# METHODOLOGY *SSM-Owned Health Plan Entities*

| | |
|---|---|
| **Document Title** | **Oversight Approach** |
| **Deliverable ID** | 605.0010.01 |
| **Department(s)** | Government Programs Oversight |
| **Abstract** | Details defining the methodology behind the oversight approach and governance. |

## Overview

The Health Plan, as a sponsor of government programs is responsible for fulfilling the terms and conditions of its governmental contracts, including establishing and maintaining an effective compliance program. An effective compliance program must have an effective system of monitoring and auditing to test and confirm compliance with applicable requirements. This system must oversee both The Health Plan and its first tier, downstream, and related entities (FDRs) as The Health Plan maintains ultimate responsibility for compliance with program requirements, even if an administrative or healthcare function is performed by an FDR.

This document is intended to be a high-level overview of The Health Plan's oversight approach methodology. This document is complemented by policies and procedures that are approved at least annually by the Chief Compliance Officer (CCO).

## Definitions

| Term | Definition |
|---|---|
| **First-Tier, DownStream, and Related Entities (FDRs)** | • **First Tier Entity:** Vendor contracted by The Health Plan to perform services related to The Health Plan's Medicare or Medicaid beneficiaries.<br>• **Downstream Entity:** Vendor contracted by a vendor of The Health Plan to perform services related to The Health Plan's Medicare or Medicaid beneficiaries.<br>• **Related Entity:** A subsidiary or affiliate of SSM Health performing services related to The Health Plan's Medicare or Medicaid beneficiaries. |
| **The Health Plan** | All applicable SSM-owned Health Plan Entities administered by Dean Health Services Company, including Dean Health Plan, Dean Health Plan (branded as Prevea360), Dean Health Insurance Company, Dean Health Services Company (branded as WellFirst Health), SSM Health Plan (branded as WellFirst Health), and SSM Health Insurance Company (branded as WellFirst Health). |

## Responsibilities

| Position | Role and/or Responsibilities |
|---|---|
| **Governing Body Sub-Committee, Compliance Committee, and** | Oversight responsibilities. |

| Position | Role and/or Responsibilities |
|---|---|
| **Auditing and Monitoring (A&M) Committee** | |
| **Chief Compliance Officer (CCO)** | Day-to-day oversight of the monitoring tasks performed. |

## Methodology

The Health Plan's CCO[1] is responsible for day-to-day oversight of the monitoring tasks performed by internal business areas and FDRs, including ensuring all oversight tasks are completed and the outcomes are properly managed.

In addition, The Health Plan has three committees with oversight duties.

- Governing Body Sub-Committee
- Compliance Committee
- Auditing and Monitoring Committee (A&M)

The Governing Body Sub-Committee remains knowledgeable about The Health Plan's compliance risks and strategies for mitigating those risks. The CCO and Compliance Committee provide regular updates on the status of the Compliance Program and evidence of its effectiveness. The Governing Body Sub-Committee is accountable to the Board of Directors.

The Compliance Committee oversees The Health Plan's system for auditing and monitoring by reviewing risk assessments, auditing and monitoring work plans and status reports, corrective action plans, and oversight metrics reports. The Compliance Committee is accountable to the Governing Body Sub-Committee.

The A&M Committee assists the CCO in overseeing The Health Plan's auditing and monitoring processes. This includes assisting in the creation of annual baseline risk assessments and oversight metrics reports, as well as, the creation and implementation of auditing and monitoring work plans. The A&M is composed of employees who, based on their job duties and responsibilities, are well-positioned to identify and understand operational risks. The A&M is accountable to the Compliance Committee.

## Implementation

### Oversight Approach

The Health Plan's auditing and monitoring activities are responsive to the risks identified through its risk assessments. Both the risks associated with operational functions that are delegated (i.e., performed by FDRs) and non-delegated (i.e., performed by employees of The Health Plan) are addressed.

#### *FDR Oversight*

The Health Plan assesses if a vendor is an FDR at the time of contracting and whenever there is a change in the services provided by the vendor. If a vendor is determined to be an FDR, it is subject to the following.

[1] Unless approval is required, the CCO may delegate any of the duties referenced in this document to a member of the Compliance department Leadership team.

### *AT Contracting*

For new vendor contracting and existing vendor expansion of scope:

- Business areas must contact the Compliance department regarding the potential contracting. The Government Programs Oversight department (GPO) reviews the proposed delegated functions and advises on the following.
  - If such an arrangement would constitute an FDR relationship
  - If the vendor would be complex or non-complex
  - Potential vendor tier according to risk based criteria as determined by the CCO
- The GPO performs an Office of the Inspector General (OIG)/General Services Administration (GSA), and System for Award Management (SAM) screening of any potential vendors.
- Business areas assist GPO in performing a delegation audit of the administrative or healthcare service functions as well as a Compliance Program Effectiveness (CPE) assessment. Ideally, delegation audits are performed prior to contracting to ensure compliance with CMS guidance, but the delegation audit timing is reliant upon when GPO is notified of the potential vendor.
- CMS-compliant contract language proposed includes appropriate delegation and oversight language as determined by the CCO.
- An owner is assigned who is the key contact for the vendor. Additionally, this individual is the liaison for the GPO to the vendor to complete investigations and remediation of non-compliance.

### *Ongoing Monitoring*

| Timing | Oversight |
|---|---|
| **Monthly** | The Health Plan ensures FDRs do not appear on the OIG and GSA exclusion lists. |
| **Annually** | • The Health Plan requires FDRs complete an attestation in which they attest to having complied with certain program requirements, including the following:<br>  • Distribute the *Code of Conduct and Ethics* and compliance policies and procedures to employees within 90 days of hire and annually thereafter.<br>  • Ensure employees receive appropriate compliance and fraud, waste, and abuse training within 90 days of hire and annually thereafter.<br>  • Screen employees and FDRs against the OIG/GSA exclusion lists prior to hire/contracting and monthly thereafter.<br>  • Timely report all suspected or known non-compliance or fraud, waste, and abuse to Dean.<br>• Based on the risk associated, GPO may perform a delegation or a CPE audit for the administrative or healthcare functions delegated to the vendor.<br>• The FDRs are reviewed for inclusion in our annual risk assessment or an independent risk analysis. |
| **As Needed** | Business Area/vendor owner is the key contact for the GPO to investigate and remediate non-compliance. |

### Risk Assessments

Annually, The Health Plan performs a baseline risk assessment of government programs business areas. The risk assessment breaks out and ranks each inherent risk associated with the operational function. Each inherent risk is assigned a risk score based on all available information, which may include, but is not limited to, the following:

- Summary of previous year audit results
- Audit protocols
- Sub regulatory guidance and best practices
- Nature of work performed by internal business unit or the FDR
- The FDR delegation audit or CPE self-assessment
- Risk assessments created by the FDR
- Prior audit and monitoring results
- Previous experience with the FDR
- The knowledge and experience of employees and/or consultants at The Health Plan

The baseline risk assessment is conducted and shared with the A&M before approval by the CCO. Periodically throughout the year, the risk assessment is reviewed and updated to ensure accuracy. The CCO has the discretion to share the results of the risk assessment with the Compliance Committee.

### Auditing and Monitoring Work Plan

The Health Plan utilizes the baseline risk assessment to develop an auditing and monitoring work plan listing all of the planned auditing and monitoring activities for the calendar year. The risk score of a business area determines if it is addressed in the work plan and the type and depth of auditing or monitoring. Once finalized, the work plan is approved by the CCO. The CCO has the discretion to modify the work plan throughout the year.

Audit work plans may include the following:

- Audits to be performed
- Announced or unannounced audits
- Necessary resources
- Types of audit (i.e., desk or onsite)
- Person(s) responsible
- Follow-up activities
- Audit schedules (with start and end dates)

Monitoring work plans may include the following:

- Compliance participation in regular meetings with a FDR/business area
- Compliance/business Subject Matter Experts (SME) review of FDR-created reports
- Business area compilation of metrics

- Business area submission of monitoring activity documentation to Compliance
- Compliance review of FDR audit workbooks and audit reports
- Compliance review of FDR/business unit policies and procedures
- Compliance/business SME review of business unit/FDR source data

### *Auditing*

All oversight audits are performed according to The Health Plan's standard process, which is defined within the Compliance Program policies and procedures. This process ensures that appropriate sample sizes are utilized, a standardized audit report is created, and identified non-compliance is fully remediated.

Business areas are responsible for assisting with delegation audits and targeted audits as deemed appropriate based on the administrative or healthcare services delegated to an FDR.

The GPO performs the audits, such as delegation, CPE, or other targeted audits. In addition, CPE audits of The Health Plan are performed by Internal Audit or a contracted independent third party.

### *Monitoring*

All monitoring activities are typically performed by business SMEs. The GPO obtains regular status reports on these activities to ensure they are being performed and are effectively addressing identified risks.

## Oversight Reporting

For each Compliance Committee meeting, the CCO creates an executive-level dashboard of compliance metrics from information gathered through monitoring. The dashboard is used to identify trends in operational activity compliance and may result in investigation of root causes, re-perform risk assessments, and/or change auditing and monitoring work plans. The CCO also creates an overview of audits finalized since the last Compliance Committee meeting. Finally, the CCO prepares information on reportable incidents with an open corrective action plan (CAP) or a CAP closed since the last meeting. Refer to the *Non-Compliance Identification, Investigation, and Remediation* section for additional information on reportable incidents.

## Non-Compliance Identification, Investigation, and Remediation

Non-compliance identified through monitoring activities is addressed through the Compliance department's standard non-compliant incident process. Under the standard incident process, potential non-compliant incidents are investigated to determine whether a non-compliant incident has occurred and, if so, classified to ensure it is appropriately remediated. If non-compliance is identified through an audit, the CCO may vary from the standard process with respect to the completion of remediation tasks or Risk Disclosure forms. Formal documentation of all conducted audits is maintained.

The GPO works with the business area owner to facilitate the non-compliance identification, investigation, and remediation. The business area owner of the vendor relationship assists the GPO in this work effort.

The investigation of non-compliance includes the following steps:

1. Determine whether a non-compliant incident occurred.

a. If yes, complete the following steps:
    i. Assess the impact.
    ii. Perform additional testing to determine pervasiveness of non-compliance, if appropriate.
    iii. Identify the root cause.
    iv. Classify the non-compliant incident.
b. If not, the Compliance Incident is typically closed.

All incidents of non-compliance are classified as either Significant Matter, Non-Reportable Matter, or Acceptable Risk.

In determining categorization, the CCO considers all relevant factors including:

- Scope of impact on members and/or The Health Plan
- Incident is a part of a trend and/or represents a recurrence of non-compliance
- Increased risk due to vendor performance
- Possible future consequences of the non-compliant incident (e.g., risk of discovery during a CMS audit)
- Scope of remediation plan, including timeframe
- Risk of recurrence
- Appropriate degree of ongoing auditing and monitoring activities

| Classification of Non-Compliant Incident | Action Required by Business Owner | Report to |
|---|---|---|
| **Acceptable Risk** | Complete Risk Disclosure Form | VP of business area and CCO |
| **Non-Reportable Matter** | Complete Limited Corrective Action Plan (LCAP) | Director of business area |
| **Significant Matter** | Complete CAP | • Compliance Committee<br>• CCO has discretion to report to government authority |

Once the non-compliant incident is classified, the CCO requires the business owner or FDR complete a CAP, LCAP, or Risk Disclosure form, as applicable. The CCO works with the business owner or FDR to ensure the CAPs and LCAPs are designed to fully remediate the non-compliance and prevent future non-compliance.

CAPs and LCAPs must be completed by the date predetermined by both parties. Once the CCO validates the remediation, the CAP or LCAP is considered closed; however, the CCO may continue to monitor compliance. If not remediated by the pre-determined date, the CCO reevaluates the situation and takes appropriate action. The reevaluation could result in reclassification of an incident initially classified as a Non-Reportable Incident to a Reportable Incident, or the termination of an FDR contract.

### Authority of this Document

On an annual basis, this document is reviewed/revised by the CCO, approved by the CCO, and reviewed by the Compliance Committee. Each task identified in this methodology is considered mandatory and subject to auditing by the Internal Audit department. Failure to complete any task must be reported to Compliance Committee.

Documentation and testing performed are stored in the Compliance and Internal Audit department systems. External parties requiring documentation should submit a request to the CCO.

## About This Document

### Categorization

**Jurisdiction**

☒ ALL

*If Jurisdiction scope is limited, select the applicable:*

☐IL ☐MO ☐OK ☐WI

**SSM Health Plan Entity**

☒ ALL

*If Entity scope is limited, select the applicable:*

☐Dean Health Plan ☐Dean Health Plan (branded as Prevea360)
☐Dean Health Insurance Company
☐Dean Health Services Company (branded as WellFirst Health)
☐SSM Health Insurance Company (branded as WellFirst Health)
☐SSM Health Plan (branded as WellFirst Health)

**Product**

☒ ADMINISTRATIVE (support services)
☐ ALL

*If Product scope is limited, select the applicable:*

☐ASO (Self-funded) ☐ASO (Stop-loss) ☐CCHP
☐Individual (FFM) ☐Individual (Non-FFM) ☐Individual (All) ☐Individual (Pre ACA)
☐Small Group (Commercial) ☐Large Group (Commercial)
☒Medicaid (BadgerCare)
☒Medicare Cost (Gold) ☐Medicare Supplement (Select) ☒Medicare Advantage (MAPD)
☐Medicare Part D (EGWP)

**Considerations**

☐ Accreditation: ☐HEDIS ☐NCQA ☐Star Rating
☒ Government: ☒CMS ☐MAR ☐OCI ☐Program Audit Scope
☐ Regulatory Compliance
☐ Other: ☐Aon ☐ETF ☐FEHBP

## Exceptions

The Health Plan, relying on the common ownership, assurances, and understanding gained through ongoing delegation audits, is allowing for a non-standard approach to the oversight model specific to Navitus. Refer to Dean Health Plan and Navitus Health Solutions – Shared Oversight Approach for full details and exception controls.

## Citations and Guidance

- None identified.

## Supporting Documentation

| Document Title | Deliverable Type | Department | Publication Location |
|---|---|---|---|
| **Auditing and Monitoring Committee Charter** | Charter | Corporate | Knowledge Café |
| **Board Audit Committee Charter** | Charter | Corporate | Knowledge Café |
| **Compliance Committee Charter** | Charter | Corporate | Knowledge Café |
| **Compliance Program Methodology** | Methodology | Compliance | Knowledge Café |
| **Dean Health Plan and Navitus Health Solutions – Shared Oversight Approach** | Exception | Navitus | Knowledge Café – Exception Requests |

## Document Ownership

| Ownership Type | Details |
|---|---|
| **Content Origin** | Government Programs Oversight |
| **SME(s)** | Manager of Government Programs Oversight; Travis Herbst |
| **Approver** | Director of Government Programs Oversight; Laura LeCaptain |

## Document History

| Revision | Publication Date |
|---|---|
| Initial publication and approval by DCC. Originally created Laura LeCaptain and approved by VP – Governance, Risk, and Compliance; Stephanie Cook. | 01/21/2019 |
| Revised with new corporate template, styles and standards. Updated the Document Ownership section. Approved by the Compliance Committee and Laura LeCaptain on 01/20/2020. | 01/22/2020 |