Compliance Vendor Risk Assessment Process

Corresponding Policy:	Compliance Program FDR and Management Contractor Vendor Oversight Policy (A20140128003)
Effective Date:	1/1/2024
Sponsoring Department:	Compliance
Impacted Department(s):	Vendor Management, Information Risk Office, Legal

Data Classification: ☐Confidential ☒Restricted

Purpose and Applicability of Process

This process outlines the Compliance Risk Assessment Process. It explains when and how an assessment is issued and how to review and complete gap analyses.

Process

Requirement Overview

The Independent Health risk assessment process encompasses four questionnaires (Information Risk, Finance, Business Continuity/Disaster Recovery, and Compliance) used to assess vendors during the contracting process and to ensure ongoing compliance. Independent Health utilizes a risk-based approach for determining risk assessment requirements and frequency through the use of service tiers. A vendor's service tier is determined based on responses to a questionnaire completed by the **vendor's business owner(s)**. Criteria used in determining a vendor's service tier include, but are not limited to:

- Type of service(s) being provided,
- Criticality and impact to Independent Health's operations,
- Ability to replicate or transition services (whether in house or to another vendor),
- Types of data and volume accessed/stored,
- Regulatory and compliance risk posed by service provider.

When a new Vendor is onboarded or a reassessment is issued by RSAM, Compliance will receive an email from Vendor Risk Management (vendorrisk@independenthealth.com) with the subject "Action Required: Review Completed Vendor Profile – *VENDOR NAME".* This email contains an overview of the vendor profile and the initial questionnaire completion responses. Compliance will review the information provided, the vendor's risk profile in RSAM, and/or the contract or statement of work to ascertain the scope of work/services offered and line(s) of business supported to determine if the Compliance Risk Assessment needs to be issued.

Compliance Risk Assessment Overview

The Compliance Risk Assessment is used to evaluate the status of a vendor's compliance program. The same questionnaire is used for initial contracting and reassessments. Compliance reviews the vendor's response to questions including but not limited to:

- Compliance Program Structure
- Training
- Sanction, Exclusion and Ineligible Persons Status Checking
- Record Retention
- Federal health care program requirements (e.g. Anti-Kickback Statute)

Initial Assessments

Initial Compliance Risk Assessments are typically only issued for **vendors** categorized as Tier 1, Tier 2, Tier 3 (based on services) as well as any **FDR** or **Enhanced Oversight** Vendors. A vendor is triggered as a Tier 3 when the services are needed, but are not important to daily operations, and may be performed in-house or performed by on-site contractors and the Vendor has access to low risk company data, limited, or no access. Compliance Risk Assessments do not need to be issued for Vendors who facilitate internal IH systems or consultant services that are not Tier 1 or Tier 2.

Reassessments

The Compliance portion of the Risk Assessment is reissued based on the designated Vendor Tier in RSAM. Any Tier 1 Vendors and FDRs (regardless of tier) will receive the compliance risk assessment annually. For FDRs that are not Tier 1, Compliance must manually contact the Information Risk Office (IRO) to have the Compliance portion of the Risk Assessment issued. Tier 2 Vendors would be issued the assessment biennially or annually (depending on the assessment results, if an issue is identified, the assessment may be issued more frequently than the typical tier schedule to ensure it is appropriately resolved). Tier 3 Vendors would be issued the assessment triennially, or more frequently (as determined by assessment results). Tier 4 Vendors would be issued the assessment on an as needed basis.

FDR/Medicaid Delegated Entity Status

Compliance maintains a list of Independent Health's **FDR** and Medicaid delegated entities to ensure appropriate risk/compliance oversight to these Vendors. FDR requirements do not apply to persons and entities whose administrative contracts with the sponsor do not relate to the sponsor's Medicare function. Only Medicaid delegated entities are considered **disclosing entities**.

Reviewing and Scoring Compliance Risk Assessments

Once the decision has been made to issue a Compliance Risk Assessment, there are 4 primary Risk Assessment Statuses in RSAM:

- Data Gathering (Assessment has been sent to the vendor for completion by IRO)
- Under Review (Vendor has returned the completed assessment)
- Under Initial Gap Review (Compliance has initiated a gap review)
- Under Final Gap Review (Compliance has completed their review of the assessment)

Assessments cannot be returned to IHA if all required fields are not completed / the assessment has not been completely reviewed and answered by the Vendor. Once assessments are returned, Compliance is responsible initiating an initial Gap review to assess the returned responses and to score the risk impact to the organization.

When reviewing the vendor's responses and any provided attachments, Compliance may need to complete additional research in RSAM to determine if a response is acceptable given their scope of work and contract requirements (such as exclusion checking, record retention, or training), or if a corrective action is needed. If any of the responses require clarification in order to be appropriately scored, Compliance is responsible for either reaching out to the Independent Health **Vendor Business Owner**, or submitting a clarification request to the Vendor through RSAM.

Any potential gaps identified that are not resolved through discussions with the vendor and vendor business owner are assessed for the level of impact (None, Very Low, Low, Moderate, High, Very High) and require a Disposition. Disposition may include:

- Stakeholder Accepts Risk (Compliance Accepts Risk)
- BO Accepts Risk (Business Owner is Accepting the Risk)
- Not an Issue
- Corrective Action Plan (Resolution Required)
- Clarification Requested (When you want to send the question back to the vendor)

Once all potential gaps have been identified and scored, Compliance will issue a final summary of the identified gaps and risk areas identified through their review in RSAM to the vendor business owner and the Legal reviewer. If the assessment is for a current vendor and/or there are no issues to note, Compliance will proceed with finalizing the risk assessment.

Definitions

- **Enhanced Oversight:** a vendor that may not be an FDR but may still require additional review as they may deal with PHI/PII or be member facing (e.g., print vendors).
- **Disclosing entity:** a Medicaid provider, medical facility or clinic, Medicare intermediary or carrier, and/or any entity that furnishes or arranges for the furnishing of health-related service for which it claims payment under any plan or program established under title V or title XX of the Act. Disclosing entities are obligated to, within 35 days of request, provide ownership or control interest disclosure of the organization and/or managing employees and disclose any criminal convictions by managing employees related to that person's involvement in Medicare, Medicaid or Title XX programs, which in turn will be disclosed to the New York State Department of Health.
- **Subcontractor/subcontracted:** 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:** 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).
- **Vendor / Vendor Business Owner** (terms used synonymously): the associate who has been assigned to manage the day-to-day relationship with the vendor. In general, this associate interacts with their vendor counterpart (account representative, relationship manager, etc.) to facilitate operations and to ensure assigned work and requirements are being met at regular intervals. Updates and general correspondence to/from the vendor are funneled through the Business Owner.
- **Management Contractor:** any person, other than staff employed by the MCO, entering into an agreement with the governing authority of an MCO for the purpose of managing the day-to-day operations of the MCO.
- **First Tier Downstream and Related (FDRs)** entity: defined by CMS as any party that enters into a written arrangement with Independent Health to provide administrative services or healthcare-related services related to our Medicare Part C and D contracts. Examples of functions/services that could relate to our Medicare Part C and D contracts include Sales and Marketing, Utilization Management, Quality Improvement, Applications processing, Enrollment, Disenrollment, Membership Functions, Claims administration, processing and coverage adjudication, Appeals and Grievances, Licensing and Credentialing, Pharmacy Benefit Management, Hotline Operations, Customer Service, Bid preparation, Outbound Enrollment Verification, Provider Network Management, Processing pharmacy claims at the point of sale, Negotiation with prescription drug manufacturers and others for rebates, discounts or other price concessions on prescription drugs, Administration and tracking of enrollees' drug benefits, including TrOOP balance processing, Coordination with other benefit programs such as Medicaid, state pharmaceutical assistance or other insurance programs, Entities that generate claims data, and Health care services.
    - **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.
    - **Downstream Entity** means any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the MA benefit or Part D benefit, below the level of the arrangement between an MAO or applicant or a Part D plan sponsor or applicant and a first tier entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services.
    - **Related Entity** means any entity that is related to Independent Health by common ownership or control and:

1. Performs some of Independent Health's management functions under contract or delegation;
2. Furnishes services to Medicare members 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.

References

Related Processes, Policies and Other Documents

- Compliance – RSAM Vendor Assessment Cheat Sheet
- Compliance Vendor Oversight Grid
- IRO - Vendor Risk Management Program Statement
- Contract Summary Form (RSAM)
- Compliance Program FDR and Management Contractor Vendor Oversight Policy, #A20140128003
- Offshore Contracting Policy, #A110418118
- Offshore Subcontracting Attestation
- Independent Health's Vendor Compliance Attestation
- Independent Health's Broker Compliance Attestation
- Vendor Compliance Guide
- Independent Health Code of Conduct and Ethics
- Delegated Vendor Management Vendor Oversight Policy, #A20180314032
- Compliance Privacy and Security Event Scoring Policy, #A20140630001
- Compliance Risk Assessment Policy, #A20140128001

Regulatory References

- 42 CFR § 455.101 - Definitions. | Electronic Code of Federal Regulations (e-CFR) | US Law | LII / Legal Information Institute (cornell.edu)

Version Control

Process Owner:
Name owner: Carolyn Kosinski
Title of owner: Manager Corporate Compliance

Revision Date	Owner	Notes
3/1/2025	C. Kosinski	Drafted