AVESIS INCORPORATED and subsidiaries

FRAUD, WASTE & ABUSE

CMS regulations under 42 CFR Sec 423.504 and the Federal Deficit Reduction Act (DRA) of 2005, Section 6032, require that all entities receiving payments for Medicaid or Medicare members in excess of $5 million, provide written policies and detailed information for preventing and detecting fraud, waste and abuse. Information must be provided to *all employees, contractors and agents* and shall include the method for preventing and detecting fraud, waste and abuse and the rights of employees to be protected as whistleblowers.

This requirement must be adhered to by Avesis as well as all of our providers.

The Fraud, Waste & Abuse Plan

is designed to:

- **Help prevent fraud, waste & abuse**
- **Help detect fraud, waste & abuse**
- **Identify clear steps for investigation using a Fraud Response Plan**
- **Reduce financial loss or damage to Avesis' reputation**

AREAS TO BE ADRESSED:

Eligibility and enrollment practices including enrollment forms, claim forms and assignment of benefits on claim forms;

Marketing practices including broker commissions;

Approval and denial of care;

Member notification of rights and benefits;

Appropriate qualifications and administration of the provider network;

Claims procedures including timeliness of payments to providers;

Security of patient information

WHAT IS FRAUD:

"Fraud is an intentional deception or misrepresentation made by someone with knowledge that the deception will result in benefit or financial gain."[1]

The difference between fraud and a mistake/error is *intent.*

WHAT IS THE COST OF FRAUD?

- **Over $2.2 trillion was spent in the US on health care every year**
- **Estimated 3% - 10% of health care dollars are lost to fraud**
- **If 5% is correct, that equals a loss of $100 billion to health care fraud annually or**

$300 million per day!

[1] iCare Training

STRATEGY:

All employees and providers are to be fair and honest;

All employees are to provide any assistance, information and support to deal with fraud, should it occur

All employees shall abide by all Company established rules, policies, procedures, codes and recommended practices

OVERVIEW:

Avesis Corporate values include *honesty* and *integrity* in all dealings;

The Company's expectation is that all employees, providers and organizations that are associated with us be honest and fair in their dealings;

Senior management and supervisors are to lead by example;

All employees have an important role in detecting fraud and are encouraged to raise any concerns that they may have;

The Company will deal with any information received in a fair and confidential manner;

A Whistle-Blowing Policy is in effect so that employees can share concerns without fear of retaliation;

Suspected fraud is to be reported immediately to appropriate personnel (CEO, CFO, COO, Fraud Officer); or, directly to CMS FWA Hotline at (800) 447-8477 (if the matter involves a BlueCross BlueShield SC member, you can contact the BCBSSC Fraud Unit at (800) 763-0703)

In certain instances, the Company may refer the matter to the appropriate law enforcement agency or State or Federal Attorney General.

PREVENTION:

Employees and Participating Providers are expected to have read and abide by all rules and procedures appearing in the:

- **Employee Handbook**
- **Code of Conduct**
- **Provider Manual**
- **Code of Ethics and/or**
- **Professional Code of Conduct;**

All employees are expected to annually sign the Company's Conflict of Interest statement;

Senior managers are responsible for ensuring that internal controls are in place to minimize the chance of fraud occurring. This includes making certain that all financial procedures are followed and that there is adequate separation of duties;

Department supervisors and managers are responsible for maintaining staff recruitment procedures. All prospective employees must undergo background investigations *prior* to am employment offer being made and complete and sign the Conflict of Interest statement;

All employees are to be provided with information regarding the Company's Anti-Fraud Plan as well as the Company's disciplinary procedures.

DETECTING AND INVESTIGATING FRAUD, WASTE & ABUSE

Employees must report *any* suspected cases of fraud to their Department Supervisor. The Department Supervisor will review the complaint and refer it to either the CEO, CFO, COO or Fraud Officer.

NOTE: Employees are assured of confidentiality. If you suspect fraudulent activity on the part of a co-worker, supervisor or provider you must report it to the supervisor, CEO, CFO, COO or Fraud Officer.

Incidences of waste and abuse must also be reported.

Providers must also report suspected Fraud, Waste or Abuse. The Avesis hotline number is on the website and they can also report directly to CMS.

REPORT IT IMMEDIATELY!

EXAMPLES OF POSSIBLE FRAUDULENT ACTS:

- Where an individual or provider has fraudulently obtained money from Avesis (benefit fraud) or where a bribe or inducement is accepted
- Non-members using Members' ID cards to obtain benefits
- Providers billing for services or materials that were not rendered
- "Phantom" provider – obtaining a Medicaid ID or NPI number and billing for materials or services never rendered
- Altering claim forms and/or receipts in order to receive higher payments
- Falsely stating the nature of the services provided or the diagnosis in support of providing the services/ materials
- Completing Certificates for Medical Necessity without having seen the patient
- Submitting prior authorization requests without having seen the patient

EXAMPLES OF FRAUDULENT ACTS:

MEMBER FRAUD EXAMPLES:

Theft of ID/Services

Unauthorized person uses a Member's Medicaid or other ID card to obtain services or materials – often a family member or acquaintance

Falsification of Documents/Forgery

Misrepresentation of Benefits

A misrepresentation by an agent of benefits in order to persuade someone to join a health plan

WHAT IS ABUSE? WHAT IS WASTE?

"Abuse" is frequently defined as a practice that is not consistent with accepted industry practices or standards that results in unnecessary costs. Abuse may be thought of as potential fraud in situations where the provider's intent is unclear.

- **Examples:**
  - **charging in excess for services**
  - **submitting claims to CMS or insurers for Members who are the responsibility of other insurers**
  - **violating the Provider Agreement or provisions of the Provider Manual**

"Waste" includes any practice that results in the unnecessary use of resources (financial, medical, etc.)

- **Examples**
  - **Printing two pages on two separate pieces of paper rather than front and back**
  - **Leaving office lights on when leaving for the day or extended periods of time**

CONTRASTING FRAUD VS ABUSE:

Billing for non-covered services

Fraud – Provider knew the service was non-covered but changed the diagnosis to obtain coverage or changed the procedure code to a covered service code (e.g. CDT code D2160 v. D2950)

Abuse – Provider billing for multiple sites when the CDT code is for one tooth

Misusing codes on the claim

Fraud - Provider knowingly, deliberately and intentionally identified loop-holes

Abuse – Provider assumes that he is billing correctly since claims were being paid

WHAT TO DO IF YOU SUSPECT FRAUD?

- **Approach your Department Supervisor – the Department Supervisor will substantiate the claim and will inform the CEO, CFO, COO or Fraud Officer (determination is based upon the nature of the complaint)**
- **You may also contact the CMS Medicare Fraud Hotline at (800) 447-8477 (if the matter involves a BlueCross BlueShield SC member, you can contact the BCBSSC Fraud Unit at (800) 763-0703)**
- **Provide as much detail as possible regarding the complaint**
- **If confidentiality is a concern, follow the Whistle-Blowing Policy, where confidentiality will be respected whenever possible.**
- **If the matter relates to another employee or your Department Supervisor, the matter may be reported directly to the CEO, COO or CFO**
- **Never make malicious complaints. These are taken seriously and action will be taken against any employee doing so.**

WHAT WILL HAPPEN NEXT?

- An initial investigation will be carried out to establish validity of the allegation

A decision will be made by the COO on how to proceed (if the complaint is of a very serious nature, the CEO and CFO will also be informed)

- Upon conclusion of the initial investigation, either further investigation will be undertaken, the matter will be referred for disciplinary action or it will be referred to the appropriate law enforcement agency, State or Federal Attorney General's office.

A determination will be made regarding how and when the matter will be reported.

- Notification will be sent by the COO to the complainant explaining what has occurred to date regarding the investigation and actions taken or to be taken

WHISTLE BLOWER POLICY

- Intended for use with serious or potentially serious allegations or sensitive issues (minor issues such as stealing of stationary, misuse of phone calls, etc. should reported to the Department Supervisor).

- Serious concerns should be brought to the attention of the CEO, COO, CFO or Fraud Officer.

- As with any type of allegation providing as much information as possible is extremely important.

- Confidentiality will be maintained wherever and whenever possible. However, in certain situations the identify of the complainant may be provided to law enforcement or the Attorney General.

- The Company will not tolerate any attempt by anyone (including supervisors, officers, co-workers or providers) to apply any type of pressure, sanction, harassment or victimization.

MISCELLANEOUS LAWS AND GUIDELINES

Anti-Kickback Statute prohibits:

"the knowing and willful offer, payment, solicitation or receipt of any remuneration in cash or in kind, direct or indirect… to induce someone to refer a patient or to purchase, order or recommend any item or service which may be paid for under a Federal Health Care program."

Anti-Kickback: Suspect Arrangements

- Paying a provider for each patient who enrolls or remains enrolled in the plan
- Conditioning compensation on a minimum percentage of enrollees
- Offering enhanced fees or fees that clearly exceed fair market value, to providers without any justification
- Accepting material gifts or perks from vendors in exchange for selecting vendor's products or services

Anti-Kickback: “Safe Harbors”

- Most important “safe harbors” for health plans
  - Discounts offered to health plans by providers in exchange for something
  - Price reductions offered to health plans by providers
  - Agreements with contractors with substantial financial risk

Other Relevant “Safe Harbors”

- Management contracts
- Increased coverage, reduced cost sharing amounts or reduced premium amounts offered by health plan to Members

False Claims Laws

Significant penalties exist for knowingly:

Submitting (or causing to be submitted) a false or fraudulent claim for payment or approval; or

Making or using (or causing to be made or used) a false record or statement in support of a false or fraudulent claim; or

Failing to return overpayments made by a government agency

"Knowingly" includes actions taken in "reckless disregard" or with "deliberate ignorance" of truth or falsity.

The *qui tam* provisions of the federal False Claims Act (FCA)

Lawsuit initiated by private individual (defined as "relator")
The government may choose to intervene in the private lawsuit
Qui tam "relator" shares in civil monetary recovery, if any, with the government

Potential False Claims Violations

Misrepresentation of information presented in reports to Medicare or Medicaid

Misrepresentation of claims or eligibility data reported to Medicare or Medicaid

Civil Monetary Penalties Law

The Social Security Act authorizes the Secretary of Health and Human Services to seek civil monetary penalties (CMPs) and assessments for many types of illegal or unethical conduct; many of which have been delegated to the OIG.

Types of prohibited conduct include, but are not limited to:

- ❑ Offering inducements that are likely to influence Medicare or Medicaid Members to order or receive items or services from a particular provider or supplier;
- ❑ Misusing Medicare and Medicaid program words, letters, symbols or emblems

Violation Examples

- ❖Submitting a claim or claims for services that were not rendered
- ❖Using a CMS logo without proper approval
- ❖Failing to promptly return a known overpayment
- ❖Offering inducements to influence decisions related to Medicaid or Medicare funds
- ❖Hiring employees who have been excluded from participation in federal programs

AVESIS RED FLAGS/POTENTIAL WARNING SIGNS

GENERAL OR POTENTIAL INDICATORS OF FRAUD:

- **Physical address is not disclosed or uses P.O. Box, attorney's office or relative**
- **Address provided is not valid**
- **Subject's SS#, name or other pertinent information doesn't match up**
- **Receive tips or rumors from co-workers, neighbor or family**
- **Recent Claims in the family or co-workers**
- **Claim filed several days, weeks or months after alleged loss**
- **Has multiple means of coverage for loss**

GENERAL RED FLAGS/POTENTIAL WARNING SIGNS

GENERAL OR POTENTIAL INDICATORS OF FRAUD:

- **Physical address is not disclosed or uses P.O. Box, attorney's office or relative**
- **Address provided is not valid**
- **Subject lives in transient housing**
- **Subject is moving around**
- **Subject uses other people's telephone numbers**
- **Subject's SS#, name or other pertinent information doesn't match up**
- **Receive tips or rumors from co-workers, neighbor or family**
- **Recent Claims in the family or co-workers**
- **Claim filed several days, weeks or months after alleged loss**
- **Recent increase in coverage**
- **Reduction of deductible**
- **High number or other recent claims**
- **Makes a social security disability claim as well**
- **Has multiple means of coverage for loss**

AVESIS RED FLAGS/POTENTIAL WARNING SIGNS

GENERAL OR POTENTIAL INDICATORS OF FRAUD - PERSONAL:

- Subject or spouse unemployed/self employed or seasonal worker
- Recent changes in family status
- Recent financial changes
- Subject has a criminal history, appears unethical, depressed or lazy
- Subject advises he is a victim of the insurance company
- Family history of claims
- Subject retains attorney immediately
- Attorney well known in the involvement of suspicious claims
- First Notice of Claims is from attorney
- Subject is threatening or abusive
- Subject might be evasive, repeating questions
- Subject is non cooperative
- Claimant’s have strong knowledge of claims process and terminology

RED FLAGS/POTENTIAL WARNING SIGNS

GENERAL OR POTENTIAL INDICATORS OF FRAUD – PERSONAL (cont.):

- **Subject never home for calls – asleep-just left etc.**
- **Subject refuses personal visits by claims personnel**
- **Subject demands payment right away**
- **Subject calls constantly/daily to get paid**
- **Subject's demands are out-of-line with the type or degree of loss**
- **Subject avoids U.S. Mail, facsimile**
- **Drops off documents in person**
- **Subject in a hurry to settle claim**

RED FLAGS/POTENTIAL WARNING SIGNS

GENERAL OR POTENTIAL INDICATORS OF FRAUD – AGENT & APPLICATION:

- **Material misrepresentation on application**
- **Clear inaccuracies on application**
- **Minimum premium paid on initiation of policy**
- **Insured paid cash**
- **Insured living with others not on application**
- **Application not signed**
- **Blank answers**
- **Application completed by two or more different people**
- **Undisclosed risk issues**
- **Some coverage, but not others**
- **Recent additions of coverage**
- **Any discrepancies of SS#, name, dob or address**
- **Walk in Clients**

RED FLAGS/POTENTIAL WARNING SIGNS

GENERAL POTENTIAL INDICATORS OF FRAUD – PROVIDER:

- Claims that duplicate or unbundle procedures to maximize payment
- Errors of an obvious nature such as subject's gender, race or age
- Diagnosis and treatment don't match
- Service location using a P.O. Box or mail drop
- Different names or addresses for dependents and insured
- Facility with several names
- Unprofessional letterhead or stationary/photocopied
- Duplicate requests for authorization that has been denied
- Referral to nearby medical testing or clinics
- Answering machine
- Multiple claims submitted on different dates for the same member (each with same date of service or overlapping dates of service)
- Spikes in claims activity or reimbursement compared to historical activity
- Inconsistency of fees for various services

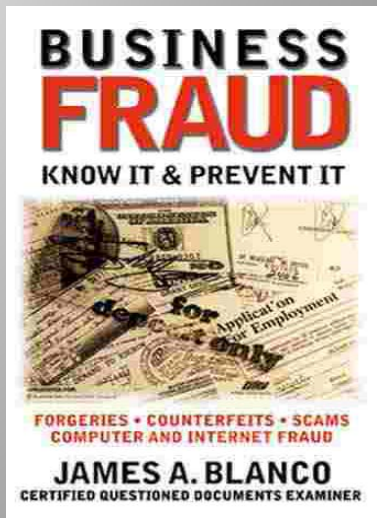
WRAP UP:

We are committed to ensuring that all necessary systems and procedures are in place to prevent fraud, waste and abuse.

When changing services or the delivery of services, managers must always take into account fraud prevention and detection in new systems.

If you are not certain if an activity is fraudulent, bring it to your supervisor's attention.

ALL OF US WORKING TOGETHER CAN MINIMIZE ANY POSSIBILITY OF FRADULENT ACTIVITY



Function and Purpose
Special Investigative Unit (SIU)

Deter
Detect
Investigate
Defeat insurance fraud

The SIU also functions as the enforcer of the requirements to train personnel and business partners to do the same.

Overview
Fraud Detection &
Documentation Procedures for referring potential fraud to the SIU

- **Remembering the “Red Flags” that may indicate fraud, be alert when reviewing any enrollment applications, group applications, commission applications, claims, etc.**

- **If you suspect that something is not correct, you are to immediately notify your immediate supervisor or Department Supervisor.**

- **Upon review of all of the information provided, the Supervisor will contact the appropriate persons to review.**

Overview
Fraud Detection & Documentation Procedures for referring potential fraud to the SIU

For possible fraud issues with regard to our FSL Commercial programs, the FSL SIU form will be completed and submitted, as required, by the QA Director. All applicable documents should be sent with the SIU form.

For fraud issues regarding our government programs, the guidelines established by the particular health plan regarding reporting to the appropriate OIG or Health Plan Fraud Waste and Abuse Officer shall be followed.

Contact Information for Fidelity Security Life Insurance Company's SIU :

Stephen Boinski
SIU Director

Special Investigative Unit, Fidelity Security Life Insurance Company

Attn.: Steve Boinski, SIU Director
3130 Broadway
Kansas City, MO 64111
(816) 756-1060, ext. 1690
antifraud@fslins.com

Contact Information for Health Partners SIU :

SIU REFERRAL HOTLINE IS:
(866) HP-SIU-4U (866-477-4848)

Special Investigative Unit at Pennsylvania DPW
(MCO Provider Compliance Hotline) number is:
(866) DPW-TIPS (866-379-8477)