DOCTORS
HEALTHCARE PLANS, INC.

COMPLIANCE PROGRAM

2026

TABLE OF CONTENTS

GOAL OF THE COMPLIANCE PROGRAM

Doctors HealthCare Plans, Inc. (DHCP) believes everyone has a role in compliance. Just like coming to a complete stop at a STOP sign, doing the right thing for the right reason means being ethical even when no one is watching. DHCP is committed to creating a workplace environment in which high ethics becomes the guiding principle modeled by each employee, every day.

Embracing this principle will enable all employees, senior leaders, board members, and other individuals associated with the plan, including providers, First Tier Downstream providers and vendors in the proactive identification and reaction to noncompliance that can have an adverse impact on the business objectives of DHCP. The DHCP Compliance Program reinforces our compliance culture where integrity and professionalism are not only encouraged but expected in all business functions. DHCP encourages the use of the Compliance Reporting Mechanisms (which includes anonymous reporting) and communication with upstream leaders and/or the Health Plan Compliance Officer without fear of retaliation.

The scope of the Compliance Program includes both internal and external requirements. DHCP is committed to comply with all federal and state standards. With the support of the Board of Directors, the CEO, DHCP Quality Improvement Committee and the Compliance Committee, the Compliance Officer holds the authority to oversee the effectiveness of the Compliance Program. DHCP has implemented measures which prevent, detect, and correct non-compliance with CMS program requirements.

The Compliance Program incorporates the seven fundamental elements of an effective Compliance Program that align with the Centers for Medicare & Medicaid Services (CMS) compliance requirements noted in Chapter 21 of the Medicare Managed Care Manual and Chapter 9 of the Prescription Drug Benefit Manual.

The Compliance Program is operationalized through the mechanisms described including establishing:

I. Written Policies, Procedures and Standards of Conduct
II. Designation of a Compliance Officer and Compliance Committee,
III. Effective Training and Education
IV. Effective Lines of Communication,
V. Well publicized disciplinary guidelines,
VI. Effective System for Routine Monitoring, Auditing and Identification of Compliance Risk
VII. Procedures and System for Prompt Response to Compliance Issues

Implementation of the Doctors HealthCare Plans, Inc. Compliance Program was established and adopted by the Compliance Committee and Board of Directors.

Last Approvals:
Compliance Committee Approved 11/11/2022
Board of Directors Approved:

ELEMENT I

Written Policies, Procedures and Standards of Conduct

The Organization maintains Operational and Compliance Policies and Procedures that articulate DHCP's commitment to comply with all applicable federal and state standards. These documents demonstrate the Plan's commitment to conduct business in a sound and ethical manner. The Compliance Program is comprised of a written program document, Code of Conduct, and Policies & Procedures. The organization has comprehensive system-wide written Policy and Procedures available to all associates on demand, via the corporate drive (P Drive) and Inovaare; the Plan's compliance platform.

a. Code of Conduct (The Code)

DHCP has developed and maintains Standards of Conduct (Code of Conduct) which articulates the commitment to doing business in a lawful and ethical manner. It is designed to guide employees, board members and business partners in upholding our high standards of fair and ethical practices, in identifying potential noncompliance and FWA, and reporting them through appropriate mechanism so issues are addressed and corrected. All employees, consultants and board members must read and sign an acknowledgment that they agree to abide by the Code as compliance is everyone's responsibility from the top to the bottom of the organization. The Code of Conduct is available for review by employees on the corporate drive (P Drive) and Inovaare Platform as well as company website.

DHCP requires that providers and FDRs abide by the Code of Conduct or implement their own that incorporates standards of compliance and requirements similar to the DHCP Code of Conduct and that comply with 42 CFR 438.608.

b. Compliance Policies and Procedures

DHCP has developed Compliance Policies and Procedures to ensure controls are in place to meet specific requirements of the Medicare program, including the Dual Special Needs Plans Medicaid requirements and operate the Compliance Program. The policies can be found in the corporate drive (P Drive) and Inovaare Platform. The Policies and Procedures support the Medicare Compliance Program and work in conjunction with department polices developed by and used on a day to day-to-day basis by DHCP business areas. The DHCP Compliance Officer manages the Organization's Compliance Policies which include but not limited to:

- Code of Business Conduct
- Fraud Waste and Abuse
- Compliance Training
- Compliance Helpline and Email
- Compliance Committee Structure
- Marketing and Communication Material Review and Filing with CMS
- Auditing and Monitoring
- Regulatory, Law Enforcement and Media Inquiries
- Part C and D Required Reporting
- Website Administration
- Sales Agent Allegation Investigation
- Record Retention Policy
- Non-Retaliation/Non-Intimidation
- Disciplinary Action for Associates Who Have Failed to Comply
- Compliance Baseline Risk Assessment and Work Plan Policy
- Compliance Investigations
- CMS Self-Reporting
- HPMS Access
- Excluded and Sanctioned Providers
- HPMS Access Changes with Applicable Law Regulations

- » Part C and D Required Reporting
- » Delegation Oversight Part C
- » Delegation Oversight Part D

c. Sales & Marketing Reviews

Compliance is also responsible for reviewing Sales and Marketing materials. Marketing materials will be developed by the Sales & Marketing team and DHCP will market and advertise accurately, fairly, truthfully and ethically and in compliance with laws and regulations. DHCP employees, providers, vendors, suppliers must follow laws, rules and regulations and policies and procedures when marketing or communicating (i.e., Chapter 3 – Medicare Communications and Medicare Marketing Guidelines, AHCA).

d. HIPAA Compliance

Member personal and protected health information is protected by the Health Insurance Portability and Accountability Act (HIPAA), HIPAA Privacy and Security Regulations 45 CFR 164, The Health Information Technology for Economic and Clinical Health Act (HITECH Act) and State Confidentiality Laws. DHCP is committed to full compliance with regulatory requirements related to health care privacy and security.

Privacy Rule/Privacy Program

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. DHCP limits use and disclosure of PHI to minimum necessary to accomplish the intended purpose. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. DHCP Compliance Officer serves as Privacy Officer and oversees the privacy program which is comprised of different policies and procedures that ensures limited access to information and that patient rights are protected. This includes but not limited to:

- » Privacy Officer
- » Notice of Privacy Practices
- » Authorization for Disclosure of PHI
- » Discontinuation of Authorization for Disclosure
- » Business Associates
- » Privacy Complaint
- » Request for Amendment
- » Inspection and Copy
- » Access of Controls
- » Accounting of Disclosure
- » Visitors and Guests
- » Request to Restrict
- » Request for Alternate Communication
- » Clean Desk, Clear Screen

Security Rule/Security Program

The Security Rule and the Privacy Rule are closely interconnected. While the Privacy Rule established standards for who may have access to PHI, and for what purposes, the Security Rule created the standards for ensuring that only those who should have access to ePHI will in fact have access. The purpose of the of the HIPAA Security Rule is to specify the safeguards that need to be implemented to protect PHI from misuse. Security Rule applies to ePHI. DHCP IT Director serves as Security Officer and oversees the Security program which ensures processes to protect against any reasonably anticipated threats or hazards to the security of ePHI, and any reasonably anticipated uses or disclosures of such information. Policies include but not limited to:

- » Information Security Policy
- » Information Security Awareness
- » Information Security Functions & Responsibilities
- » New Employee Security Orientation
- » Computer Security Violation Reporting
- » Passwords Control
- » Remote access
- » Internet Access
- » Data and Software Access Control
- » Portable Computer Security Considerations
- » Encryption
- » Email Security and Electronic Information
- » HIPAA Transaction and Code Set Standards
- » Information Security Incident Response

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 included a series of modifications to the HIPAA privacy and security standards. Many of the changes were enacted to address the concerns of privacy advocates and other stakeholders. The HITECH Act created a notification requirement for breaches of unsecured (i.e., unencrypted) PHI, increased the civil monetary penalties for violating HIPAA, and expanded and strengthened enforcement activities by the Office for Civil Rights. It also made business associates of covered entities (i.e., companies and consultants with whom covered entities share PHI to help them operate) directly liable and subject to civil and criminal penalties for HIPAA violations.

e. Distribution of Compliance Policies and Procedures and Standards of Conduct

DHCP maintains, at all times a designated full-time Compliance Officer (CO) qualified by knowledge and training, and experience in healthcare or risk management, to promote, implement, and direct the overall compliance program and to oversee the DSNP's compliance with non-discrimination requirements in this DSNP State contract. The CO exhibits knowledge of relevant regulations, provides expertise in the compliance processes and is qualified to design, implement, and oversee a fraud and abuse prevention program. The FWA program is designed to ensure program integrity through fraud and abuse prevention and detection, which identifies and addresses emerging trends of fraud, abuse, and waste, pursuant to the Medicare MA and State's DSNP contract; as well as State and federal law. The CO is dedicated 100% to the DHCP Medicare Advantage Contract, including the applicable State's DSNP Contract. The CO shall be accountable to Senior Management and the DHCP Board of Directors.

Policies and Procedures are provided to all employees via the P Drive and Inovaare platform within 30 days of hire, when there are updates to the policies, and annually thereafter. Documents are placed on the P Drive for access anytime as well as Inovaare platform and employees will receive information from Compliance annually with the updated Standards of Conduct to review and sign. FDRs and business partners will be notified during the pre-delegation/pre-implementation process that the Standard of Conduct is available on the website for anytime access and should be adhered too. FDRs may also utilize their own comparable policies and procedures, Standards of Conduct, and training. This will be collected for review during the pre-delegation process and annually thereafter. The plan may periodically audit FDRs and review compliance policies and procedures, training, and Standards of Conduct. FDRs are required to keep proof of training such as copies of sign-in sheets, employee attestations, and/or electronic certifications from employees taking and completing training. DHCP requires FDRs to maintain records of employee training for a period of ten (10) years.

ELEMENT II

Compliance Officer, Compliance Committee and High-Level Oversight

a. Compliance Officer

Mayra R. Campuzano, Vice President, Compliance Officer (CO) reports directly to the Chief Executive Officer (CEO) and is appointed by Board of Directors. The Compliance Officer has unrestricted, direct access to the Board of Directors. The CO is a full-time employee and is responsible for the day to day operations of the Compliance Program and on behalf of the Compliance Committee will provide periodic reports to the Board of Directors on the activities and status of the Compliance Program. The Compliance Officer works in conjunction with the executive team, Compliance Committee, and management staff to implement the Compliance Program. The activities reported will include but not be limited to compliance internal metrics, audit statuses, delegate quarterly reports, educational and training programs, and issues reported via the Plan's Compliance Help-Line. Other issues reported to FWA will be investigated and resolved by the SIU with the help of the CO if needed. The CO has full authority to access all documents relevant to compliance activities, interview employees and other relevant individuals regarding compliance issues, and will work with SIU to report potential FWA to CMS, law enforcement, or regulatory agencies.

b. Compliance Committee

The DHCP Compliance Committee is comprised of senior leaders, members from the Board of Directors and the CO who serves as the Chair of the committee. Compliance Committee members have decision making authority for the organization as it relates to Compliance and serve to advise the CO. The Compliance Committee will be responsible for the implementation, operation, and oversight of the Compliance Program. The Compliance Committee is responsible to ensure sufficient funding and support for DHCP Compliance Program. The Compliance Committee meets at least on a quarterly basis, or more frequently as necessary and is accountable to DHCP Board of Directors. The Compliance Officer provides information to the DHCP Board of Directors and meets as needed.

c. Governing Body

The Board of Directors remains responsible for the content and operation of the Compliance Program and must exercise reasonable oversight with respect to the implementation and effectiveness of the Compliance Program. The Compliance Program functions under the direction of the Board of Directors, which is the governing body responsible for the overall effectiveness of the Compliance Program. The Board of Directors delegates Compliance Program activities to the Compliance Officer who reports into the CEO and Compliance Committee.

d. Senior Management Involvement in Compliance Program

The CEO and senior management recognize the importance of the Compliance Program. In addition, the CEO and senior management ensure the CO is fully integrated into the organization and has the credibility and authority to operate the compliance program.

ELEMENT III

Effective Training and Education

DHCP implements and provides effective training and education for its employees, the CEO and senior management, for the Board of Directors, and FDRs. Training occurs upon hire and annually thereafter.

Compliance training may be delivered via the KnowBe4 training platform that tracks training completion dates and retains completion of training attestations. Through this platform, DHCP staff receive multiple reminders of pending trainings to ensure compliance. Understanding of concepts presented in the training modules is measured via quiz questions required to be taken and passed with a satisfactory score. The completion of trainings and test results are maintained in the system, allowing for a process to verify training completion.

a. General Compliance Training

Compliance training includes:

- Code of Conduct
- Confidentiality
- Doctors HealthCare Plans Compliance Program
  - Fraud, Waste and Abuse
  - Privacy and Security
- Conflict of Interest
- The Employee Handbook and Risk Management are also required trainings.

The successful completion of DHCP Compliance Training is required as an ongoing condition of employment. New Hire Compliance Training must be completed within the first 30 days of the employees' effective start date of employment. Employees completing the Annual Compliance Training requirement will have 60 days from the initial training notification to complete training. Employee's that are not working due to family medical leave (FMLA), disability, and/or worker's compensation during the annual training period will have 30 days upon return to complete the required Annual Compliance Training. Regular paid time off is not considered as an exception to the training requirement.

All first tier, downstream and related entities that provide services to Medicare Advantage enrollees are required to complete compliance and fraud, waste and abuse training. Contracted providers and FDRs have the option of conducting their own training.

Compliance Training is an ongoing activity. Remember, all employees are responsible for the effectiveness of DHCP Compliance Program. As with the New Hire and Annual Compliance Training, the training content will be reviewed and updated to reflect changes in law and regulatory policy.

The CO will be responsible for the ongoing training of themselves and their staff(s) by attending conferences and webinars, subscribing to publications and OIG's email list, monitor OIG's website, and network with peers to stay up-to-date and get ideas. Training related documents will be maintained by DHCP for a period of ten (10) years. Examples of proof training has occurred include but is not limited to: training agendas, attendance logs, and individual assessment scores.

b. Fraud, Waste, and Abuse Training

Employees will receive FWA training within 30 days of initial hire, and annually thereafter, and as much as deemed necessary. DHCP has implemented measures to detect, prevent, and correct Fraud, Waste, and Abuse. Measures are outlined in the company's Fraud Waste and Abuse Program. The FWA Program includes initial background checks for all potential employees and Board Members via the National Criminal Database. In addition, employee, physicians, and FDRs are reviewed prior to hiring or contracting of any new associate, Board of Director member or FDR monthly against CMS Preclusion List, Office of Inspector General (OIG) List of Excluded Individual and Entities and the System for Award Management (SAM) and Agency for Health Care Administration.

DHCP maintains a FWA email (reportfraud@doctorshcp.com) and hotline (833) 342-7911 for anonymous reporting. All reports of potential FWA will be investigated. DHCP will work with designated State and Federal agencies, the National Benefit Integrity Medicare Drug Integrity Contractor (MEDIC) and law enforcement to pursue individuals or organizations who may be involved in activities that fall under the FWA umbrella and will pursue prosecution of health care fraud and abuse.

Actual or suspected fraud or other misconduct is a violation of the DHCP Code of Conduct. It is the duty of an employee or affiliates acting on behalf of DHCP to report actual or suspected misconduct. If an employee or an affiliate is contacted by law enforcement or other government agencies, such contact should immediately be reported to the Legal Department and to the Compliance Officer.

ELEMENT IV

Effective Lines of Communication

DHCP works diligently to foster a culture of compliance throughout the organization by regularly communicating the importance of performing jobs in compliance with regulatory requirements and reinforcing the company expectations of ethical and lawful behavior. DHCP has established and implemented effective lines of communication while ensuring confidentiality. A primary role of the CO is to ensure a culture of compliance and compliance awareness within DHCP. Every day Compliance is accomplished through the messaging delivered by the CO and by the visible presence of the CO in the operational areas of the organization.

a. Effective Lines of Communication Among the Compliance Officer, Compliance Committee, Employees, Governing Body, and FDRs

DHCP provides resources that enable employees to have open lines of communication between the CO and the employees to ensure easy access to ask questions and/or report compliance concerns. Open lines of communication are also encouraged for members of the compliance committee, managers and the Board of Directors as well as first tier, downstream, and related entities.

b. Communication and Reporting Mechanisms

Resources include:

» Reporting issues to **supervisor, others on the management team**

» Reporting issues to the **Compliance Email** (compliance@doctorshcp.com), **Compliance Help Line Phone** (833) 500-3427, **Compliance Help Line Fax** (786-578-0294), **Compliance mailing**

(Doctors HealthCare Plans, Inc., Attn: Compliance Department, 2020 Ponce de Leon, Blvd, PH 1, Coral Gables, FL 33134) or **website forum on the Contact Us page**. All lines of communication are confidential, toll-free resources available 24 hours a day, 7 days a week to report violations or raise questions or concerns related to compliance. All may be made anonymously.

» Reporting issues the **FWA Email** (reportfraud@doctorshcp.com), **FWA Help Line Phone** (833) 342-7911, **FWA Help Line Fax** (786) 628-2600, **FWA mailing** (Doctors HealthCare Plans, Inc., Attn: Special Investigations Unit, 2020 Ponce de Leon, Blvd, PH 1, Coral Gables, FL 33134) or **website forum on the Contact Us page**. All lines of communication are confidential, toll-free resources available 24 hours a day, 7 days a week to report violations or raise questions or concerns related to compliance. All may be made anonymously.

The above is disseminated via Compliance Training and the Code of Conduct. DHCP also includes information on Website and Provider Manual. All suspected violations will be investigated and disciplinary action will be taken when violations occur.

Utilizing the resources listed is confidential and allows for anonymous, good faith reporting of potential compliance issues. DHCP supports and enforces a strict policy of non-intimidation and non-retaliation for the good faith reporting of suspected compliance concerns and good faith participation in the compliance program. This includes but is not limited to reporting potential issues, investigating issues, conducting self-evaluations, audits, and remedial actions, and reporting to appropriate officials.

c. Enrollee Communications and Education

DHCP will educate their members about the identification and reporting of potential FWA. These education methods may include flyers, mailings, or website postings.

ELEMENT V
Well Publicized Disciplinary Standards

This is explained in annual training and Code of Conduct. All Employees are informed that violations may result in appropriate disciplinary action up to and including termination of employment.

a. Disciplinary Standards

DHCP supports a compliant culture by maintaining well publicized disciplinary standards and guidelines. These policies are clearly written and easily accessible and available on the public (P) drive. Disciplinary policies undergo annual reviews; changes necessary to these policies outside of a scheduled review will be disseminated to all employees accordingly. These standards include, but not limited to, the following policies: expectations for reporting compliance issues and assisting in their resolution; identification of non-compliant or unethical behavior; and; provide for timely, consistent, and effective enforcement of the standards when noncompliance or unethical behavior is determined.

b. Methods to Publicize Disciplinary Standards

Human Resources together with the CO maintain and communicate disciplinary policies and implement procedures which include good faith participation in the Compliance Program by all individuals. As with other important documents, policies can change with revisions to law or governing regulations.

c. Enforcing Disciplinary Standards

Business partners and first tier, downstream related entities are responsible for complying with DHCP Policies and Procedures via the Provider Manual. Potential disciplinary action for violations could include Corrective Action Plans (CAP), retraining related to the identified violation or termination of the contract with the individual/entity.

ELEMENT VI

Effective System for Routine Monitoring & Auditing and Identification of Compliance Risks

a. Routine Monitoring and Auditing

Monitoring and auditing are critical element in the Compliance Program. Compliance related elements are used to develop metrics for evaluating performance against regulatory standards. Monthly metrics were developed with key operational areas (Claims, Clinical/Medical Management, Enrollment/Disenrollment, Pharmacy, Member Services Call Service and CTMs, Appeals &Grievances, and SNP) and delegate operational areas (Pharmacy PDE & Claims, Transitions, and MTM) to monitor key regulatory requirements and confirm ongoing compliance.

The CO and Compliance Committee must ensure the implementation of an audit function appropriate to the size of the organization, scope and structure. The Compliance Department audits business unit operations as part of its overall program to identify and mitigate compliance risk.

b. Development of a System to Identify Compliance Risks

To assist with the identification of such risks and the prioritization of monitoring and auditing activities the Compliance Committee conducts an Annual Baseline Risk Assessment. Risk identified will be ranked to determine which risk areas will have the greatest impact and DHCP will prioritize the monitoring and auditing strategy accordingly.

The annual risk assessment using data and information from a variety of sources which may include:

- Audit/Improvement Plans Root Causes
- Results of Departmental Compliance Risks
- Review of Part C and D Program Audit and Enforcement Report
- Review Advance Notice
- OIG Annual Work Plan
- Part C and Part D Enforcement Actions
- HPMS Memos Released
- Emails/Memo from Medicaid Program Integrity Unit
- Self-Reporting Issues
- CMS Call Center Monitoring Results
- CMS Final Rules and other regulatory guidance

c. Development of the Monitoring and Auditing Work Plan

The result of risk assessment drives the development of the Compliance Department Annual Work Plan and oversight audits. The Work Plan provides the details to routine monitoring and auditing activities that will be conducted throughout the year to address compliance risk. The Compliance Department may modify its audit work plan based on issues that arise within the organization, focusing on high risk areas to confirm effective corrections were taken based detected areas of non-compliance or compliance risks. Medicare Compliance Audits are based on regulatory guidance and rely on:

1. The Medicare Managed Care Manual
2. The Medicare Prescription Drug Benefit Manual
3. CMS Audit Protocols
4. Other applicable CMS guidance and publications
5. State DSNP Agreement
6. State Medicaid Coverage Policies

d. Audit Schedule and Methodology

Similar to the process CMS uses in its audits. Compliance will prepare a report of findings and the audited department will develop a corrective action plan where necessary. The audit report and corrective action plan are reported to the Compliance Committee and audited department management.

e. Audit of the Sponsor's Operations and Compliance Program

Annually, according to CMS requirements, the DHCP Compliance Program will be audited and the results will be shared with the governing body. The audit will be performed by Financial Operations (not a member of the compliance department) or an external auditor.

f. Monitoring and Auditing FDRs

DHCP contracts with various parties to administer and/or deliver Medicare Advantage Benefits. These first-tier parties and their downstream contractors must abide by specific contractual and regulatory requirements. Audits will be conducted to evaluate the FDRs compliance with requirements as well as effectiveness of the compliance program.

The Compliance Department oversees DHCP relationships with FDRs. The team monitor FDRs' activities and performance to ensure they fulfill their contractual requirements and meet established performance standards. Monitoring is conducted via quarterly reporting and random spot checks. Audits are conducted annually as they validate compliance, develop corrective action plans in response to detected offenses and report oversight activities through their respective delegation oversight committee.

When needed, Compliance will issue corrective action plans (CAPs) that should be completed within 30 days unless otherwise specified. All CAPs will be reported to QIC and Compliance Committee. If deficiencies have not been cured to the satisfaction of DHCP, the deficiencies will be presented at DHCP's Compliance Committee and appropriate actions will be determined by leadership including the possibility of termination.

g. Tracking and Documenting Compliance and Compliance Program Effectiveness

All Compliance efforts are documented via the Inovaare Monitoring and Auditing module and presented to the Compliance Committee at least quarterly. Also, via the Regulatory Library module, Compliance tracks the company's compliance with new HPMS Memo guidance released.

h. OIG/GSA Exclusion/Preclusion

DHCP reviews OIG List of Excluded Individuals and Entities, GSA Excluded Parties List System and the Preclusion list prior to the hiring or contracting of any new employee, temporary employee, volunteer, consultant, governing body member, or FDR, and monthly thereafter to ensure compliance.

i. Use of Data Analysis for Fraud, Waste, and Abuse Prevention and Detection

The Plan has a FWA Director who is responsible for proactive measures to avoid inappropriate payments made by DHCP.

j. Special Investigation Units (SIUs)

The Director of FWA is responsible for the direction, implementation and activities of the SIU functions. This is separate from the Compliance Department, as required, although the departments work collaboratively and are active members of the Compliance Committee. The prevention and detection activities for FWA are implemented by Director of FWA. Please refer to the FWA Program.

k. Auditing by CMS or its Designee or AHCA

CMS, the federal government, or any auditor acting on behalf of these entities has the authority to perform audits and inspect any books, contracts, medical records, patient care documentation, and other records of FDRs that pertain to any aspect of services performed. The OIG also has independent authority to conduct audits and evaluations as necessary. DHCP is required to comply with the MEDIC and NBI MEDIC or its designee as well. The Agency for Health Care Administration (AHCA) may conduct, or have to conduct audit and monitoring reviews.

ELEMENT VII

Procedures and System for Prompt Response to Compliance Issues

a. Conducting a Timely and Reasonable Inquiry of Detected Offenses

DHCP has developed policies and procedures, processes and systems for the identification of and prompt response to compliance issues as they are raised. Utilizing the tools in place to conduct timely investigations of identified issues, to proactively conduct self-assessments/self-evaluations and audits of business practices (self-reporting) and correcting such problems promptly and thoroughly to reduce the potential for recurrence, and ensure ongoing compliance with CMS requirements as well as adherence to regulations and law is the most effective method to demonstrate our commitment to compliance.

The CO is committed to the enforcement of Policies & Procedures and the prompt response to Compliance issues. The CO will act promptly, and take appropriate corrective action. The CO will ensure that noncompliance or FWA committed by DHCP employees is documented and includes ramifications should the employee fail to satisfactorily implement the corrective action; this requirement is also applicable to noncompliance of FWA committed by FDR's. The CO will develop and be responsible for creating a system or process to track the resolution of complaints; additionally, the CO will maintain documentation of all compliance deficiencies identified and the corrective actions taken. The CO will conduct ongoing monitoring of corrective action plan (CAP) post implementation to ensure the effectiveness of the CAP. Polices will be enforced consistently through appropriate disciplinary actions.

b. Corrective Actions

DHCP must conduct appropriate corrective actions (e.g., repayment of overpayments and disciplinary actions against responsible individuals) in response to a potential violation of payment or delivery of items or services.

c. Procedures for Self-Reporting Potential FWA and Significant Non-Compliance

DHCP expects all employees and delegates to ensure polices are adhered to and to raise concerns via the Compliance Hotline and/or the other communication resources referenced in the Code of Conduct available when a compliance issue is suspected. The Compliance Issue Reporting Form must be completed when a compliance issue arises as well as a member impact analysis if beneficiaries were impacted. DHCP's commitment to investigate allegations on non-compliance including allegations of fraud and misconduct is to initiate an investigation within 1-2 business days for when DHCP becomes aware of the alleged misconduct. If DHCP discovers evidence of misconduct related to payment or delivery of items or services under the contract, it will conduct a timely, reasonable inquiry into that conduct. Investigations of FWA are concluded within a reasonable amount of time

d. NBI MEDIC & Referrals to the NBI MEDIC

Medicare Drug Integrity Contractors (MEDIC) are organizations CMS contracts to perform integrity functions for Medicare Part C and D. Its primary role is to identify potential fraud and abuse in these areas. The National Benefit Integrity (NBI) MEDIC will investigate referrals from different sponsors, develop their investigations, and make referrals to law enforcement agencies when necessary. DHCP FWA will voluntarily self-report to the NBI MEDIC any potential fraud or misconduct related to the Medicare program. Refer to the FWA Program for more information.

e. Responding to CMS-Issued Fraud Alerts

Fraud Alerts received by CMS will be reviewed and deemed if appropriate action, including denying or reversing claims and terminating contracts is needed. Fraud Alerts are disseminating via Inovaare Regulatory Module to keep track of all activity.

f. Identifying Providers with a History of Complaints

Files will be maintained for 10 years for both in-network and out-of-network providers. This includes a file for identifying a pattern of complaints, investigations, violations, and prosecutions. Specifically, Quality of Care complaints related to providers will be opened, logged, and assigned. All will be presented to QIC Committee after the investigation is complete. A recommended course of action is then determined on a case by case basis and may include: no further action, practitioner notification and education, development and implementation of corrective action plan, or disciplinary action. Recommended disciplinary action could involve sanctions, suspensions or termination from the network. In addition, any practitioner/provider with three or more quality of care cases from same or a different member in a quarter is referred to the QI Committee for review and recommendation.

The Compliance Officer, the Compliance Committee and the Board of Directors are responsible and dedicated to foster a culture of compliance supported by the effective implementation of the DHCP Compliance Program.

APPROVALS

MAYRA CAMPUZANO: . . . . . DATE: . . . . . .
VP, Compliance Officer

BRANDON HAUSHALTER: . . . . . DATE: . . . . . .
Chief Executive Officer

DOCTORS
HEALTHCARE PLANS, INC.

2020 PONCE DE LEON BLVD., PH 1
CORAL GABLES, FLORIDA 33134

DIRECT (786) 578-0965
FAX (786) 578-0290

WWW.DOCTORSHCP.COM