud activity, abuse to patients, and current license status. Knowing this information in real-time stops reimbursement payments before they are even made.

Common Fraudulent Behavior:

BILLING FOR SERVICES NOT RENDERED

UPCODING, FRAGMENTING AND UNBUNDLING

BILLING FOR MEDICALLY UNNECESSARY SERVICES

RECEIVING AND/OR PAYING KICKBACKS EITHER FOR RECRUITING/ REFERRAL OF PATIENTS OR FOR SPECIALTY SERVICES, DURABLE OR EXPENDABLE EQUIPMENT, SUPPLEMENTS AND SALVES, ETC.

SIGNING ORDERS FOR UNNECESSARY LAB AND DIAGNOSTIC TESTS FROM INDEPENDENT DIAGNOSTIC AND TESTING FACILITIES

SIGNING ORDERS FOR UNNECESSARY PHYSICAL THERAPY AND OTHER THERAPIES, HOSPICE CARE, OR DRUGS FOR PATIENTS NEVER SEEN

BILLING FOR EQUIPMENT, DRUGS, SERVICES NOT PROVIDED, OR BILLING FOR HIGH-END ITEMS AND SUPPLYING LOW-END ITEMS

FALSIFYING MEDICAL RECORDS IN ORDER TO MISREPRESENT CONDITION AND DIAGNOSIS—AND THE LIST GOES ON

FEDERAL HEALTH CARE SOURCE

MEDICARE OPT-OUT LIST

The Health Care Fraud Prevention and Enforcement Action Team is a valuable strike force created to combat health care fraud.

When credentialing providers, it is important to check and monitor against the list of those providers who have opted out of Medicare. Health care providers can decide independently to opt-out of participation in Medicare which covers all Medicare programs including original fee-for-service Medicare, Medicare Managed Care Plans, Medicare+Choice Plan, and Medicare Advantage Plan. An opt-out covers all services, items, and locations.

Fines per incident, civil monetary penalties, plus restitution can be levied by the Federal Government if services provided by an opted-out provider are submitted to Medicare for reimbursement. The Centers for Medicare and Medicaid (CMS) publishes a list of providers who have opted out of Medicare according to the Medicare Access and CHIP Reauthorization Act (MACRA) of 2015 that requires in Section 106(a)(2) that the list of all providers with approved affidavits of opt out be available to the public.

Reasons for opting out can be that a provider no longer wants to serve Medicare beneficiaries, that the provider no longer wants to follow the fee-for-service charges mandated by Medicare and practices medicine on a cash basis, or that a type of specialty service is not covered by Medicare. There is a growing trend of providers opting out who feel fatigued from having to comply with the more than 11,000 regulations governing medical practice. Other reasons include wanting to become eligible to order, certify and prescribe, or that they prescribe Part D Prescriptions to Medicare beneficiaries.

Opting out is also used as a strategy to conceal and avoid an impending exclusion, sanction, debarment, or disciplinary action, and dodge being listed on the Health and Human Services (HHS) Office of Inspector General's (OIG) List of Excluded Individuals and Entities (LEIE).

The regulatory compliance checkpoints built into the Medicare programs that are designed to protect patients and mitigate fraud, waste, and abuse are no longer enforceable if the provider has opted out. Other efforts to conceal adverse behavior include changing license type and state of practice. The online searchable Affidavit opt-out list published on the CMS website is updated monthly and includes first and last name, NPI number, specialty, opt-out effective date, opt-out end date, address, and eligibility to order and refer.

With only this information, true identity matching can be tricky if a provider has changed his/her name, is using an alias, has multiple NPI numbers, has changed provider type, or changed his/her address. The Affidavit application contains the provider's social security number, date of birth, and license number, along with additional contact information that could be used to positively match an opt-out record to an individual with utmost certainty. However, without that protected information, there is room for error.

TRICARE

TRICARE is a Health Benefit of the Military Health System.

TRICARE is a benefit of the Military Health System (MHS). Those who are eligible to receive the benefits of TRICARE include uniformed service members and their families, National Guard/Reserve members and their families, survivors, former spouses, Medal of Honor recipients and their families, and others registered in the Defense Enrollment Eligibility Reporting System (DEERS). When a provider is excluded by the Health and Human Services (HHS) Office of Inspector General (OIG) and included on the List of Excluded Individuals and Entities (LEIE), that means exclusion from all Federal programs, including TRICARE. The list is readily available, and all programs are required to screen against the LEIE before submitting for reimbursement on products or services provided. However, sanctions, disciplinary actions, debarments, and exclusions originate in many different environments and are discovered and determined by myriad regulatory bodies. Reporting up, down, and laterally is yet another layer of administrative activity that has its delays, inaccuracies, and process. In line with a federal motto to be "a responsible steward of taxpayer dollars", and to deliver "integrated, affordable, and high-quality health service to all Department of Defense (DOD) beneficiaries", there is an ongoing effort to grant authority to all Federal agencies who administer benefits. Initially, TRICARE gained regulatory authority under 32 Code of Federal Regulations (CFR) 199.9 to sanction or exclude providers for acts of fraud and/or abuse against the TRICARE Program.

TRICARE's authority expanded on March 28, 2013 when a final rule took effect that gave authority to TRICARE to sanction third-party billing agents from the TRICARE program for committing fraud or abuse. In May of 2019, the U.S. Department of Defense (DOD) issued a proposed rule that would give the Secretary of Defense authority to impose civil monetary penalties (CMPs) against providers and suppliers found guilty of committing fraud and/or abuse against the TRICARE program. This rule is based on the same section 1128A of the Social Security Act that outlines civil monetary penalties levied by the Department of Health and Human Services for fraud and abuse offenses against Medicare and Medicaid. Adding penalties is an effort to create a program that will be known as the "Military Health Care Fraud and Abuse Prevention Program" that embodies the powers of prosecution, sanctions, exclusions, as well as civil monetary penalties as forces to impede and prevent fraud and abuse against TRICARE. A Program Integrity Division Operational Report published by the Defense Health Agency (DHA) for the period of January 1, 2018, to December 31, 2018, states that it oversees 9.6 million Department of Defense (DOD) beneficiaries with the mission to "manage healthcare anti-fraud and abuse activities for the Defense Health Agency to safeguard beneficiaries and protect benefit dollars."

STATE CONTRACTOR DISQUALIFICATION LIST

One of the most common behaviors of those who commonly abuse the system is what's known as state hopping.

The State and Federal arms of the government work separately to detect fraud and then share information through exclusion, sanction, debarment, and disqualification lists. The General Services Administration (GSA) administers the System for Award Management (SAM) that manages federal procurement systems for several federal agencies.

Each state manages its procurement process and can disqualify a contractor from being awarded a public works contract or subcontract as a result of committing an offense against the contract. When a contractor is disqualified, it carries throughout the entire organization including corporate officers and subcontractors.

One of the most common behaviors of those who commonly abuse the system is what's known as state hopping. If a contractor is disqualified from working with state A, that person or company simply moves to state B and continues the adverse behavior until it is necessary to move to state C and so forth.

As of yet, there is no government source of a consolidated list of disqualified contractors, but data aggregators can be known to aggregate and verify disparate sets of data.

The State Contracting Standards Board governs the process of reviewing and ultimately disqualifying those from participating in state procurement contracts. Each state board is comprised of 14 members. Eight members are appointed by the Governor, two by the speaker of the House of Representatives, two by members of the president pro tempore of the Senate, one by the majority leader of the Senate, and one by the majority leader of the House of Representatives. In the event the Governor's party also controls both houses of the General Assembly, there is a different distribution of board member assignments.

The board members must have knowledge and experience in Federal and state statutes regarding procurement, contract negotiation, outsourcing and privatization, competitive bidding, contract risk assessment, real estate transactions, building construction and architecture, engineering and information technologies, business insurance and bonding, ethics and equality in public contracting, human services and personnel and labor relations.

Led by the State Contracting Standards Board, the relevant state contracting agency, and the Attorney General review the case and may disqualify a contractor for five years or less. Causes for disqualification can include a criminal offense, embezzlement, theft, forgery, bribery, falsification, or destruction of records, violation of antitrust laws, conspiracy or collusion, accumulation of suspensions, reckless failure to perform in accordance with the terms of contracts, agreements of subcontracts, and any other offense deemed worthy to disqualify by the Board, the Attorney General, local law enforcement, and the contracting agency.

STATE MEDICAID EXCLUSION LIST

Screening for Medicaid exclusion for all past addresses assures the provider is eligible to enroll in Medicaid.

State Medicaid programs are undergoing several layers of change, placing a greater accountability on each state to manage provider credentialing and enrollment, as well as screening and monitoring of all affiliates.

The ground is being laid for localized oversight and accountability towards reducing fraud against federal entitlement programs with the ultimate result of better outcomes through better delivery of care.

There are two drivers to the changes affecting the management of State Medicaid programs.

It is the Affordable Care Act that stipulates each state independently enroll providers for participation in Medicaid and Managed Care Organizations. The idea is to distribute the burden of not only enrollment, but of fraud prevention. It is CMS' Program Integrity Enhancements to the Provider Enrollment Process that went into effect November 4, 2019, that requires states to deny or revoke a provider's or supplier's enrollment in Medicaid based on affiliations with companies that commit fraud against any federally funded program.

In order to assure access to health care, it is each State's responsibility to enforce compliance to Federal requirements in order to avoid exclusions, debarments, and disciplinary actions against its provider population.

Screening and monitoring each state's exclusion database will give a heads up to the actions of individuals and entities who may try to evade exclusion. One common practice is where a provider or supplier surrenders a license or opts out of Medicaid in order to remain undetected for fraudulent acts in one state while setting up shop in another state.

However, there are flaws in having each individual state manage a system without pre-set uniformities. Currently there is ambiguity regarding cause for termination and data sourcing. CMS recommends that State Medicaid programs enroll all providers participating in Medicaid managed care, and not only those offering Medicaid fee-for-service.

Ultimately, adding each state as an additional layer of screening and monitoring will contribute to better outcomes and a reduction of fraud, waste, and abuse—an epidemic plaguing the health care industry at large.

SEX OFFENDER REGISTRY

Data analysts at Verisys Corporation have found that two out of every 1,000 providers are listed on the NSOPW.

Health care is a trust-based industry. A health care consumer selects a primary care physician based on the providers within his or her insurance plan, by proximity, and sometimes by a Star Rating. Often, a friend or relative will recommend a physician with whom they have had a positive experience. Referrals for specialists are usually made by the primary care physician from the in-network pool and can range from a podiatrist to a transplant team.

There is the assumption that an institution such as a pharmacy, hospital, surgical center, or practice group carefully vets its providers and employees to assure the quality of service to patients, as well as safety in the workplace. However, many health care organizations focus on bare-bones regulatory compliance to participate in entitlement programs. Some institutions take the additional steps to adhere to requirements of standard-setting organizations that may or may not include screening and continuous monitoring against the National Sex Offender Public Website (NSOPW). Data analysts at Verisys Corporation have found that two out of every 1,000 providers are listed on the NSOPW.

The National Sex Offender Publish Registry (NSOPR) was established in 2005. Then-President George W. Bush signed the Adam Walsh Child Protection and Safety Act into law in July of 2006. The Department of Justice (DOJ), in conjunction with all states, U.S. Territories, Districts, and Tribal Nations, contribute data to the NSOPW searchable database of registered sex offenders that is available to the public.

The DOJ's Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART) site maintains the NSOPW and provides technical support to reporting jurisdictions, private, and public organizations; and offers updates to legal and legislative developments.

Title 1 of the Walsh Act, the Sex Offender Registration and Notification Act (SORNA) classifies sex offenders into three tiers and requires offenders to update their whereabouts on a frequency based on the tier. Tier 1 offenders must update annually with 15 years of registration, Tier 2 offenders must update every six months with 25 years of registration, and; Tier 3 offenders must update every three months with lifetime registration requirements. Failure to register and report according to the requirements is a felony. Adding data sources such as the NSOPW, as well as including additional staff members and vendor entities to the screening and monitoring process beyond what is required for regulatory compliance, is often out of reach based on time and resource limitations. Also, most compliance requirements involve screening and monitoring only the licensed provider population leaving the bulk of the workforce that has access to patients unchecked against NSOPW.

There are no laws or regulations that prevent a provider from practicing medicine as a convicted and registered sex offender. To legally terminate an employee or disqualify a candidate for committing a sex offense, a clearly stated policy to that effect must be included in the bylaws.

ABUSE REGISTRIES

Most states publish abuse registries.

The health care industry should be a safe haven from abuse of any type. It is designed, based on the Hippocratic Oath that contains the phrase, "first, do no harm" to serve a patient's welfare above all else.

However, the health care system is comprised of millions of individuals who, on many levels, come into contact with patients. And when we are patients, we are all vulnerable because we have placed ourselves into the care of another. But, when it comes to populations who are designated as vulnerable, extra care must be taken.

Whether it be the surgeon, the housekeeping staff, security, the charge nurse, the primary care physician, or a volunteer, there is potential for patients to come face-to-face with someone having a documented pattern of abuse.

State abuse registries are maintained through the respective Departments of Health, and include names of persons who have abused, neglected, exploited, or misappropriated the property of vulnerable persons. The list serves to identify and prevent those on the list from providing services to vulnerable persons as defined by each respective state code.

There are three main categories of abuse registries; National Sex Offender Registry, State Child Abuse Registries, and State Adult Abuse Registries. In some cases, the abuse registries are combined.

States publish abuse registries but searching every state to ensure a registered abuser hasn't moved to a different state to avoid detection can be time-consuming to stay on top of the data as it is refreshed on a regular schedule. Also, it is essential to rule out the use of an alias or a spelling alteration. This is where data analytics comes in.

Federal and state regulations governing health care compliance require screening and monitoring against abuse and sex offender registries. Going through the motions of searching the registries will allow you to check the box of completing the action, however, you could face fines if your organization accidentally hires and then submits to a state or Federally funded program for reimbursement on services provided by an individual on one of the registries in a different state than where currently practicing. Worse, due diligence without identity resolution could be putting your vulnerable populations at risk by assigning their care to a registered sex offender or serial abuser. "...first, do no harm."

LICENSE VERIFICATION

Quality health care is the collective goal of patients, health care organizations, providers, government entitlement programs,and commercial payers.

One of the factors to providing quality health care is assuring competency through verifying that the type of care a physician is providing matches to the type of license that physician holds; and that all levels of care are backed by proper training for specialties and subspecialties.

With hundreds of medical boards, it is an insurmountable administrative burden to monitor and verify a provider's license or multiple licenses. The health care industry ascribes to a code of conduct that suggests if the information is attainable, it should be collected and used to assure full transparency on health care providers.

Patients rely on the provider and the health care organization for truth in care—that the provider caring for them and their family has a current license to practice; as well as the assurance of the quality of the provider's character from a historical perspective.

It is the responsibility of medical staff services professionals to research the license history of a provider to rule out a pattern of losing or surrendering licenses for adverse behavior. This effort requires ongoing contact with every licensing board in the United States on behalf of every provider. The same process would apply to verify the status of a license, then connecting each license to the state of practice, and the type of care the provider is offering. Much like finding a moving needle across hundreds of haystacks.

On an important and additional tier of transparency, a health care organization is well served when protecting itself from fines, civil monetary penalties, and legal risk. Seeking reimbursement from a State or Federal entitlement program on services offered by a provider with an expired license, or the incorrect license type, can result in millions of dollars of fines as well as exposure to lawsuits and possible negative news coverage in the event of causing harm to patients.

In the fast-paced regulatory health care environment, staying ahead of the curve will assure the sustainability of quality health care and access through provider transparency and organizational solvency.

STATE MEDICAL BOARDS

Medical boards assure that a licensed provider has the proper education and training, as well as impose disciplinary action, fines, and penalties for unprofessional conduct.

When a state medical board issues a license to practice medicine, it is responsible to assure that the licensed provider has been properly trained and maintains skills through education and clinical practice to assure the highest level of care to that state's patient population.

Another highly important function of the state medical board is to respond to and investigate complaints by patients, other medical boards, health professionals, government agencies, and health care organizations. When appropriate, the board disciplines and publicly reports those disciplinary actions. It is important to keep in mind that state medical boards are passive and rely on reporting.

Most state boards publish notices of administrative and disciplinary actions. These notices are available to anyone on the board's respective websites. The notices typically include the date of issue, name of the physician, city and state of practice, license number, type of action, and date of the action. Most patients may not go through the process of independently researching their doctor as it is assumed that a health care organization as well as the insurance company would assure the quality of its provider staff and network, respectively.

Even if a health care consumer or the medical staff services department of a health care organization searches a single state medical board's database, it would be difficult to find out if a provider left a surrendered, revoked, or an impaired license in one state. Then apply for, and receive a license in another state.

The Federation of State Medical Boards (FSMB) promotes quality health care and embraces the mission of protecting patients. And as part of that mission, it compiles data on provider discipline for all U.S. jurisdictions. There are 70 medical boards represented by the FSMB. The Docinfo portal allows anyone to search a provider by name to see if there are any sanctions, restrictions, or disciplinary actions affecting a provider's license nationwide. Searching the FSMB database would reveal a provider's behavior across state lines.

MALPRACTICE CLAIMS DATA

Malpractice claims data exposes high-risk providers.

Screening and monitoring against malpractice data are the most direct ways for health systems and provider organizations to protect patients. It is important to screen the broad population of an organization against malpractice claims data because it's not only physicians who harm patients from malpractice; injuries can be caused by radiologists, surgeons, surgical staff, nurses, assistants, aides, pharmacy staff, pharmaceutical manufacturers, and administrators.

An NBC News report from July 2019, states that more than one in 10 patients are harmed by medical mistakes and more than 10 percent of those mistakes caused permanent damage or death. Medical errors are one of the leading causes of death in the U.S. despite technological advancements. It is believed that between 250,000 and 400,000 deaths occur annually due to medical errors. A 2016 study by Johns Hopkins supports the 250,000 number of deaths related to medical error.

Types of adverse effects from medical treatment include drug response, surgical events, poor medical management, medical or surgical devices. Other medical errors include misdiagnosis, delayed diagnosis and failure to treat.

Filing a malpractice claim is one of the only ways for patients to try and recover from the devastation of medical malpractice. And for those responsible for screening and monitoring health care professionals, finding out information about medical malpractice suits and settlements can be daunting. Searching through public licensing board records state-by-state is time-consuming, and often the data is old. To close gaps in the reporting criteria, a Department of Health and Human Services (HHS) decision mandates that all medical malpractice claims involving the exchange of payment or compensation must be reported to the NPDB extending the requirement to report beyond the prior wording of "written claim or written demand for payment."

Further outlined in a Modern Healthcare article published in 2014, the HHS ruling was designed to capture disclosure of out-of-court settlements including mediation. Oregon and Massachusetts passed a law that characterized payment received through mediation or non-litigative settlements as outside of the "written claim or written demand for payment" clause and therefore not required to report to the NPDB.

An article published by American Medical Forensic Specialists (AMFS), said that the payments must be reported to the NPDB even when the provider is determined not at fault.

The HHS ruling clarified the requirements for reporting, however, there is no formal enforcement around reporting. The NPDB relies on reporting by authorized, eligible entities as earlier described and there are loopholes where malpractice events remain under the radar. In cases where doctors enter into mediation and personally pay a settlement from personal funds, the settlement will not be reported to the NPDB. This is one of the reasons many providers decide to "Go Bare", the term used for those who don't carry any medical malpractice, also known as professional liability insurance. Another reason providers give for not carrying liability insurance is the cost of the coverage. Additionally, some providers and organizations believe that knowledge of liability coverage invites claims by patients. The requirement to carry medical malpractice insurance is imposed by states, not the Federal government. According to a Gallagher blog, some 36 states do not require medical malpractice insurance and no minimum levels of insurance. However, there are instances where providers may be required to carry coverage such as for high-risk procedures, or physicians requesting visiting privileges.

Gaining access to the National Practitioner Data Bank (NPBD), the federal database of malpractice claims and provider sanctions, requires registration and eligibility under federal regulations as spelled out in the NPDB Guidebook, Chapter B:

ELIGIBLE ENTITIES INCLUDE:

BOARDS OF MEDICAL EXAMINERS

DEA

FEDERAL AGENCIES UNDER SECTION 1921 AND 1128E

HEALTH CARE ENTITIES

HEALTH PLANS

MEDICAL MALPRACTICE PAYERS

PEER REVIEW ORGANIZATIONS

FRAUD AND LAW ENFORCEMENT AGENCIES AND CONTROL UNITS

LICENSING BOARDS

ACCREDITATION, PROFESSIONAL AND QUALITY IMPROVEMENT ORGANIZATIONS, AND OTHERS

HOW VERISYS COLLECTS, VERIFIES AND DELIVERS DATA FOR A TURNKEY COMPLIANCE SOLUTION

Understanding the full array of data sources helps to see why full transparency is the only way to prevent and mitigate fraud, waste, and abuse against the health care system as well as assure quality care to patients. Verisys believes in providing a 360-degree view of providers as well as all levels of employees of a health system, its board, affiliates, and vendors. The 360-degree view means access to longitudinal data—past and real-time; it means checking all sources of data relative to the practice of medicine; and it means checking all sources of data that expose criminal and abusive behavior. Removing serial fraudsters, sex offenders, violent criminals, drug and weapons traffickers, and other threatening individuals from the health care system takes effort and diligence.

Verisys was originally founded on the vision of two former highly placed government appointees in 1992 and preceded the Federal Government's Health Care Fraud and Abuse Control Program. John O'Shaughnessy, former assistant secretary of the DHHS, and Dick Kusserow, former Inspector General for DHHS began creating their database called Fraud Abuse Control Information System, FACIS®. Knowing the need for a centralized data platform that aggregates and stores verified data from primary sources, they built FACIS record by record, and today it holds more than 8 million records. Continuously collecting from more than 3,500 primary sources, it grows daily, adding to the cumulative data since 1992 for a longitudinal view of health care entities and individuals. Searching FACIS instantly reveals arrests, indictments, debarments, disciplinary actions, sanctions, exclusions, license infractions, actions announced in press releases from state and Federal enforcement agencies, and minutes from license board hearings.

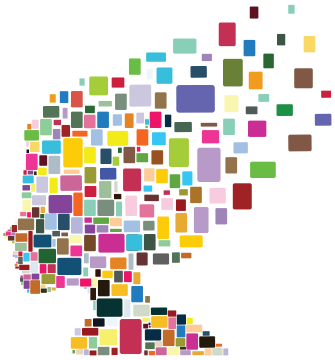
SUMMARY

From the foundation of proprietary data collection and verification, Verisys developed CheckMedic®, a turn-key credentialing and enrollment platform with more than 320 million records that issues a secure, digital credentialing profile, the MedPass®, to each provider and entity. At any time, an administrator, or a provider logs in to review a provider's credentials, the MedPass is current and accurate.

With hundreds of millions of records being matched through searches on million-plus health care providers, verification and identity matching must be accurate, or the system fails. The highly skilled content team at Verisys uses proprietary matching logic algorithms to reach 99.5% accuracy on identity matching nearly all of the time. The combination of automation and hands-on attention delivers reliable and actionable results, whether it be through an enterprise-wide implementation of CheckMedic, or a single verified search through Verisys Connect®, the self-serve online search engine for FACIS (3,500 primary sources), national license, OFAC Plus, NPI, Abuse and Sex Offender Registries.

ProviderCheck® was developed to verify prescriber credentials and is widely used by some of the largest retail pharmacies. It is a real-time transaction engine that protects organizations from fines and exposure by checking a provider's credentials and issuing a pass/fail for each of the five criteria on provider transactions. ProviderCheck utilizes a provider's NPI number to return a Yes/No response for five key data points: Exclusions/Debarments, Medicare Enrollment (PECOS), Active Licensure, Active DEA Registration and Schedules, and NPI Data (NPI type, multiple NPI numbers used, and primary NPI number) for a specified date of service.

The health care industry receives no exception as a victim to those who intend to defraud and abuse. However, the health care industry has the most to lose at the hand of fraudsters and criminals targeting health care—the well-being and lives of innocent patients. For this reason, Verisys works tirelessly to collect data and innovate ways to deliver this critical data in real-time to those who are the at the front lines of preventing and stopping those bad actors who cause harm and commit fraud from entering the doors of their health system and treating patients; getting behind the counter of their retail pharmacy; or illegally seeking reimbursement from government entitlement systems and commercial payers.



DATA

UNLOCKING THE KEYS TO DATA FOR BEST PRACTICE HEALTH CARE COMPLIANCE

UNDERSTANDING HOW DATA PROTECTS PATIENTS, YOUR ORGANIZATION AND THE HEALTH CARE INDUSTRY

VERISYS.COM

A VERISYS CORPORATION PUBLICATION