



CONFIDENTIAL

Waste, Abuse, and Fraud Prevention Compliance Plan

In meeting client expectations compliant to appropriate state and federal regulations, ValueOptions of Texas, Inc. submits the following Waste, Abuse, and Fraud Prevention Compliance Plan.

Revision History

Date of Revision:	Revision Made By:	Revision (s)	Version Number:
November 1, 2011	McKenzie Frazier	Formatting; Added Content	Version 1.0 - SFY 12
November 9, 2011	McKenzie Frazier	Added Content	Version 1.1 - SFY 12
December 18, 2011	McKenzie Frazier	Revised Content	Version 1.1 – Amend - SFY 12
June 1, 2012	McKenzie Frazier	Formatting; Added Content	Version 1.2 - SFY 13
August 9, 2013	McKenzie Frazier	Revised Wording; Corporate Retention Policy LC313 and LC313A Added	Version 1.2 - SFY 14
March 19, 2014	McKenzie Frazier	Revised Content	Version 1.3 - SFY 15
April 29, 2015	Adam Fields	Revised Content	Version 1.4 - SFY 16

ValueOptions of Texas' Compliance/Program Integrity Department maintains the original electronic version of this document. Any changes or revisions made are the responsibility of the Compliance/Program Integrity Department.

Texas - NorthSTAR
Waste, Abuse, and Fraud Prevention Compliance Plan – SFY 2016

Table of Contents

	<u>Page</u>
I. INTRODUCTION	4
II. PLAN OVERVIEW	4
III. PURPOSE AND SCOPE	5
IV. DEFINITIONS	5
V. COMPLIANCE PLAN CRITERIA	7
VI. FRAUD AND ABUSE CRITERIA	10
VII. FRAUD AND ABUSE REPORTING AND INVESTIGATING	11
VIII. PHARMACY BENEFITS MANAGER	13
IX. COMPLIANCE AUDIT PROCESS	17
X. DISCIPLINARY ACTIONS/CORRECTIVE ACTION PROTOCOL	18
XI. COMPLIANCE/PROGRAM INTEGRITY UNIT	18
XII. SUMMARY	19
XIII. ATTACHMENTS	
a. STAFF LETTER	
b. SUBCONTRACTORS AND MEMBERS LETTER	
c. TEXAS NORTHSTAR COMPLIANCE ORGANIZATIONAL CHART	
d. LC101B - FRAUD & ABUSE PREVENTION AND DETECTION POLICY	
e. HHSC-OIG MCO-SIU PROVIDER ENFORCEMENT & RECOVERIES POLICIES	
f. LC313 - DOCUMENT RETENTION POLICY	
g. LC313A - DOCUMENT RETENTION SCHEDULE	

Texas - NorthSTAR

Waste, Abuse, and Fraud Prevention Compliance Plan

I. INTRODUCTION.

It is the policy of ValueOptions of Texas, Inc. (“TXNS”), and ValueOptions, Inc. (“VO”), to comply with all laws governing its operations and to conduct business in keeping with legal and ethical standards. It is also the policy of TXNS to deal with employees and behavioral health recipients using the highest clinical and business ethics as well as to maintain a culture which promotes the prevention, detection and resolution of possible violations of laws and unethical conduct. Compliance is a priority built into all levels of operations. This plan is reviewed annually and as needed by the VO National Director of Compliance, VO National Director of Program Integrity and/or the Texas Compliance Committee. Necessary revisions are forwarded to the Texas Health and Human Services Commission – Office of Inspector General (HHSC-OIG), the Texas Department of State Health Services (TX-DSHS), and the North Texas Behavioral Health Authority (NTBHA) for approval.

TXNS supports the government in its goal to decrease financial loss from false claims and has as its own goal, the protection of the State of Texas through the reduction of potential exposure to fraud, waste and abuse. TXNS shall operate its anti-fraud program under the direction of the VO National Legal & Compliance Department. TXNS shall have access to an array of resources to support its compliance efforts and to implement an anti-fraud plan. TXNS shall also have a Compliance/Program Integrity Department and Compliance Committee vested with the appropriate authority to administer the fraud and abuse program.

II. PLAN OVERVIEW.

The reporting of suspected fraud and abuse is intended to avoid the misappropriation of Federal, State, and Local funds. In the context of this plan, fraud is considered an act of purposeful deception committed by a person or behavioral health provider to gain an unauthorized benefit. Abuse committed by a behavioral health provider means activities that are inconsistent with standard fiscal, business, or medical practices, and that result in unnecessary costs to the TX-DSHS programs. Persons receiving care in the behavioral health system can also commit acts of abuse (e.g., by loaning or selling their identification cards).

Behavioral health providers must be cognizant of suspected fraud and abuse within the public behavioral health system. When detected, behavioral health providers are obligated to report such occurrences to TXNS or the appropriate state entity. Fraud and abuse can result in the misuse of Federal and State funds, can jeopardize the care and treatment of persons receiving behavioral health services, and can result in monetary fines, criminal prosecution, termination of providers, and prohibition from participation in Medicare/Medicaid Programs. Procedures to report suspected cases of fraud and/or abuse for behavioral health providers who are contracted with TXNS are included herein.

TXNS distributes annually a memorandum and requires training regarding TXNS Waste, Abuse, and Fraud Prevention Compliance Plan for all engagement center employees. The memorandum instructs employees to use due diligence regarding suspected fraudulent activities and explains how to report suspected fraudulent activities that could jeopardize the integrity of the benefits program or VO. The memorandum further explains that there is zero tolerance for improper business conduct or fraudulent behavior. Waste, abuse, and fraud

issues that may result in the potential loss of State property, monies, assets or associated confidential information must be reported to HHSC-OIG and TX-OAG-MFCU.

III. PURPOSE AND SCOPE.

The purpose of the TXNS Waste, Abuse, and Fraud Prevention Compliance Plan is to develop a mechanism to prevent and detect fraud, waste, or abuse in the behavioral health system under the scope of the TXNS contract with the TX-DSHS, through effective communication, training, review, and investigation. It is intended to be a systematic process aimed at ensuring that TXNS and its subcontractors comply with applicable laws, regulations, and standards in addition to contractual obligations. The TXNS Waste, Abuse, and Fraud Prevention Compliance Plan serves as a guiding document in the development, implementation, evaluation and maintenance of all related fraud and abuse operations and procedures, and it establishes a process for identifying and reducing risk and improving internal controls.

IV. DEFINITIONS.

Abuse – provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the Medicaid program, or in reimbursement for services that are not medically necessary, or that fail to meet professionally recognized standards for health care. It also includes recipient practices that result in unnecessary cost to the Medicaid program (42 CFR 455.2).

Elements of Abuse:

- Inconsistency (pattern of not following known laws, rules, regulations, contracts or industry practices/procedures);
- Costs (unnecessary loss of money to a governmental program);
- Medically unnecessary/does not meet standards (general disregard for professional or industry standards and practices).

Dispute – a request made by a provider or member for a neutral party to review an adverse action taken by TXNS to determine whether the action complied with the Medicaid laws, regulations, and/or policy. The dispute shall be governed by TX-DSHS' regulations and any and all applicable laws and court orders.

Claim – an itemized statement requesting payment for services rendered by health care providers (such as hospitals, physicians, or other professionals, etc.), billed electronically or on the CMS 1500, and/or UB-92.

Company – partnership of ValueOptions, Inc. (VO) and ValueOptions of Texas, Inc., established as ValueOptions NorthSTAR (TXNS).

Compliance Plan – same as anti-fraud plan, waste, abuse, and fraud prevention compliance plan, or program integrity plan.

Covered Service – medically necessary behavioral health and case management services for Medicaid and Indigent members as described in Article VII of the TXNS Contract (No. 2012-039051).

Disclosing Entity – a Medicaid provider (other than an individual practitioner or group of practitioners), or a fiscal agent (42 CFR 455.101).

Federal Health Care Program – any plan or program providing healthcare benefits, whether directly through insurance or otherwise, that is funded directly, in whole or part, by the United States Government (other than the Federal Employees Health Benefits Program), or any State health care program (42 CFR 1001.2).

Fraud – the intentional deception or misrepresentation made by a person or entity with the knowledge that the deception could result in payment of an unauthorized benefit. It includes any act that constitutes fraud under applicable Federal or State law (42 CFR 455.2).

Elements of Fraud:

- The act (evidence of wrong-doing);
- Knowledge and intent (willfully intended to commit act – generally evidenced by a pattern of wrong-doing); and
- Benefit (some type of measurable benefit obtained from the act by the person committing the act).

HHSC-OIG – Texas Health and Human Services Commission – Office of Inspector General

Incidents – situations of suspected fraud and/or abuse, which have the potential for liability to the State of Texas, TX-DSHS, TXNS, or its subcontracted providers.

Knowingly, or knowingly and willfully – a person, with respect to information:

- (a) Has actual knowledge of the information
- (b) Acts in deliberate ignorance of the truth or falsity of the information; or
- (c) Acts in reckless disregard of the truth or falsity of the information; and
- (d) No proof of specific intent is required (42 CFR 402.3)

Material Violations – substantial overpayments or a matter that a reasonable person would consider a potential violation of criminal, civil, or administrative laws applicable to any Federal health care program for which penalties or exclusions may be authorized. A material deficiency may be the result of an isolated event, or a series of occurrences.

Medical Necessity – an item or service provided for the diagnosis or treatment of a patient’s condition consistent with community standards of medical practice and in accordance with Medicaid policy.

Medical Record – a single complete record kept at the site of the member’s treatment(s), which documents all of the treatment plans developed, medical services ordered for the member and medical services received by the member.

Member – an individual having current Medicaid or NorthSTAR eligibility who shall be authorized by TX-DSHS to receive behavioral health services.

NTBHA – The North Texas Behavioral Health Authority serves as the local behavioral health (mental health and substance abuse) authority for the entire NorthSTAR service area, and functions include planning, oversight, single portal authority functions, as well as a local problem solving resource that includes ombudsman services.

Preponderance of the Evidence – evidence that shows a fact to be proved is more probable than not.

Probable Cause – a reasonable ground for belief, based on the facts that fraud and abuse has occurred; more than mere suspicion.

Provider – an institution, facility, agency, person, corporation, partnership, or association enrolled with TX-DSHS which accepts as payment in full for providing benefits the amounts paid pursuant to a provider agreement with TXNS.

Provider Agreement – an agreement between a TXNS and a provider or TXNS’ subcontractor and a provider of behavioral health services, which describes the conditions under which the provider agrees to furnish covered services to TX-DSHS’ members.

Services – see covered service.

Service Authorization – the act of authorizing specific services or activities before they are rendered or activities before they occur (formerly called prior authorization).

State – Texas.

State Medicaid Fraud Control Unit – a unit certified by the Secretary as meeting the criteria of 42 USC § 1396b (q) and § 1002.305 (42 CFR 1001.2).

Subcontractor – any State approved organization or person who provides any function or service for TXNS specifically related to securing or fulfilling TXNS’ obligations to TX-DSHS under the terms of the TXNS Contract (No. 2012-039051).

TX-DSHS – Texas Department of State Health Services

TX-OAG-MFCU – Texas Office of Attorney General – Medicaid Fraud Control Unit

Under-coding – coding for a service rendered through the use of a code which pays/encounters at a lower rate than the service actually provided.

Up-coding – coding for a service rendered through the use of a code which pays/encounters at a higher rate than the service actually provided.

Utilization Management – the process of evaluating the necessity, appropriateness and efficiency of health care services against established guidelines and criteria.

Texas Administrative Code (“TAC”) – contains regulations of all of the Texas State Agencies.

Waste – thoughtless, careless expenditure, consumption, mismanagement, use or squandering of healthcare resources, including incurring costs because of inefficient or ineffective practices, systems or controls.

V. COMPLIANCE PLAN CRITERIA.

TXNS shall establish and maintain a Compliance Program that, to the extent applicable, conforms to the Compliance Program Guidance issued by the Office of the Inspector General of the U.S. Department of Health and Human Services and other relevant state compliance program guidelines that directly affect the operations of TXNS.

1. A clear commitment to compliance. TXNS, in partnership with VO, has adopted a standardized Code of Conduct. The Code of Conduct Handbook explains the Company’s commitment to ethical standards and sets expectations for all employees in achieving and maintaining these standards. Employees are trained on the Code of Conduct upon hire and periodically thereafter. Training includes review of the Code and the Compliance Program, various compliance related case studies and provides the opportunity for clarification and questions. At the conclusion of training, employees are required to certify that they have read and understand the Code, agree to abide by its principles and report any suspected or possible violations. The Code of Conduct may be updated periodically and establishes the ethical standards employees must uphold in critical areas and aspects of the Company’s operations.

2. Designation of a Director of Compliance/Program Integrity and Compliance Committee – Oversight. The day-to-day operations of the compliance/program integrity program and compliance plan shall be administered by the TXNS Compliance/Program Integrity Department, led by the VO National Director of Compliance and VO National Director of Program Integrity, who shall report directly to the VO Sr. Director of National Compliance and VO Sr. Director of National Program Integrity respectively. TXNS compliance/program integrity staff shall have appropriate qualifications and experience.

TXNS shall establish a Compliance Committee to provide oversight for the compliance program and be responsible for regularly reviewing the compliance plan, recommending and authorizing changes as needed and assuring that related TXNS policies and procedures are in accordance with the compliance plan. The Compliance Committee shall consist of representatives from primary departments including: Quality Management, Claims, Clinical, Information Technology, Network Operations, Credentialing, Provider Relations and Finance. It shall be chaired by the VO National Director of Compliance or designee (*42 CFR 438.608*).

The VO National Director of Compliance, VO National Director of Program Integrity and the Compliance/Program Integrity Department shall function independently of any other TXNS department and have several responsibilities, including, but not limited to:

- Establishing and maintaining all necessary policies and procedures to support the compliance plan;
- Conducting reviews and fields audits;
- Reporting findings to the TXNS Engagement Center Vice-President (“ECVP”) and Compliance Committee; and
- Reporting suspected fraud, waste and abuse to HHSC-OIG and TX-OAG-MFCU.

Committee member responsibilities include, but are not limited to:

- Reviewing new regulations affecting compliance issues and revising strategies accordingly;
- Reviewing new and ongoing compliance issues, including corrective action plans;
- Identifying suspected fraud and abuse issues that may put TXNS, TX-DSHS, the State of Texas, and the program at risk and developing strategies to avoid such problems;
- Understanding fraud and abuse procedures and to provide this information to each functional area and its employees to ensure effective communication and understanding regarding fraud and abuse detection and deterrence;
- Developing training programs that support the prevention and detecting of fraud and abuse;
- Reviewing the Compliance Plan annually to assure that it is meeting the needs, requirements and contractual obligations of TXNS relating to fraud and abuse;
- Assisting TX-DSHS and cooperating with any performance reviews to provide copies of all records and documentation arising out of TXNS’ performance of contractual obligations;
- Assist in the development of any corrective action plans required by TX-DSHS in the event a review identifies and deficiencies;
- At the request of any contracted or non-contracted providers, offer technical assistance and support, as needed;
- Developing/modifying contract language to support required federal and state laws/regulations; and
- Developing and monitoring audit processes and outlier reporting processes.

The Compliance Committee shall meet quarterly or as needed to review and discuss significant cases from the past period. Each committee meeting shall include an update from the VO National Director of Program Integrity on cases opened, cases closed, cases referred, new trends and new vulnerable areas along with updates on other functions of the Compliance/Program Integrity Department. All Compliance Committee discussions, findings, decisions, etc. shall be documented and signed by the VO National Director of Compliance and the TXNS ECVP.

It is important to remember the sensitive nature of the information and topics the Committee shall be discussing and to assure that each member does not share information on investigations outside of the Committee. In order for the Compliance/Program Integrity Department audits and investigations to be conducted properly and to maintain the integrity of any possible future civil or criminal actions taken against a subject, strict confidentiality must be maintained by the Committee and any related TXNS employee. On an annual basis, each Committee Member will sign a Confidentiality and Non-Disclosure Agreement as part of their compliance related duties of VO and its affiliates. Copies of these agreements will be kept by the VO National Director of Compliance.

If there are any revisions made to the Waste, Abuse, and Fraud Prevention Compliance Plan, TXNS employees will be notified within twenty (20) day of that revision.

3. Effective training and education programs. TXNS shall require all employees and providers to attend training on the Compliance Program; identifying fraud and abuse, reporting fraud and abuse; compliance-related policies, procedures, and standards; and the Code of Conduct.
4. Auditing and monitoring. To detect and discourage fraud and abuse, the Compliance/Program Integrity Department shall ensure that appropriate monitoring, reviewing, and auditing are performed. These activities, referred to generally as audits, shall be focused on identified high-risk areas and vulnerable processes and systems. Various and appropriate audit methods shall be used to provide a reasonable assurance of detecting fraud and abuse. The audit methods used shall include, but are not limited to:
 - Data Review, Verification and Validation;
 - Random and Targeted Field Audits;
 - Desk Reviews of Data and Documents.

The purpose of Compliance audits shall be to detect and correctly identify instances of suspected fraud, waste or abuse based on the totality of the circumstances, information and evidence. The audits shall be conducted in accordance with applicable laws, standards, policies and procedures and shall result in a report detailing findings of fact. The Compliance/Program Integrity Department shall not provide opinions or recommendations unless requested by the Compliance Committee. See the *Compliance Audit Process* section for additional information.

5. Effective lines of communication. VO, a partner of TXNS, maintains an Ethics & Privacy Hotline and other procedures to foster an open atmosphere for employees, members, and providers to report issues and concerns, free from retaliation. Employees and management are encouraged to ask questions and report any problems or concerns which they may have about the company or its operations. Employees may direct any questions or concerns to their supervisor, manager, operating unit executives, the VO National Director of Compliance, the VO National Director of Program Integrity, or any member of the Compliance Committee. In addition, employees, members, and providers may use the Ethics & Privacy Hotline or other communication systems to report issues or concerns which may require investigation to assure compliance with the requirements of the Compliance/Program Integrity Program and applicable laws. Written procedures are available to all

employees who may want advice on certain policies and procedures, or who wish to report actual or suspected violations of law or applicable company policies and procedures.

Effective lines of communication shall also be maintained between TXNS and all of its employees, agencies, subcontractors, providers and clients operating under the scope of the compliance plan. Communication shall be conducted using the best and most appropriate means available, by way of direct mail, telephone, e-mail, web-site and Committee meetings.

6. Internal investigation and disciplinary processes. TXNS may use internal processes to evaluate compliance, including, but not limited to, on-site review; interview of personnel involved in management, operations, finance, and other related activities; questionnaires developed to solicit impressions of a broad cross-section of employees; review of financial and compliance related documents; financial, claim, or record auditing; trend analyses that seek deviations in specific areas over a specific period of time. These investigations shall be reported to the Compliance Committee and any corrective action, if applicable, shall be developed for areas of non-compliance according to a corrective action protocol.
7. Response to identified offenses and application of corrective action initiatives. TXNS, with its legal counsel when necessary, shall promptly respond to and investigate all allegations of illegal or improper activities by its employees, agents, members, or providers, whether the allegation is received through the Ethics & Privacy Hotline or in any other manner. Following such investigation, TXNS shall use reasonable efforts to correct the problem and develop appropriate corrective action plans if necessary. See the *Fraud and Abuse/ Compliance Audit Process* section for additional information.
8. Advertising and Marketing. TXNS manages a NorthSTAR program for the TX-DSHS for a defined Medicaid and indigent population for seven (7) North Texas counties. Marketing and advertising has been limited to the enrollee handbook that is distributed via the enrollment broker for Medicaid and as requested by indigent consumers. Any advertising and marketing materials, including any informational materials targeted to recipients, utilized by TXNS will be complete and accurately reflect the information about TXNS.

VI. FRAUD AND ABUSE CRITERIA.

Unless otherwise directed, the following is the criteria TXNS shall use for determining if fraud or abuse is suspected.

At least one of the following criteria must be met:

- Evidence of knowing and intentional:
 - Duplicate billings;
 - Upcoding;
 - Miscoding;
 - Unbundling;
 - Misrepresentation of services;
 - Billing for services not rendered;
 - Evidence of false or altered documents;
 - Evidence of missing documentation;
 - Evidence of irregularities following sanctions for same problem;
 - Evidence of unlicensed or excluded professional or facility at time of services;
 - Evidence of management knowledge of fraudulent activity;
 - Reports of material irregularities by more than one reliable source.

And all of the following criteria must be met:

- Pattern of occurrence of irregularities;
- Actual loss to a governmental program;
- Loss would be considered material for nature and type of activity and provider.

Or at least one of the following criteria is met:

- Direct personal knowledge of fraudulent activity by known reliable individual;
- TXNS documented audit findings that show suspected fraud;
- Report showing evidence of suspected fraud from another government or law enforcement agency.

VII. FRAUD AND ABUSE REPORTING AND INVESTIGATING.

Upon receipt of TXNS internal reports or its own reasonable indications of suspected noncompliance, the Compliance/Program Integrity Department shall investigate the allegations to determine whether a material violation of applicable law or the requirements of the Compliance Program has occurred. If it is determined that there is a current deficiency or area of noncompliance, the Compliance Department shall oversee the development of a corrective action plan to resolve the problem. The corrective action plan may include the appointment of a task force, the engagement of legal counsel and, in certain circumstances, the return of any overpayments and sanctions. TXNS shall notify HHSC-OIG if a problem is identified with the recoupment.

All instances of potential or actual fraud and abuse must be reported within thirty (30) business days of initiation of any investigative action by TXNS. Reports shall be sent to HHSC-OIG and TX-OAG-MFCU in writing via email or fax and shall include a detailed account of the incident, including names, dates, places, and suspected fraudulent activities (*See TAC Rule 353.502*). All instances of potential or actual fraud and abuse investigated and/or reported to, or by TXNS shall be logged and tracked by the VO National Director of Program Integrity and subsequently reported monthly to HHSC-OIG and TX-OAG-MFCU utilizing the reporting template specified by HHSC-OIG and outlined in the HHSC Uniform Managed Care Manual.

The log may include, but is not limited to:

- Case Number;
- Date Case Opened;
- Date Case Completed;
- Allegation(s);
- Source of Allegation;
- Time Period of Allegation;
- Provider Name;
- MCO Provider #;
- State Issued TPI # (if available);
- Provider Tax ID;
- Provider NPI;
- Description of Complaint / Allegations;
- Description of MCO Investigative Actions to Date;
- Description of Findings;
- Number of Client, Claims, Details, Dollars in Population;
- Number of Clients, Claims, Details, Dollars Found in Error;
- Number of Records Reviewed;
- Description of Actions Taken;
- Total Dollars Identified for Recovery;
- Overpayment \$-4-\$ or Extrapolated;

- Dollars Recovered to Date;
- Date of Final Recovery;
- Case Closed (Y or N);
- Date Case Closed; and
- Comments

Per TAC Rule 353.502, TXNS will conduct a preliminary investigation within 15 working days of the identification or reporting of suspected or potential waste, abuse, or fraud. During the preliminary investigation, TXNS will, at a minimum:

- Determine if TXNS has received any previous reports of incidences of suspected waste, abuse or fraud or conducted any previous investigations of the provider in question. If so, the investigation will include a review of all materials related to the previous investigations, the outcome of the previous investigations, and a determination of whether the new allegations are the same or relate to the previous investigation;
- Determine if TXNS has provided the service provider with any educational training in regard to the allegation;
- Conduct a review of the provider's billing pattern for suspicious indicators;
- Review the provider's payment history for the past three years, when available, for suspicious indicators; and
- Review the policies and procedures for the program type in question to determine if what has been alleged is a violation.

If fraud is suspected, an investigation shall be initiated and may include interviews and a review of relevant documents. During the investigation, the provider or member must allow access to originals or copies of all pertinent documents and to any data stored electronically and in the form specified by TXNS. A full investigation shall continue until sufficient evidence is gathered to determine, by a preponderance of the evidence that the alleged fraud and abuse has occurred, or has not occurred. All cases where fraud is suspected or detected shall be referred to HHSC-OIG and TX-OAG-MFCU prior to the initiation of any actions or recoupment efforts. TXNS shall cooperate with all fraud and abuse investigation efforts by TX-DSHS and other State and Federal entities and shall provide support to HHSC-OIG and TX-OAG-MFCU on matters relating to specific cases involving detected or suspected fraud. In addition, the Compliance/Program Integrity Department shall review the specific facts and circumstances to determine whether the problem is systemic and whether modifications to the Compliance Program are necessary or advisable to increase the likelihood that similar situations will be detected and prevented in the future.

Any contractor, subcontracted provider of care, or non-contracted provider who fails to report suspected fraud and/or abuse, has committed an act of unprofessional conduct and may be subject to disciplinary action by the appropriate professional regulatory board or department and shall be referred to the appropriate professional regulatory board or department.

Verification of Member Services. TXNS has an established process for the verification of member services (42 CFR 455.20). The process is conducted and overseen by the Compliance/Program Integrity Department.

The process is:

- TXNS verifies receipt of member services received based on claims paid for TXNS members to TXNS providers;
- The verification process occurs quarterly for a sample of the previous quarter's paid claims across multiple outpatient provider locations and is focused on suspicious billing activity and outliers;
Note: Inpatient verification is managed outside of this process as VO Clinical department conducts pre-authorization and daily continued stay review for Inpatient levels of care.

- The sample is pulled quarterly and notification letters are sent to members by the end of the month following the quarter being reviewed for services paid in the prior quarter;
- The member notification letter verify the following with the member:
 - Date of Service;
 - Facility/Provider Name; and a
 - Call back number for disputes or reporting potential fraud.
- TXNS' tracking process to determine the effectiveness of the verification of member services process includes the following elements, and occurs monthly:
 - Track the total number of notification letters mailed;
 - Track the total number of returned notification letters;
 - Track the total number of responses about the notification letters;
 - Track the total number of referrals made to SIU based on member's response to notification letters;
 - Track the total number of referrals made to HHSC-OIG and TX-OAG-MFCU based on member's response to notification letters;
 - Track the total number of complaints based on the notification letters.

SIU Referrals:

- The identifying staff member will refer potential cases of waste, abuse, and fraud to the National Director of Program Integrity as soon as possible.
 - Compliance/Program Integrity - SIU inquiry queue: D1TXCOMWAF.

Withholding Payment:

- Federal regulations under 42 C.F.R. § 455.23 (2011) make payment suspensions mandatory where an investigation of credible allegations of fraud exists under the Medicaid program.
 - TXNS with assistance from VO have a process in place to adhere to the aforementioned federal regulation.

Assigned Officer for reporting all investigations:

Adam L. Fields, CIA, CFE
 National Director of Program Integrity
 ValueOptions, Inc.
 240 Corporate Boulevard
 Norfolk, VA 23502
 Office: 602-903-0625
 Email: adam.fields@valueoptions.com

VIII. PHARMACY BENEFITS MANAGER.

Pharmacy Benefits Manager. TXNS contracts with CaptureRx and Navitus Health Solutions (“Navitus”) for pharmacy services. CaptureRx is the Pharmacy Benefits Manager (PBM) and Navitus is the entity that contracts with the pharmacies in TXNS’ network and pays pharmacy claims. The following includes Navitus’ definitions, process, and procedure for performing audits:

Pharmacy Audits: The Navitus Pharmacy Audit team is responsible for monitoring pharmacy compliance, verifying the integrity of claims submitted to Navitus, identifying instances of potential FWA and taking corrective action when errors are identified. The audit scope includes those risks identified internally by Navitus, as well as 16 FWA measures included on the High Risk Pharmacy Assessment List, produced quarterly by CMS.

Daily Claims Pre-Payment Review: Navitus monitors claims data daily to correct individual quantity and pricing errors on a pre-payment basis. This process educates Participating Pharmacies and helps reduce retroactive audit recoveries that may occur through a pharmacy desktop or onsite audit. Pre-payment review is conducted for certain medications and not all claims. The pre-payment claims review complements the desktop and onsite audit processes and is not intended to review all audit elements considered in a desktop or onsite audit.

During desktop and onsite audits, the audit team identifies certain drug categories or drug dosages that show patterns of incorrect billing. These identified drugs are then placed on the daily prepayment review report. This pre-payment review practice was implemented based on recommendations from the FWA Oversight Committee. Our audit team will then use this report to contact each pharmacy before payment is made to ensure the claim was submitted and processed accurately. In the event of an overpayment identification, Navitus will request that the pharmacy reverse and reprocess the claim. These types of pre-payment reviews also provide the audit team with vital information about a specific pharmacy that may have frequent instances of incorrect billing, resulting in the pharmacy being included on the desktop or onsite audit list.

Audit Selection: In addition to the patterns of frequent incorrect billing identified during prepayment audits, several other situations could trigger a desktop or onsite audit. These include:

- Request or inquiry by a client, plan sponsor, member or government agency;
- Pharmacy general billing history;
- Untimely or insufficient response to issues identified through the pre-payment inquiry or pre-payment daily claims review;
- Referral from the Navitus Compliance or SIU team;
- Routine audit of pharmacies selected on a random basis;
- CMS High Risk Pharmacy Assessment that includes 16 FWA measures

The Navitus audit plan is reviewed monthly and revised as needed based on new trends, recommendations from the Credentialing Committee, client needs, drug manufacturer alerts or CMS fraud, waste and abuse alerts.

Desktop Audits: Navitus performs desktop audits to remediate pharmacy billing errors; to identify potential FWA; and to educate pharmacists on billing practices that comply with federal and state requirements, the Pharmacy Participation Agreement and the Navitus Pharmacy Provider Handbook.

Navitus conducts a 100% post-payment audit using an audit software, called ClaimwiseRx, with algorithms that identify risks such as inappropriate billing, incorrect use of dispense-as-written coding, incorrect quantity, incorrect drug, or incorrect patient. This 100% review allows Navitus to identify if there is a safety impact or if error trends suggest potential FWA. If the algorithm shows an error, the audit team will then request the hard copy prescription from the pharmacy and compare the prescriber's request with the claim submission by the pharmacy. The post-payment audit is completed monthly.

Navitus performs additional pharmacy monitoring and auditing activities as risks are identified, including completion of FWA training and completion of the exclusion screening against the HHS/OIG and GSA lists.

Onsite Audits: Onsite audits are broader in scope than desktop audits. In addition to reviewing claims and identifying FWA, the onsite audit also considers operational deficiencies, and ensures the pharmacy is in compliance with the network contract, the provider handbook and state and federal regulatory requirements such as licenses and privacy.

During an onsite audit the auditor review items related to prescriptions, signage, licensing, medication, and other infrastructure compliance. The auditor provides the participating pharmacy with a written audit report,

which includes details of any discrepancies or relevant audit findings and education on the types of errors identified within the audit.

External Audits: Additionally, Navitus may contract with external auditors to support audit activities related to any of the areas identified above or to consider the effectiveness of internal controls since these controls are the operational tool to mitigate FWA risk.

Audits that assess the control environment consider the design, implementation, and effectiveness of the controls. The auditors also make recommendations on improvements. FWA controls may include: segregation of duties for financial reporting and auditing; authorization or review of transactions by appropriate person(s); retention of records; physical safeguards such as cameras or locks; IT security such as use of user names and passwords to ensure access is restricted to authorized personnel; system edits to check that data was entered accurately; accounting for transaction in numerical sequences; training and education; and management reviews of reports comparing actual performance versus plans or goals. Each year, Navitus engages an external and independent audit firm to conduct an SSAE 16 SOC 1 and SOC 2 audit (formerly known as SAS 70), to validate internal controls. Clients may request a copy of the most recent report by contacting the Navitus Chief Compliance Officer.

Investigations: When potential fraud is identified or suspected, the Navitus Special Investigation Unit (SIU) conducts a confidential investigation that will result in either no finding, or a potentially substantiated finding with a recommendation to the client. SIU investigators will sometimes collaborate with the pharmacy audit team to gather additional information necessary for a thorough investigation. This may include accompanying the auditor during an onsite audit or conducting interviews with the pharmacy staff. The SIU Investigator may also work with a client's SIU team to gather additional information as needed.

The SIU reports to the Associate Director of Compliance and Regulatory Affairs and is supported by other compliance staff. The SIU investigators are all certified fraud examiners.

Mechanisms: SIU uses a variety of mechanisms to detect and investigate FWA across all lines of business as well as detection of fraud schemes that may occur with downstream entities. Some of the activities include:

- Ensuring that appropriate policies and procedures are developed and disseminated annually;
- Working with the compliance staff to develop effective training programs and marketing materials for employees, pharmacies and vendors to identify the current FWA environment and how to recognize FWA schemes;
- Monitoring the FWA confidential hotline number and referral email account;
- Ensuring appropriate logging and tracking of referrals and allegations to help identify trends;
- Developing procedures and checklists to ensure Navitus responds to data requests from government authorities or law enforcement;
- Timely review and reporting of all FWA referrals or allegations of potential FWA received from through the email, online form or through the Hotline;
- Coordinating and cooperating with MEDICs, CMS, Medicaid Fraud Control Units (MFCU), State Attorneys General, State OIG, and law enforcement requests for information regarding potential fraud schemes; and
- Providing periodic trend reports to Navitus leadership to ensure investigation results are considered when developing and revising the Work Plan.

Referral Process: Referrals are submitted by members, pharmacies, prescribers, law enforcement, clients, and internal audit, among others. The SIU provides Navitus member services representatives with specific key indicators that might suggest FWA and protocols for how to refer this information to the SIU team. In addition to a free-flow text email, referral sources may also use a standardized referral form that is provided for internal use and includes specific information to aid the investigator in assessing the matter prior to a full

investigation. Once a referral is received, the case is triaged utilizing the SIU Triage Worksheet. The SIU triage process allows the investigator to quickly determine if the internal reporter has correctly identified potential FWA or if additional training might be appropriate. Additionally, the triage process allows for the prioritization of cases. An SIU hotline and email is posted on the Navitus website and included in all training materials and in the Pharmacy Network manual.

Investigative Process: SIU conducts standard investigations using accepted methods established by the Association of Certified Fraud Examiners (ACFE), The Institute of Internal Auditors (IIA), and the National Association of Drug Diversion Investigators (NADDI). The process includes:

- Gathering Evidence
SIU utilizes the Navitus Navi-Gate 3D system to run claims reports to gather evidence for an investigation. In addition, SIU may need to contact various internal and external sources for information. SIU will investigate all referrals from clients, government entities and law enforcement, and all referrals from member services related to external activities. For referrals of fraud, waste and abuse allegations related to Navitus employees, SIU will escalate the matter to the Chief Compliance Officer and a determination as to whether the matter will be investigated internally or outsourced will be made on a case-by-case basis.
- Analyzing Evidence Using Industry Best Practice Methods
To determine if allegations are credible SIU will analyze available data including contract Agreements, claims data, licenses, prior history, exclusions, and publically available documentation, policies and procedures and training.
- Validating or Substantiating the Allegation of FWA, by Considering:
 - Who is involved in the fraud;
 - Who made the allegation and why;
 - What the direct evidence supports;
 - Any indirect evidence that is present;
 - How long the activity has been in progress;
 - Whether the individual was trained or informed of appropriate practices; and
 - Internal control environment, including systemic controls.
 - Determining Recommendations for Mitigation and Corrective Action by Considering:
 - Patterns and likelihood of ongoing activities;
 - Ease of correction, e.g., Locked-in Program; and
 - Level of sophistication of activity.

Pharmacy Watch List: The Pharmacy Audit Team maintains a Watch List that includes the pharmacy name, NPI, NABP, address, Pharmacist in Charge (if available), the year and quarter the pharmacy was added to the list, and the reason why it was added. Pharmacies may be placed on the Watch List if they have been previously terminated from the Navitus network, if they are currently being monitored or investigated by Navitus for certain activities, if they are sanctioned or investigated by external agencies as result of an audit or allegation, or if they have a prior debarment, conviction, loss of license, or Board action. Pharmacies may also be placed on this list for identified industry reports. The Pharmacy Watch List is utilized internally by the pharmacy network area when credentialing new pharmacies or re-credentialing existing pharmacies. The Watch List helps prevent previously terminated pharmacies or pharmacies with potential to commit FWA from becoming part of the Navitus Participating Pharmacy Network again.

Prescription Verification Audit: Navitus' prescription verification audit is used to identify and validate that claims billed for prescription drugs were actually received by the member. The audit can also help to identify if drugs may have been returned to stock without crediting Navitus, or billed for a different strength or quantity than what was provided. Navitus' Audit team randomly surveys members that received a chosen medication within the audit timeframe. Survey results are tracked and investigated.

Data Analyses: Navitus uses data, such as prepayment claims data, pharmacy profile reports, and an Averages/Outlier report, to assist in monitoring and detecting potential FWA. Any analysis that raises a risk of FWA controls or suspected activity is referred to the Chief Compliance Officer.

IX. COMPLIANCE AUDIT PROCESS.

Periodic audits are conducted to ascertain compliance with applicable fraud and abuse requirements. These audits are used to ascertain that the compliance plan is being followed and focuses on risk areas which may be identified by the government from time to time. They include periodic claims sampling and documentation reviews to assess TXNS operations. The goal of the audits is to assure personnel competency and uncover improper claims activity (patterns of improper activity in particular, e.g., up-coding) before potential violations become significant enough to warrant government-imposed penalties. Feedback is provided to the individuals involved in the various phases of claim development and submission.

Specific controls TXNS shall have in place for the prevention and detection of fraud and abuse, include:

- Claim edits – The VO claims system, utilized by TXNS, shall perform validation edits that include, but may not be limited, to the following:
 - Service authorization – Certain services must be prior-authorized to receive payment;
 - Valid dates of service – the system assures that dates of services are valid dates and not in the future;
 - Duplicate claims – the system automatically informs the provider that the current claim is an exact or possible duplicate and denies that claim;
 - Covered service – the system shall verify that a service is a valid covered service and is eligible for payment under TX-DSHS' behavioral health benefit for that eligibility group;
 - Provider validation – the system approves for payment only those claims received from providers that would have been paid in the absence of other primary insurance coverage for Medicaid and Indigent covered services;
 - Eligibility validation – the system confirms the member for whom a service was provided was eligible on the date the service was incurred;
 - Quantity of service – the system validates claims to assure that the quantity of services is consistent with TX-DSHS' rules and policy;
 - Rejected claims – the system determines whether a claim is acceptable for adjudication and reject claims that are not;
 - Managed care organizations (MCO)– the system rejects claims that should rightly be processed and paid by a member's MCO for any and all physical health treatments;
 - Other insurance coverage – the system rejects claims that should rightly be processed by a member's primary health care carrier;
 - Service limits – the system verifies that a service is not covered outside of TX-DSHS' established service limits, including but not limited to once in a lifetime procedures; and
 - Correct payment amounts – the system pays the claim at the lesser of the billed amount or VO' allowable amount, other third party pay coverage, etc.
- Post-processing review of claims – TXNS produces reports that show overlapping dates of service to determine if any claims have been submitted and were adjudicated for services that did not fail the claim edit logic.
- Provider profiling and credentialing – All providers must be registered with TX-DSHS with the appropriate provider type and categories of service and be credentialed by VO prior to contracting or entering into a single-case agreement.
- Contract provisions – the TXNS provider agreement requires providers to report any incidents of suspected fraud or abuse to TXNS.
- Training for employees – During new-employee orientation and in regular training, meetings and/or

forums, employees receive training on fraud and abuse.

- VO and TXNS maintain a training log for all training pertaining to waste, abuse and/or fraud in Medicaid. The log includes the name and title of the trainer/facilitator, names of all staff attending the training and the date and length of the training. The log will be provided upon request from the TX-HHSC-OIG, TX-OAG-MFCU, and OAG-Civil Medicaid Fraud Division (CMFD), and the United States Health and Human Services-Office of Inspector General (HHS-OIG). (*1 TAC 353.502 (Medicaid)*)
- Member and subcontracted provider training and education – Fraud and abuse training shall be made available to providers routinely and at least annually.

X. DISCIPLINARY ACTIONS/CORRECTIVE ACTION PROTOCOL.

In order to fully benefit from the detection of material mistakes, inaccuracies and instances of fraud and abuse, TXNS shall take corrective action with those relevant individuals and/or organizations. If directed by the Compliance Committee and in coordination with TX-DSHS, TXNS may also recommend a process for improving the systems involved. Corrective actions recommended by TXNS for its providers may include, but are not limited to:

- Repayment of funds;
- Fines and sanctions;
- Mandatory remedial training;
- Referral to law enforcement for criminal investigation and prosecution;
- Referral to other regulatory authorities; or
- Termination of contract.

If the results of an initial or follow-up audit disclose claims/encounters without adequate supporting documentation, those claims/encounters shall be reversed and the funds shall be recouped.

Upon completion of an audit, the total number of claims/encounters in error (undocumented encounters, correctness issues and timeliness issues) is divided by the total number of claims/encounters reviewed in the sample to determine the error rate. ValueOptions has established an audit error rate threshold of 10% to determine whether the *provider/participating provider* had accurate, complete and timely claim/encounter submissions for the audit review period. The audit error rate and the corresponding audit findings are utilized to determine necessary corrective actions.

Provider error rates shall be maintained and tracked to indicate an overall performance level. The Compliance Department shall routinely review these trends and report consistent noncompliance to the Compliance Committee as necessary.

XI. COMPLIANCE/PROGRAM INTEGRITY UNIT.

McKenzie Frazier, M.H.S.A., CFE, CPCO is the VO National Director of Compliance and Adam L. Fields, CIA, CFE is the VO National Director of Program Integrity. In these positions, Mr. Frazier and Mr. Fields have access to all aspects of the activities performed by TXNS for the State of Texas as the NorthSTAR Contract holder. They are in the best position to implement processes articulated in this Waste, Abuse, and Fraud Prevention Compliance Plan.

The National Director of Program Integrity serves as the primary point of contact for the HHSC-OIG and their authorized representatives. All questions regarding the administration of this Plan and TXNS' compliance with this Plan should be first directed to the National Director of Program Integrity. Where contacting TXNS prior to or during an investigation does not compromise an investigation, HHSC-OIG, TX-OAG-MFCU, TX-

DSHS, and NTBHA should include the National Director of Program Integrity in all communications with the TXNS staff.

XII. SUMMARY.

The TXNS Compliance Plan confirms the establishment of a VO National Director of Compliance, a VO National Director of Program Integrity, a Compliance Committee, and a program for effective training and education, auditing and monitoring. Effective and clear lines of communication have been established and internal investigation and disciplinary processes developed. Specific controls have been set in place to prevent and detect fraud and abuse, and procedures for the reporting of fraud and abuse are in place. TXNS has established a clear commitment to compliance.

As the foundational document for TSNS' fraud and abuse control activities, this compliance plan shall be reviewed and amended as necessary. The Compliance Committee Chair (representing the Compliance Committee) shall direct the Compliance/Program Integrity Department in regards to any revisions and shall have final approval for all changes.

CONFIDENTIAL