alessa

Battling Health Insurance Claims Fraud

Introduction

Insurance companies and providers of health care benefits lose hundreds of millions of dollars yearly due to fraudulent claims for health benefits. Some of these are bogus claims that originate from insured persons, while others are payments for insured services that are not needed but are wrongly prescribed by providers who stand to make illegal profits.

The U.S.-based National Health Care Anti-Fraud Association estimates health care fraud costs the nation no less than $68 billion annually — about three percent of the nation's $2.26 trillion in health care spending. Others say that number may be substantially higher.

The bottom line is fraud costs everyone through higher premiums or through tax dollars spent on public health benefits. Benefits fraud is a serious crime and is treated that way by law enforcement agencies around the world.

This white paper will outline common schemes and case studies to help your organization prevent or uncover fraud ahead of it being paid out.

Case Study: Los Angeles doctor and patient recruiter guilty in $33M fraud scheme

A federal jury found a Los Angeles doctor and patient recruiter guilty for their roles in a $33 million Medicare fraud scheme in which Medicare was billed for clinic, home health, hospice services and durable medical equipment that patients did not need or receive.

Following a seven-day trial, Robert Glazer, M.D., 73, was found guilty of one count of conspiracy to commit health care fraud and 12 counts of health care fraud. Co-defendant Marina Merino, 62, a marketer who recruited patients in exchange for kickback payments, was convicted of one count of conspiracy to commit health care fraud and eight counts of health care fraud.

Merino and other marketers received payments to recruit Medicare beneficiaries to Glazer's clinic. Thereafter, Glazer billed Medicare for office services and tests that patients did not need or did not receive. Glazer also referred Medicare patients for a variety of services, including home health and hospice services, as well as ordered medical equipment that patients did not need or did not receive.

Together, the defendants and their co-conspirators submitted and caused to be submitted claims of approximately $33 million, of which Medicare paid approximately $22 million, the evidence showed.

Source: FBI

Fraud Schemes

Billing for services not rendered

This kind of scheme involves the charging for services that are not rendered by the medical provider.

Detecting billing fraud schemes

- Identify the reported dates for the received medical services in the claim form and cross check them with the medical file
- Make cross check verifications with the medical facility on the specific dates filled on claim forms
- Check with the facility sign-in logs and appointment calendars
- Verify billing details with the listed doctor
- Check if the type of the customer's condition matches with the doctor's area of specialty

Case Study: LA dentist sentenced to prison in $3.8-million health care scheme

A Los Angeles, California-based dentist was sentenced recently to 40 months in prison for his role in a $3.8 million health care fraud scheme in which he billed numerous dental insurance carriers for crowns and fillings that were never provided.

Benjamin Rosenberg, D.D.S., 59, of Los Angeles, was also ordered to pay $1,414,011.59 in restitution. Rosenberg pleaded guilty on Jan. 31, 2019, to one count of health care fraud.

As part of his guilty plea, Rosenberg admitted that he submitted approximately $3,853,931 in false and fraudulent claims to various insurance companies for dental care that he knew had not been rendered.

Rosenberg further admitted that he submitted these false and fraudulent claims to eight insurers, which caused them to pay Rosenberg approximately $1,415,011. The FBI investigated this case.

Source: FBI

Unnecessary medical testing / overtreatment

At times, a patient is advised that they need additional medical testing to diagnose the problem. In fact, the testing is not required and the fee for the unnecessary work often is split with the physicians. In some cases, physicians own the medical testing service.

Sometimes insurance providers are billed for something more than the level of care actually required. This can include medical equipment as well as services.

Detecting unnecessary treatments

- Check if the medical testing procedures are in line with the patient's condition
- Look for medical testing procedures that are redundant, repeated, or are related to totally different medical conditions that fall outside of the patient's condition

Case Study: Chicago-area physical therapy centre and nursing facilities to pay $9.7M

The U.S. Attorney's Office in Chicago announced that a Chicago-area physical therapy center and four nursing facilities have agreed to pay $9.7 million to resolve civil allegations that they violated the False Claims Act by providing unnecessary services to increase Medicare payments.

The allegations also contend that the providers rendered skilled therapy to patients who did not need it or could not benefit from it, as part of an effort to bill the highest possible amount to Medicare.

The settlements and consent judgments resolve a civil lawsuit under the whistleblower provisions of the False Claims Act. The Act permits private citizens to bring lawsuits on behalf of the United States for false claims, and to share in any recovery. The United States intervened in the lawsuit prior to the settlements and consent judgments.

Frances Parise, the owner of the nursing homes, also agreed to be excluded from all participation as a provider in Medicare, Medicaid and all federal health care programs for a period of five years.

Source: FBI

Fictitious providers – Bogus doctors

In this scheme an individual who is not a doctor opens a medical practice. The individual obtains or creates a doctor's ID number to appear legitimate.

Detecting bogus doctors

- Check official databases of medical providers
- Verify the medical providers against a checklist of official qualifications that must be in place
- Verify the address of the medical provider or doctor
- Verify that the physician has not been suspended by its regulatory body

Double billing

Double billing occurs when the insured and / or the provider seek to be paid twice for the same service. The fraud might be perpetrated by the insured with the complicity of the provider, or the provider alone might do it.

Preventing multiple billings

- Look for multiple submissions for the same type of expense and/or treatment
- Check for submissions from blacklisted providers
- Check for multiple submissions for the same date
- Investigate sudden increases in reimbursements

Coding fragmentation/fictitious coding/unbundling

In this case, bills for a service are submitted a bit at a time or staggered over time to increase charges. Sometimes these services cost less when bundled together, but by separating the claim into components, a higher charge is billed to the insurance provider resulting in a higher payout to those committing the fraud.

In coding fragmentation, there is also a possibility for misrepresenting a non-covered medical service as a covered one. In order to justify a medical procedure against a diagnostic code, a fictitious diagnostic code might be entered in order to appear legitimate. The false billing takes place if the physician or the other primary provider knowingly enters an incorrect diagnostic code.

Red flags for detecting the scenario

- Use analytics to determine whether each code submitted is a subcomponent of one or more comprehensive codes.

Case Study: Baton Rouge doctor imprisoned for 'unbundling' health scheme

A Baton Rouge, Louisiana-based doctor was sentenced to 37 months in prison followed by two years of supervised release for his role in a scheme to defraud Medicare and other health care insurers. John Eastham Clark was also ordered to pay $254,962.80 in restitution. Clark admitted that he and others conspired to submit fraudulent claims saying minor surgical procedures occurred on days subsequent to office visits when the procedures took place on the same day. Clark admitted the "unbundling," was done to defraud health care insurers for non-reimbursable office visits.

Source: FBI

Kickbacks

Kickbacks are payments or non-monetary gifts or rewards used to entice medical professionals into using specific medical services. This could be a cash kickback for using a specific clinic or service when not required.

Detecting and preventing the scenario

- Review vendor transactions to detect unusual concentrations of activity with a few providers
- Review year-to-year comparisons in transactions for significant increases with providers or where costs of materials or services are out of line
- Flag for potential cases of overbilling
- Review vendor addresses to employee addresses to look for matches

Case study: Doctors and marketers charged with taking kickbacks

Three physicians and five marketers in Tulsa, Oklahoma have been charged with violations of the federal anti-kickback statute and other criminal offenses.

The men allegedly got kickbacks and caused federal health care insurance programs to pay them directly for fraudulent and expensive compounding drug prescriptions written by recruited doctors.

Dr. Krishna Balarma Parchuri, 44, of Tulsa, is charged with Christopher R. Parks, 57, of Tulsa, Dr. Gary Robert Lee, 58, of Tulsa, and Dr. Jerry May Keepers, 65, of Kingwood, Texas, with conspiracy to commit health care fraud. Keepers and Parchuri are also charged with soliciting and receiving illegal bribes and kickback payments.

The criminal indictment alleges Parks and Lee engaged in a conspiracy to unlawfully pay kickbacks and bribes to physicians in order to induce the physicians to write expensive compounding prescriptions to pharmacies they controlled.

The defendants then allegedly submitted $4.3 million in claims for payment to federal health care programs and divided the profits.

Conspiracy to violate the anti-kickback statute carries a possible maximum sentence of five years in prison and a $250,000 fine, while violating the anti-kickback statute carries up to 10 years in prison and a $100,000 possible fine. A conviction of health care fraud without injury or death also carries a possible maximum of 10 years in prison.

Source: FBI

Claim submission fraud

Multiple claims

An insured may have multiple coverage policies, and has the right to submit claims to more than one insurer and under more than one policy. Insurance coverage provisions require that one carrier be designated as the primary insurer and the other companies will be secondary or tertiary insurers.

The insured commits a fraud when he makes a claim for a covered loss without revealing that he has already been paid for that loss. Such fraud may involve both fraudulent concealment of the prior claim and payments and misrepresentations that the loss has been uncompensated.

Alteration

A dishonest claimant could inflate a prescription or medical bill by placing an additional number in front of the amount charged. The claimant could also alter the date of service so it becomes a recoverable expense.

Another form of alteration is when the individual submitting claim may change the name on the bill from an uninsured family member to one included in the insurance plan. Other forms of alteration include using:

- Ineligible dependants
- Name and address of the person receiving the treatment
- The patient's true relationship is to the insured
- A complete description to the person receiving the treatment
- A complete physical description of the impersonator
- Complete hospital records, including the emergency room report, the admitting history, and the physical description of the patient

Third-party fraud

This category involves the use of an insured's identification card by another person. The actual ID holder is made aware that his insurance plan has been used by another person. The ID holder then makes the claim to the insurance company and falsely claims that he actually received the services personally.

Detecting and preventing the above scenarios

Look for the following when trying to detect multiple claims, alterations and third-party fraud:

- Misspelled medical terminology
- Unusual charges for a service
- Similar handwriting by the claimant and the provider of the service
- Typed rather than printed billings
- Bills with irregular columns
- Unassigned bills that normally are assigned
- Drug receipts from the same pharmacy but on different paper
- Erasures or alterations
- Lack of any provider's signature on a claim form
- Absence of the provider's medical degree
- An illegible provider's signature
- Pressure by claimant to pay a claim quickly
- Individuals who hand-deliver their claim and insist on picking up their claim cheque
- Continuous telephone inquiries regarding the status of a pending claim
- Poor quality photocopies of documents that should be original documents
- Frequent change of medical providers
- Independent medical exams that reveal conflicting medical information

Case Study: 10 charged in $200 million prescription drug fraud

Ten defendants face charges in a 103-count indictment that includes a nurse practitioner, the owners, a pharmacist, managers, sales representatives, and billers, of a Haleyville, Ala.-based pharmacy. The staff at Global Compounding Pharmacy are charged with fraudulently billing health care insurers and prescription drug administrators for over $200 million in prescription drugs. In one listed instance, the defendants' fraudulent conduct caused a prescription plan administrator to pay over $29,000 for one tube of a cream advertised as treating "general wounds."

The indictment describes a multi-faceted health care fraud and mail fraud conspiracy and scheme in which the defendants billed for medically unnecessary drugs. Aspects of the scheme included paying prescribers to issue prescriptions; directing employees to get medically unnecessary drugs for themselves, family members, and friends; altering prescriptions to add non-prescribed drugs including controlled substances such as Tramadol and Ketamine; automatically refilling prescriptions—often as many as 12 times—regardless of patient need, among other schemes.

The defendants billed health insurance plans and their prescription plan administrators over $200 million and were paid over $50 million.

Source: FBI

Other red flags to consider

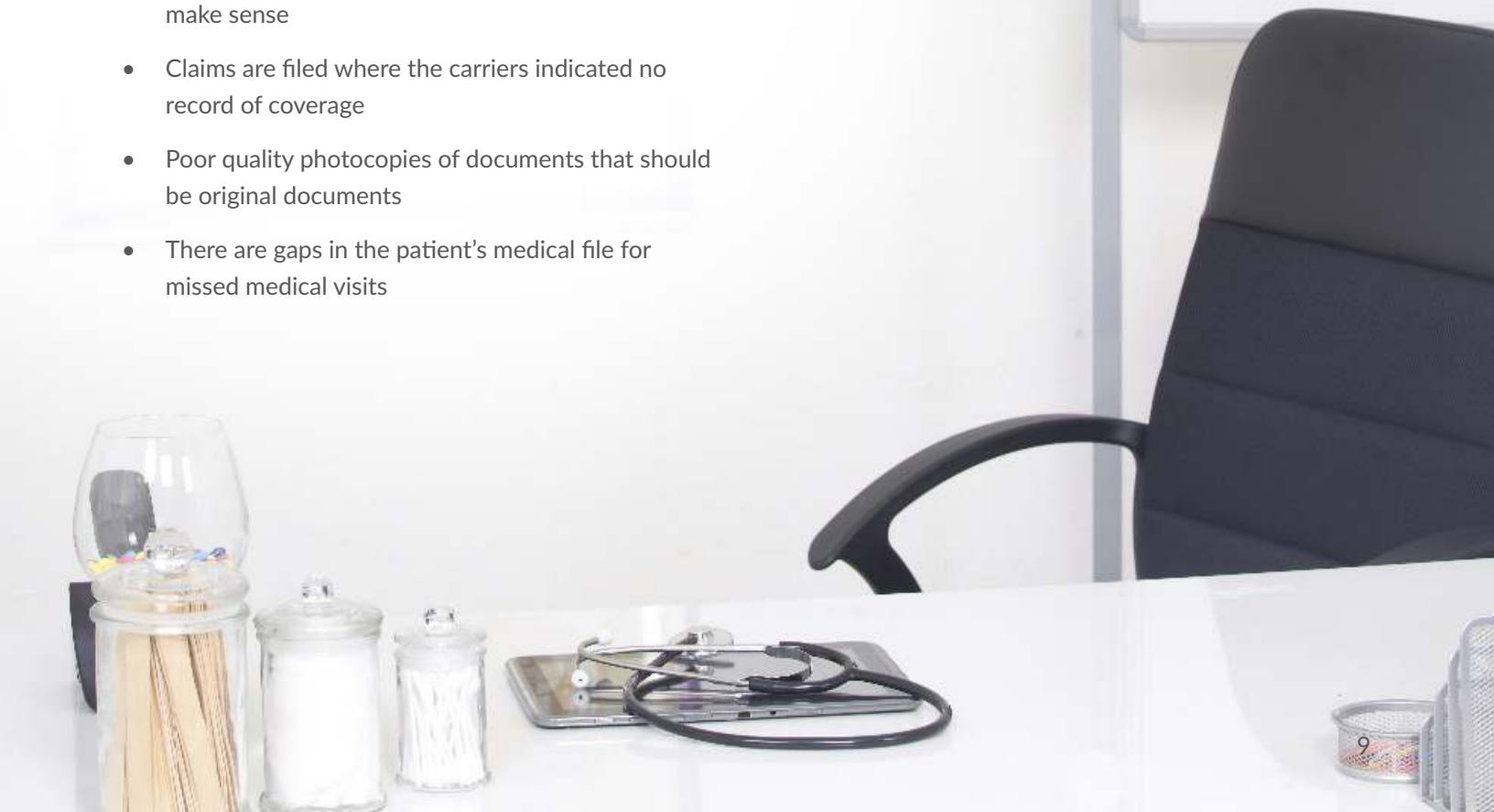
Documentation red flags

The insured refuses or is unable to answer routine health questions

- The insured provides supporting evidence and documentation that cannot be corroborated
- Information on a life insurance application is vague or ambiguous as to the detail of health history
- The physician's report is vague on details of past medical history and does not coincide with the information shown in the application
- A series of prescription numbers from the same drug store do not line up chronologically with the dates of the prescriptions
- Documents are obviously altered; whiteout or erasure is evident
- Documents are improperly filled out, entries are in the wrong place, and information provided does not make sense
- Claims are filed where the carriers indicated no record of coverage
- Poor quality photocopies of documents that should be original documents
- There are gaps in the patient's medical file for missed medical visits

Claimants red flags

- Are soon to retire, facing disciplinary action or layoffs
- Take unexplained or excessive time off prior to claimed issue
- Have inappropriate or a lack of medical treatment for injuries
- Are experiencing financial difficulties
- Change physicians to achieve a different diagnosis
- Frequently change medical providers
- Have demands for quick or early settlements
- Have independent medical exams that reveal conflicting medical information
- Have unprofessional diagnostic terminology




HEALTH INSURANCE
CLAIMANT INFORMATION
REPLAY
MODE
OFF
DEL
AC/ON

Conclusion

Fraud is not a victimless crime. We all pay for fraud through higher premiums or lost services because governments or insurance providers have to spend part of their budgets toward these fraudulent claims.

If you suspect fraud, report it. In the United States, the FBI is tasked as the primary agency for investigating federal or private health insurance fraud. Patient-driven fraud can mean others needing treatment are unable to receive it, while conspirator fraud may mean some patients do not get the full and necessary treatment they deserve.

Tier1 Financial Solutions offers a solution called Alessa to help screen transactions and ongoing business between caregivers and insurance company staff.

Transaction monitoring and screening: Alessa offers the ability to identify potentially fraudulent insurance claims prior to payout. In these cases, the claim management system sends the claims transactions to Alessa. Alessa then examines them using its anomaly detection engine and scores the transaction based on its attributes. If the transaction is considered high-risk then a message is returned to the claims management system, the status is updated to "At Investigations" and an alert is sent to the appropriate person(s). If after investigation the decision is made to deny the claim, the platform sends a new message to update the status to "Denied."

Investigation Tools: Alessa offers dynamic workflows to guide processes and investigations. Enterprise search capabilities allow for easy searching of data within internal and external sources, while case management offers a collaborative approach to investigations, compliance, and decision making.

Risk Scoring: Alessa uses data from various sources, including sanctions lists, to provide an assessment of the risks with transactions or of doing business with an individual or business. The solution also periodically reviews an organization's customer base and updates their risk level based on their activity and third-party data.

Configurable: With Alessa, organizations can select the functionality they need or the complete solution. Permission-based functionality allows different users to access only the information they need to perform their responsibilities, and data can be maintained in the cloud or on premise, ensuring compliance with regulations.

Data Management: Alessa accesses data from any platform, including ERPs, bespoke applications, and core business systems. The data is then cleansed and aggregated to increase its accuracy, and cross-referenced to reveal big-picture insights. Better data means better insights.

Metrics & Insights: Alessa offers configurable dashboards that track key metrics and allow compliance staff to drill down into the alerts. Advanced analytics allow for sound decision-making and actions to be taken based on comprehensive information and insights.

To learn more about Alessa can help your organization fight fraud and other forms of financial crimes, visit our website at **www.alessa.com.**

About Alessa

Alessa, by Tier1 Financial Solutions, is a compliance, controls monitoring and fraud prevention solution for banking, insurance, fintech, gaming, manufacturing, retail and more. With deployments around the world, Alessa allows organizations to quickly detect suspicious transactions, identify high-risk customers and vendors and decrease fraud risks that reduces profitability and increases costs. To learn more about how Alessa can help your organization ensure compliance to regulations, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at https://www.alessa.com/.

150 Isabella Street, Suite 800,
Ottawa, ON K1S 1V7, Canada

1-844-265-2508

alessa@tier1fin.com

www.alessa.com

alessa
by Tier1 Financial Solutions