HEALTHSPARQ®

COPY EDITING SAMPLE 1

COMPANY® COMPLIANCE PLAN

INTRODUCTION

The Company Compliance Plan serves three functions:

- It outlines the elements of Company's Compliance Program.
- It helps ensure Company's commitment to exercise due diligence to prevent, detect, and correct violations of the law.
- It contributes to an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Organizational integrity is at the core of Company's values. It depends on the actions of each individual employee. Company expects that every individual employee will comply with legal requirements and that they will act with integrity and trust. The Company Code of Conduct expresses these commitments as guiding principles of our Company. The Code of Conduct is supported by strong ethics and compliance efforts.

Company's Compliance Program is built upon the United States Sentencing Commission's Guidelines for an ~~e~~Effective Compliance Program aimed at promoting compliance and ethical conduct while preventing, detecting, and resolving non-compliant and illegal conduct, including fraud, waste, or abuse. Company's Compliance Program also incorporates concepts of compliance plan effectiveness from the Medicare Managed Care Manual, the Affordable Care Act requirements, and the Federal Acquisition Regulations. Company's Compliance Program includes, but is not limited to, the following elements:

- Written Policies and Procedures
- Compliance Oversight: Officers and Committees
- Education and Training
- Effective Lines of Communication
- Auditing and Monitoring
- Enforcement of Standards through incenting compliance and well-publicized disciplinary guidelines

Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

- Detecting and responding to offenses and developing Corrective Action Plans

Company's Compliance Plan describes the ~~manner~~ way in which each of the Compliance Program elements will be achieved.

The Manager of Product Regulatory Logistics is responsible for oversight of the Company Compliance Plan.

Formatted: Font: 12 pt

Formatted: first page body copy

Formatted: Font: 12 pt, Not Bold

PARENT COMPANY-COMPANY RELATIONSHIP

Company is a wholly-owned subsidiary of Parent Company Health Solutions. Company utilizes several Parent Company Shared Services teams, including Human Resources and Compliance, to manage aspects of its business.

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

I. WRITTEN STANDARDS OF CONDUCT, POLICIES, AND PROCEDURES

The policies and procedures governing Company's Compliance Program are collected on the company intranet, organized for ease of access and understandability under each topic area. Our Code of Conduct is also accessible by members of the public and is given to anyone who contracts with Company.

Code of Conduct

Formatted: Heading 4

The Parent Company Code of Conduct (the Code) articulates Company's commitment to lawful and ethical business conduct. The Code is designed to guide Company workforce members and business partners in upholding Company's principles of fair and ethical practices. All workforce members, including employees, board members, contractors, downstream~~,~~ and related entities are expected to follow the Code of Conduct.

The Code is endorsed by the executive board. It is approved by the Parent Company Audit & Compliance Committee. From time to time, Parent Company's full Board also re-approves the Code. The Parent Company Ethics department maintains, revises~~,~~ and publishes the Code on an annual basis. An electronic copy of the Code is provided to all new workforce members and is available for review on Company's intranet by all workforce members. The Parent Company Ethics department gathers and retains all attestations from workforce members stating they have received, understood~~,~~ and will abide by the Code. Each Company manager, director~~,~~ and officer is responsible for reinforcing the Code in their respective departments.

Delegated contractors and entities who are responsible for the administration of Company business ensure that Company's Code of Conduct is distributed, and certification maintained, such that representatives have read and will comply with the Code of Conduct.

Conflict of Interest (CoI) Disclosure and Management

Company maintains an enterprise-wide CoI disclosure and management program in order to fulfill its regulatory obligations, as well as define workforce members' fiduciary responsibilities to Company. The Parent Company Ethics department is responsible for the CoI program and maintains the policies and procedures outlining the requirements of the program. Workforce members, including non-employed board and committee members, are required to disclose real, potential, or perceived CoIs within thirty days of the onset of employment, at the onset of a new potential CoI, and annually thereafter. The Parent Company Ethics department will distribute and enforce completion of the CoI disclosures and manage real CoIs with consultation with Medicare Compliance, Compliance, Legal, Sourcing, and/or Human Resources on a case-by-case basis. Sourcing will alert Ethics if they come across any conflicts concerning potential supplier engagements.

Confidentiality

Company values its consumers' privacy and is committed to the protection of their personal information. The Company privacy and information security compliance team ensures that Protected Health Information (PHI) and Personally Identifiable Information (PII) are safeguarded according to applicable laws, regulations, and policies. The Company privacy and information security team maintains Company's confidentiality policies, which set forth requirements under state and federal laws to protect the privacy of the PHI and PII that are created, received, or maintained by Company. PHI and PII must be used or disclosed only as permitted or required by the Parent Company Corporate Privacy and Security Policies.

Federal Exclusion Lists

Company maintains policies and procedures for ensuring that Office of Inspector General (OIG) and General Services Administration (GSA) exclusion verifications are conducted for various areas including, but not limited to, employees, producers, medical providers, members, and Delegated Contractors and Entities. These procedures also include verification of exclusions based on the Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list. Screening is performed monthly by the Parent Company Compliance team.

Medicare

Standards of conduct applicable to those working to support Medicare products are outlined in the Code, which is available on the Parent Company intranet. In addition, the Parent Company Medicare Compliance department maintains, and updates annually, relevant compliance departmental policies and procedures.

Training on Medicare Parts C & D Compliance and Fraud, Waste & Abuse regulations is mandatory for all new hires within 90 days of hire and annually for all Company staff. This training is administered by the Company compliance staff and records of staff course completions are maintained and available.

Formatted: Font: Not Bold

Formatted: Heading 4

Commented [WC1]: As opposed to "fake COIs"? Is this the right term? 😉

Formatted: Font: (Default) +Headings (Arial)

Formatted: Heading 4

Formatted: Font: (Default) +Headings (Arial), Not Bold

Formatted: Heading 4

Formatted: Font: Not Bold

Formatted: Heading 4

Product® is compliant with Medicare provider directory requirements. Policies and procedures exist to ensure process controls are in place to meet these relevant and specific requirements of the Medicare program.

Qualified Health Plans (QHP)

Formatted: Font: (Default) +Headings (Arial), Not Bold
Formatted: Heading 4

Product complies with federal QHP provider directory regulations. Policies and procedures exist to ensure processes are in place to meet specific requirements for provider directories related to QHPs.

Standards of Conduct applicable to those working to support QHPs are outlined in the Code, which is available on the Company intranet. The Compliance department works with business partners to implement new requirements, to audit and monitor compliance, and to drive corrective action if violations do occur.

General Compliance

Formatted: Heading 4

Company maintains policies and procedures to ensure compliance with legal requirements. The Manager of Product Regulatory Compliance maintains, and updates annually with managerial support, relevant policies and procedures.

Additional non-product-specific compliance standards and related policies and procedures are maintained by the Parent Company Compliance team.

Fraud, Waste, and Abuse

Formatted: Heading 4

The Parent Company External Audit and Investigations department (EAID) maintains a Fraud, Waste, and Abuse (FWA) Program to prevent, detect, and correct incidents that could lead to fraud, waste, or abuse.

Parent Company EAID maintains internal mechanisms, as well as reporting telephone lines (listed below in the Effective Lines of Communication section), designed to detect and respond to allegations of potential fraud, waste or abuse. EAID investigates all reports of potential fraud, waste or abuse and works with designated government agencies and law enforcement to pursue remediation of cases preliminarily determined to be confirmed FWA.

HIPAA, Privacy, Information Security

Formatted: Heading 4

A separate, dedicated Company information security and compliance team manages privacy and information security processes and policies. This team oversees compliance with HIPAA/HITECH, SOC 2, and other information security and privacy requirements.

II. OVERSIGHT: COMMITTEES, COMPLIANCE OFFICERS AND PERSONNEL

Parent Company's compliance oversight committees and officers are integral parts of Company's overall compliance program. Parent Company's compliance committees and officers are responsible for the collective compliance leadership of Parent Company Health Solutions.

Committee Oversight:

Audit & Compliance Committee

The Audit & Compliance Committee is charged with assisting the Parent Company Board of Directors in overseeing Parent Company's compliance program. The Audit & Compliance Committee is responsible for overseeing the Company's compliance with legal requirements and ethics, including compliance with the Code of Conduct. The Committee meets at least four times annually and meets with the Chief Compliance Officer and the Medicare Compliance Officer in executive session as part of each meeting. The Chief Compliance Officer also provides a written report to the Committee noting such information as highlights and lowlights, significant regulatory audits, industry risks, discipline received, and metrics relating to prevention, detection, and correction of non-compliance.

Company Compliance Committee

The Parent Company Compliance Committee is comprised of Parent Company senior leaders. The Committee meets quarterly and has four roles. First, it assists the Compliance officers with effecting compliance across the organization and driving accountability for compliance in business operations. Second, it advises the Compliance officers. Third, it is accountable to, and provides regular reports to, the CEO and the Audit & Compliance Committee, via reports by the Chief Compliance Officer. Fourth, it can act as the Audit & Compliance Committee's delegate to oversee and approve certain aspects of the compliance programs.

Internal Fraud Leadership Committee

The Internal Fraud Leadership Committee is comprised of leaders from External Audit and Investigations, Compliance, Ethics, Human Resources, Finance, and Internal Audit. The Committee is responsible for ensuring that alleged internal fraud complaints are appropriately investigated, triaged, monitored, and reported with cross-domain oversight, and that fraud and abuse awareness training is provided to employees. The Committee meets quarterly.

Legal and Regulatory Review Committee

The Legal and Regulatory Review Committee (LRRC) is comprised of operational and compliance leadership, as well as interdepartmental subject matter experts. The Company Manager of Product Regulatory Logistics is a member of the LRRC and regularly attends its meetings. The Committee is accountable for identifying and assigning new applicable state and federal laws and regulations for implementation. This includes analyzing the requirements for impact to the company and assigning implementation responsibility to the appropriate business areas. The Committee meets once a month or

Formatted: Heading 4

Formatted: Heading 5

Commented [WC2]: Could we instead format this paragraph as:

The Parent Company Compliance Committee is comprised of Parent Company senior leaders. The Committee meets quarterly and has four roles:

1. It assists the Compliance officers with effecting compliance across the organization and driving accountability for compliance in business operations.
2. It advises the Compliance officers.
3. It is accountable to, and provides regular reports to, the CEO and the Audit & Compliance Committee, via reports by the Chief Compliance Officer.
4. It can act as the Audit & Compliance Committee's delegate to oversee and approve certain aspects of the compliance programs.

Formatted: Heading 5

Formatted: Heading 5

more often as needed. Implementations of new requirements related to Government Programs are handled differently, described below.

Health Plan Management System Memoranda Implementation

Formatted: Heading 5

Medicare provides important information to plans and vendors such as Company, such as regulatory updates, model documents, general information and important deadlines. To ensure that the appropriate individuals are aware of this information, the memos are tracked and housed in an online SharePoint with access by multiple individuals within Compliance and the business units. Memos are distributed directly to key stakeholders by the MCO or a delegate. On a bi-weekly basis, the memos are reviewed with a team of stakeholders and assigned an implementation level and owner. Memos are tracked to completion and corresponding documentation is maintained. The Company Manager of Product Regulatory Logistics regularly attends Parent Company HPMS review meetings.

Privacy and Security Oversight and Governance Committee

Formatted: Heading 5

The Privacy and Security Oversight and Governance (PSOG) committee is a cross-functional body of leaders from throughout Parent Company who act in an oversight and governance capacity to the Parent Company Privacy and Security Offices. The PSOG's key goals and related activities include establishing and maintaining transparency of Privacy and Security policies and standards within Parent Company; providing support to the Privacy Office and Security Office in their efforts to protect the security and confidentiality of Company information and to ensure compliance with privacy and security regulatory requirements; and receiving regular status reports and updates related to strategic and operational activities from the Privacy and Security Offices.

Enterprise Risk Management Committee

Formatted: Heading 5

The Enterprise Risk Management Committee ("ERMC") is an interdisciplinary committee that facilitates Parent Company's ability to achieve Enterprise Objectives through application of a consistent process (called the Enterprise Risk Management Methodology) for assessing and responding to enterprise risks.

The ERMC meets as needed, but no less than quarterly, to monitor the status of all significant enterprise risks. The Senior Vice President of Corporate Accountability and Performance reports aggregate information to the Parent Company Leadership Team, and the Audit & Compliance Committee. Information about enterprise risks is also presented to and discussed by a broader leadership team during quarterly corporate performance review meetings.

Compliance Officers:

Formatted: Heading 5

Medicare Compliance Officer

Formatted: Font: Bold

Reporting to the CCO, the Medicare Compliance Officer is responsible for to implementing and maintaining an effective Medicare Compliance Program that meets all Centers for Medicare & Medicaid Services (CMS) requirements. The Medicare Compliance Officer is also responsible for design and delivery of required Medicare Compliance education to applicable workforce members. The Medicare Compliance Officer has

express authority to provide unfiltered, in-person reports to the Audit & Compliance Committee and senior leadership. The Medicare Compliance Officer is responsible for escalating Medicare compliance deficiencies and ongoing issues of non-compliance to the Parent Company Compliance Committee, senior management, Parent Company's President and CEO, and/or to the Audit & Compliance Committee.

The Company compliance team (Product and Information Security teams) works closely with Parent Company's compliance officers and team members to keep ~~aware~~ abreast of regulatory compliance changes affecting Company's business and products.

III. EDUCATION

Formatted: Keep with next, Keep lines together

Education is an essential element in Company's Compliance Program.

Except for contractors who are exempted because their employers provide sufficient training, Ethics and Compliance education is required of all workforce members within ~~ninety~~ 90 days of the onset of employment and annually thereafter. These education programs are managed and administered by Parent Company compliance and human resources teams. ~~-~~Company staff members must take all compliance, security, harassment, privacy, safety~~,~~ and other education courses required of all Parent Company employees. ~~-~~At minimum, the following compliance education topics are delivered and tracked in annual and new hire training:

Ethics/Code of Conduct

Formatted: Heading 4

Required education about responsibilities defined by the Code, including:

1. ~~1)~~ Reporting non-compliant activity and violations of the Code
2. ~~2)~~ Conflicts of Interest
3. ~~3)~~ Gifts and Business Entertainment
4. ~~4)~~ Business Relationships
5. ~~5)~~ Safeguarding Information and Property

Formatted: Font: (Default) +Body (Arial)

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Privacy and Security

Formatted: Heading 4

Required education that provides an overview of laws relating to privacy and security of Protected Health Information (PHI) and Personally Identifiable Information (PII). The course reviews Company's policies and procedures regarding the handling of PHI and PII and when and how to report privacy- and security- related issues. The course also addresses how maintaining cyber and physical boundaries are critical to protecting our privacy and confidentiality.

Records Information Management

Formatted: Heading 4

Required education that provides an overview of certain legal requirements relating to records retention. The course reviews the definition of a document, explains retention periods, and emphasizes the elements and importance of legal holds for litigation preservation.

Medicare Compliance

Formatted: Heading 4

Required education that provides an overview of Parent Company's Medicare Compliance Program. The Medicare Compliance training is focused on each individual's accountability for following federal and state laws, rules and regulations related to the Medicare program. The training also outlines the effects of non-compliance. It provides practical guidance to help individuals think compliantly and outlines each person's accountability to report non-compliance.

General Compliance

Formatted: Heading 4

Required education that provides an overview of compliance at Parent Company. This compliance training provides practical instruction for workforce members on how to meet their compliance obligations. This training is mandatory for all workforce members.

Fraud, Waste and Abuse

Formatted: Heading 4

Formatted: Keep with next, Keep lines together

Required education detailing how to detect, prevent, and report potential fraud and abuse.

In addition, we provide annual training for our Board members on Ethics, Compliance, Medicare Compliance, and Fraud, Waste, and Abuse. The various Compliance areas may also provide, facilitate or track the operational areas' specialized training, which is responsive to specific needs identified through industry trends or internal experience.

IV. EFFECTIVE LINES OF COMMUNICATION

Parent Company believes that a strong ethics and compliance culture fosters an environment in which the organization's expectations and commitment to ethics and compliance are regularly and clearly communicated to its workforce members and that workforce members are empowered and feel safe asking questions and reporting concerns without fear of retaliation.

The Parent Company Ethics Program fosters proactive and two-way communication about ethics related concerns. No less than quarterly, the Ethics department publishes and distributes communications and tools such as discussion guides, case studies, FAQ's, posters, and enterprise-wide newsletter articles outlining ethics-related expectations and requirements.

In addition, each of the following departments maintains its own internal website with department-specific contact information readily available to all workforce members. Area-specific websites are dedicated to educating workforce members in key compliance-related activities and encouraging a dialogue about those requirements:

- Ethics
- Fraud, Waste and Abuse
- General Compliance
- Information Security
- Medicare Compliance
- Physical Security
- Privacy
- Records Information Management

The websites contain, at minimum:

- Compliance program information
- Multiple avenues for submitting questions
- Anonymous reporting lines and other communication options
- Instructions for reporting potential violations, both anonymously and in-person
- Educational materials
- Policies

Additionally, the Parent Company Compliance Program maintains systems to receive, record, and respond to compliance questions, or reports of potential or actual non-compliance, from all levels of workforce members, as well as the general public. Any workforce member who suspects a potential violation of policy or law is required to report the matter as soon as possible using any of the provided resources.

- To their supervisor/manager or another leader in the organization, or
- Via reporting lines:

Anonymous Reporting Line	To report an ethical or compliance concern anonymously
Ethics Office	

  - For questions or concerns related to expectations of the Code of Business Conduct or what constitutes a conflict of interest
  - To report an ethical concern

V. PRODUCT COMPLIANCE

Because of our commitment to partnering with our (heavily-regulated) health plan clients, Company views compliance as a strategic imperative. As such, our Manager of Product Regulatory Logistics heads up our compliance management function, focusing on compliance.

Formatted: Font: (Default) +Body (Arial)
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"
Formatted: Font: (Default) +Body (Arial)
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"
Formatted: Font: (Default) +Body (Arial)
Formatted: Font: (Default) +Body (Arial)
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.5" + Indent at: 0.75", Keep with next, Keep lines
Formatted: Font: (Default) +Body (Arial)
Formatted Table
Formatted: Indent: Left: 0.05", Hanging: 0.19"
Formatted: Font: (Default) +Body (Arial)
Formatted: List Paragraph, Indent: Left: 0.05", Hanging: 0.19", Bulleted + Level: 1 + Aligned at: 0.5" + Indent at: 0.75"

As a foundation to managing compliance, this role leads a recurring forum for compliance management across our company. This forum focuses on providing updates to the company on developing mandates, leading deep-dive reviews of implemented mandates to assess gaps and develop solutions, providing status updates on solution implementations in progress, and holding an open forum for the company to raise issues to the larger group for review and planning.

As a wholly-owned subsidiary of Parent Company Health Solutions, we leverage their legal, regulatory and legislative affairs departments to help track national and regional regulations, conduct legal reviews and coordinate support from external counsel as appropriate. Our Manager of Product Regulatory Logistics meets regularly with counterparts at Parent Company to gain insights into changes affecting our delegated functions.

Company monitors changes in governmental mandates affecting our functions and services by many methods, including subscriptions to CMS newsletters and memo services, regular meetings with our parent company's Compliance team, regulatory committee and legal team, and direct and indirect client communications. We carefully evaluate such regulatory changes to determine an approach to bringing our products into full compliance with the revised laws and guidelines. The Manager of Product Regulatory Logistics and the Information Security team will create appropriate service tickets and work with our product managers, developers, business analysts, implementation specialists and client services teams to make configuration and/or coding changes to support the identified mandates. We endeavor to meet any target implementation dates for the mandate changes specified by the relevant regulatory body.

Product is compliant with CMS Medicare Advantage provider directory requirements.

Product is compliant with federal regulations relevant to provider directories in the Affordable Care Act (Section 1557), non-discrimination regulations, and online applications accessibility standards in Section 508 of the Rehabilitation Act of 1973 (revised).

Product is currently NCQA certified as an HIP application (NET 6 standards).

VI. PRIVACY AND INFORMATION SECURITY

Our commitment to full compliance with HIPAA and data privacy regulations is evidenced at many levels, including the following:

Executive Oversight: The Parent Company Privacy and Security Oversight and Governance (PSOG) committee is a cross-functional body of leaders who act in an oversight and governance capacity to our Privacy and Information Security Offices. The PSOG's key goals and related activities include establishing and maintaining transparency of Privacy and Security policies and standards; providing support to the Privacy Office and Information Security Office in their efforts to protect the security and confidentiality of information and to ensure compliance with privacy and security regulatory requirements; and receiving regular status reports and updates related to strategic and operational activities from the Privacy and Information Security Offices.

Security: The Parent Company Information Security Office–in conjunction with internal auditors, external auditors and other vendors—determines the security requirements to ensure Company complies with the

HIPAA Security Rule (and all other applicable regulations), contracts and industry standards. Additionally, Company maintains an Information Security team to ensure compliance with Parent Company security standards and applicable regulations.

Privacy: The Parent Company Chief Privacy Officer is responsible for organizational compliance with all privacy requirements. This includes identifying, investigating and resolving privacy incidents, as well as developing policies, procedures and training relative to HIPAA privacy responsibilities and standards administration. Additionally, Company maintains an Information Security team to ensure compliance with Parent Company privacy standards and applicable regulations such as HIPAA.

Training: Onboarding and annual training provides an overview of laws relating to privacy and security of PHI and PII. These courses review policies and procedures regarding the handling of PHI and PII and when and how to report privacy- and security-related issues. These courses also address how maintaining cyber and physical boundaries are critical to protecting our customers' privacy and confidentiality.

Third-Party HIPAA Risk Assessment: Annually, we engage a third-party firm with HIPAA expertise to perform an independent risk assessment of our compliance with the HIPAA Security and Privacy rules.

Change Log

Date	Description
November 1, 2018	Initial Version

We want to hear from you!

Give us your thoughts on how we can improve this document at docs@Company.com. Please include the document name (Company-Compliance Plan CUS-100 Company) in your email.