Compliance Program Risk Assessment Policy

Policy Number:	A20140128001
Effective Date:	2/4/2014
Sponsoring Department:	Compliance
Impacted Department(s):	All Independent Health, and its affiliated organizations (Nova, Reliance Rx, PBD)

Type of Policy: ☒ Internal ☒ External

Data Classification: ☐Confidential ☒Restricted ☐Public

Applies to:

☒ Corporate (All)
☐ State Products, if yes which plan(s): ☐MediSource; ☐MediSource Connect; ☐Child Health Plus; ☐Essential Plan
☐ Medicare, if yes, which plan(s): ☐MAPD; ☐PDP; ☐ISNP;☐CSNP
☐ Commercial, if yes, which type: ☐Large Group; ☐Small Group; ☐Individual
☐ Self-Funded Services *(Refer to specific Summary Plan Descriptions (SPDs) to determine any pre-authorization or pre-certification requirements and coverage limitations. In the event of any conflict between this policy and the SPD of a Self-Funded Plan, the SPD shall supersede the policy.)*

Specific Line of Business Applicability

N/A

Applicable to Vendors? Yes ☒ No☐

Purpose and Applicability:

The Compliance Program Risk Assessment Policy is intended to ensure an effective compliance program for Independent Health operations as required by state and federal law and regulations. This policy details the Compliance Department's approach to compliance risk assessments as a key activity in developing an effective strategy for monitoring, auditing and oversight of regulatory requirements as it relates to Independent Health operations, its subsidiaries and its **vendor** partners. This policy applies to all lines of business and corporate compliance oversight.

Policy:

Administered by the Chief Compliance Officer and overseen by the Risk Governance Council (Compliance Committee) and Risk and Compliance Committee of the Board of Directors, the Compliance Department periodically, but no less than annually, conducts a formal risk assessment of regulatory compliance against a baseline compliance risk assessment for all lines of business to form the basis of the Compliance Work Plan. This compliance risk assessment includes but is not limited to a review of federal health care program plans, risk adjustment activities and the Anti-Kickback statute risks associated with Arrangements, Medicaid Managed Care Contract requirements, as well as other regulatory entity requirements.

The risk assessment process includes the (1) identification and prioritization of risks, (2) development of work plans or audit plans (as appropriate) related to the identified risk areas, (3) implementation of those work plans and audit plans, (4) development of corrective action plans in response to the results of any internal audits performed, and (5) tracking the implementation of the work plans and any corrective action plans and assessment of the effectiveness of such plans.

When conducting the compliance risk assessment, most operational areas of Independent Health are taken into consideration, including but not limited to Benefit Administration, Claims Operations, Finance, Government Product Operations, Health Care Services, Marketing, Membership Operations, Network Contract Management, Pharmacy, Pharmacy Benefit Management, Sales, Servicing, and Special Investigations Unit.

Each operational area is assessed for distinct compliance risks that may exist by line of business. Considerations include but are not limited to:

- Size of department
- Complexity of work
- Amount of training
- Past compliance issues and audit findings
- Budget

External sources are also used to help generate considerations for key risk areas to review regulatory compliance. The Compliance Department often uses references cited by: the Office of the Inspector General (OIG) Work Plan; Office of the Medicaid Inspector General (OMIG) Work Plan; and Centers for Medicare and Medicaid Services (CMS) Memorandums (i.e. Common Findings and Best Practices, Annual Readiness Checklist).

Risk Assessment Periodic Review Process:

The periodic review process begins with a review of the existing annual Risk Assessment, recent audit findings, new or updated regulatory requirement, supplemental reports and current

compliance reports (Monitoring Reports, Compliance Key Indicators [Dashboard]) to determine areas at risk of being found to be non-compliant or requiring improvement. External sources are also used to help generate effective risk consideration, such as those mentioned above. Once this review is completed, the Compliance Department schedules meetings with key operational areas to review relevant regulatory requirements and that department's performance when measured against such requirements. In these meetings, a review is conducted of the existing risk inventory as it compares to the current state of the departmental operations with the goal in mind of evaluating the status of previously identified and inventoried risks, and to determine if additional risks have surfaced that should be added to the risk inventory (or if enough controls have been implemented to reduce the risk score).

Risk Ranking:

Operational risks are ranked and prioritized using a calculation derived from a combination of the impact and likelihood and compared against the strength of controls currently in place. Risk scores are calculated and agreed to by the operational areas and the Compliance Department. The scoring method provides a framework and structure to prioritize and rate each risk in order to develop a response strategy for each risk. Risks are assigned a response strategy of: Accept, Improve, Monitor, Investigate, or Validate (Audit), and this is also jointly agreed to by the operational area in collaboration with the Compliance Department. This risk response assignment subsequently serves as the basis for the Compliance Program Monitoring and Auditing Work Plan.

- **Improve**: Independent Health commits to making changes that will improve the outcomes (i.e. system or process updates) and reduce the inherent risk of the issue.
- **Monitor**: Independent Health operational areas and/or the Compliance Department monitor the transactional activity (compliance) of the identified risk through reporting or quality assurance processes to assess risk level through management oversight. This approach will allow for a prompt response to any trends or changes in metrics to suggest additional action may be required.
- **Investigate**: Independent Health will gather additional information in order to assess the appropriate risk response and strategy.
- **Validate**: Independent Health will recommend a formal audit of the risk issue identified, including but not limited to process review, testing, and assessment to demonstrate compliance with required laws and regulations.
- **Propose Closure** – Independent Health will take no additional action to the identified risk, beyond the existing process or efforts already in place and/or risk has been properly mitigated.

Vendor Risk Assessment:

In conjunction with this operational risk assessment, an annual **vendor** compliance risk assessment is also performed against the baseline risk assessment for **vendor** partnerships which fall under the

categories of delegation, management services, **first tier**, **downstream**, or **related entity** agreements. The **vendor** compliance risk assessment is performed in collaboration with the vendor business owner of the relationship to review all operational delegations of the **vendor**, as well as the oversight of any monitoring and auditing by Independent Health. The assessment includes the same considerations applied for internal compliance risks as along with the business owner's accountability for **vendor** management, to determine an overall risk ranking for each **vendor** partner identified as requiring compliance risk assessment review.

Compliance Risk Review:

The assessment of compliance risks is an ongoing process and is embedded in many other activities of the overall compliance program. Corrective action plans may be opened in response to results of any internal audits performed to assess the status of identified risks. Compliance risks are periodically reevaluated based on monitoring and/or audit results, external audits, evolution and updates to laws and regulations, and operational or system changes. For this reason, the monitoring and audit strategy of the Compliance Department is a fluid process requiring flexibility and refocus as appropriate.

Definitions

- **Downstream Entity** means any party that enters into a written arrangement acceptable to CMS, below the level of the arrangement between Independent Health and a first tier entity.
- **First Tier Entity** means any party that enters into a written arrangement with Independent Health to provide administrative services or health care services for a Medicare eligible individual.
- **Related Entity** means any entity that is related to Independent Health by common ownership or control and:
    1. Performs some of the Independent Health's management functions under contract or delegation; or
    2. Furnishes services to Medicare enrollees under an oral or written agreement; or
    3. Leases real property or sells materials to Independent Health at a cost of more than $2,500 during a contract period.
- **Subcontractor/subcontracted** means any organization that Independent Health contracts with to fulfill or help fulfill requirements in its Medicare (Part C and/or Part D) contracts, Medicaid Managed Care and Child Health Plus Model contracts, Qualified Health Plan contract, and any other legally binding agreement. Additionally, this term could also refer to one of Independent Health's direct subcontractors, that then itself subcontracts work or services to yet another entity.
- **Vendor** means any business, entity or person that Independent Health enters into a written arrangement (or similar agreement) to provide administrative, consultative, health care, data

storage, and application development services. A vendor could also be a delegated and/or **a First Tier and Downstream (FDR) entity**, a **Business Associate**, and/or a **Subcontractor** (see definitions above).

References

Related Policies, Processes and Other Documents

- Baseline Compliance Risk Assessment Grid
- Compliance Program FDR and Management Contractor Oversight Policy #A20140128003
- Designation and Responsibilities for the Compliance Officer Policy #A070101337
- Mechanisms for Reporting/Disclosing Noncompliance and Corrective Action Policy #A990801007

Regulatory References

- 42 CFR 422.503(b)(4)(vi)(F)
- 42 CFR 423.504(b)(4)(vi)(F)
- 18 NYCRR Part 521.3(c)(6)
- SSL §363-d
- Medicare Managed Care Manual Chapter 9/21, section 30

Version Control

Sponsored By:
Name sponsor: Nicole Britton
Title of sponsor: VP-Chief Compliance Officer
Signature of sponsor:

Revision Date	Owner	Notes
3/3/2015	D. Odrzywolski	Revised
2/4/2016	D. Odrzywolski	Reviewed
11/16/2016	D. Odrzywolski	Reviewed
1/1/2017	D. Odrzywolski	Reviewed, Minor Changes
1/1/2018	D. Odrzywolski	Reviewed, no changes
1/1/2019	Nicole Britton	Reviewed, no changes
1/1/2020	N. Britton	Reviewed, updated vendor definition

1/1/2021	N. Britton	Reviewed, added Investigate as risk response and updated FTE definition
1/1/2022	N. Britton	Reviewed, minor changes
1/1/2023	N. Britton	Reviewed, minor changes
1/1/2024	N. Britton	Reviewed, minor changes
1/1/2025	N. Britton	Reviewed, minor changes
3/1/2025	N. Britton	Added clarification on risk assessment process, RGC approval and updated policy sponsor