Weill Cornell Medicine	**Policy Title**	Clinical Compliance Risk Assessment
	Policy Number	1.04
	Department	Clinical Compliance
	Effective Date	November 1, 2021
	Last Reviewed	November 1, 2021
	Approved By	Clinical Compliance Committee
	Approval Date	November 11, 2021

Policy

The Compliance Department shall conduct an annual risk assessment and internal review process across the organization to identify and prioritize compliance risks associated with professional fee billing, develop a compliance risk audit work plan ("Compliance Work Plan") related to the identified compliance risks, implement such plan, develop corrective actions in response to results of compliance risk audits performed, and track implementation of the Risk Assessment Work Plan in order to assess its effectiveness.

The Compliance Department will utilize a risk-based compliance methodology and approach to effectively identify organization risk areas, systematically prioritize identified risk, and conduct the required auditing and monitoring activities. Risk-based assessment starts with a four (4) phased approach to develop the compliance workplan through use of internal and external inputs. Each phase of the approach is led by Compliance in collaboration with business partners resulting in a data driven compliance workplan. Risk-based approach will provide the organization greater insight to the internal and external risks and related management of such risks. This approach will enable the Compliance team to produce a compliance workplan which focuses on higher impact areas and related operational activities.

Purpose

In accordance with Office of Inspector General (OIG) Compliance Program Guidance, the U.S. Sentencing Guidelines and in support of the eighth element of an effective compliance program, Weill Cornell Medicine has developed and implemented a risk assessment methodology and internal review process to identify and address risks associated with the Organization's participation in Federal health care programs, including but not limited to the risks associated with the submission of claims for items and services furnished to Medicare and Medicaid program beneficiaries. Annually, Compliance, Internal Audit, Legal and other Operations conducts a risk assessment and internal review process.

Scope

Unless otherwise specified, the scope and applicability of this assessment methodology includes all Weill Cornell Medicine representatives with professional fee billing responsibilities.

Definitions

TBD

Procedure

1. **Risk Identification -** As part of the risk identification process, the following actions/factors may be taken to assist in assessing compliance risk:
    a. **Internal actions/ factors:**

i. Conduct interviews with key personnel, including but not limited to: Senior Associate Dean for Clinical Affairs, Chief Financial & Operating Officer, Central Business Office Director, Chief Information Officer, Chief Patient Safety & Quality Officer, General Counsel, Chief Administrative Officers of Clinical Departments, Clinical Compliance Physician Leaders and Liaisons, and other key stakeholders from the Finance, Human Resources, Information Technology, Quality, Clinical Operations and Legal Departments.
ii. Review the OIG Workplan, prior audit results, government audit results, exit interviews, hotline call trends, investigation trends, risk management cases, and quality assurance and performance improvement indicators, for potential areas to further evaluate.
iii. Conduct data analytics on billing and claims data to identify trends and/or aberrancies.
iv. Incorporating areas for consideration such as bad debt, billing and coding, clinical, cost reports, credit balances, clinical research, documentation, excluded providers, quality, finance, EMR and practice management system processes and workflows, , physician transactions (Stark Law), licensure, reimbursement, regulatory, medical necessity, policies, and procedures, staffing, education, and mergers, acquisitions and divestitures, etc.

b. **External actions/ factors:**
   i. Regularly review Work Plans issued by the Officer of Inspector General for the U.S. Department of Health and Human Services (OIG) and the New York State Office of Medicaid Inspector General; and
   ii. Review government issued reports or audits, such as comprehensive error testing rate (CERT) reports, corporate integrity agreements, Department of Justice settlement agreements, and/or enforcement trends across the healthcare industry.
   iii. Review of MACs, RACs, and Insurance audits including NCDs and LCDs
   iv. Reviewing regulatory changes and emerging legislation/regulations, such as changes in government payment models or implementation of new regulations, that could impact the organization.

2. <u>Risk Ranking:</u>

a. Once the list of risks has been developed, they will be ranked according to probability of occurrence and potential impact or consequences based on following broad categories:
   i. **Impact** - An estimate of the severity of adverse effects, the magnitude of a loss, or the potential opportunity cost should a risk be realized
   ii. **Vulnerability -** The extent to which the functional area may be exposed or unprotected in relation to various risk factors after existing controls have been considered
   iii. **Speed of Onset -** How quickly the risk event may occur will be a key determining factor among the classification

b. Each risk will be been assigned a score and level (i.e. low, medium, high) based on the following criteria:

Impact		Vulnerability	
7-9 High	• Substantial business impact, including material financial loss • Sustained, widespread reputational damage • Catastrophic operational event • Very rapid onset; little or no warning, instantaneous	**7-9 High**	• Controls are non-existent or ineffective • Organization has no capability to manage this risk, or this risk impacts critical business processes • Organization has no / inadequate assignment of ownership for mitigation of the risk
4-6 Medium	• Large business impact • Widespread negative publicity • Severe interruption of operations • Moderate onset; several days or weeks to occur	**4-6 Medium**	• Controls are minimally-somewhat effective (inconsistent) • Organization has limited capability to manage this risk or risk impacts complex business processes
1-3 Low	• Minimal - noticeable business impact • Minimal - localized negative publicity • Minimal interruption to operations • Very slow onset; several months or years to occur	**1-3 Low**	• Controls operate well or somewhat effectively • Organization has well developed or reasonable capabilities to manage this risk
0 N/A	• Not applicable to our organization • Zero effect if risk were to occur	**0 N/A**	• Not applicable to our organization • Zero effect if risk were to occur

An underlying consideration when evaluating impact should include consideration of the effect a non-compliant incident would have on our patients.

3. **Risk Prioritization**
    a. Risk Prioritization would be based on assigned impact and vulnerability rating and considering related business and financial interdependencies (i.e., technology implementation, new clinical areas/specialists)
    b. Based on risk ranking, determine areas that present highest risk to the organization and prioritize. Prioritization should be:
        i. informed by the assigned impact and vulnerability rating
        ii. Considered against related business and financial interdependencies (i.e., technology implementation, new clinical areas/specialists)

4. **Work plan:**
    a. The Compliance Department will develop an annual Compliance Work Plan that places the greatest emphasis on addressing areas of highest risk.
    b. The plan includes the following:
        i. Specific areas of the organization's high-risk areas which will be audited or reviewed during the year by Compliance.
        ii. Considerations per feedback from relevant stakeholders (clinical and non-clinical), staffing levels to execute the workplan, and routine monitoring activities.
        iii. Defined audit scope, estimated timing, level of effort, staffing plan, and other relevant details

Audits and reviews may be conducted internally or by persons or entities outside the organization that have knowledge of health care compliance requirements in the specific area. The Compliance Department will engage outside auditors, as required, and ensure the vendor has entered into appropriate contracts with the organization including Business Associate Agreements (BAA).

Compliance with this Policy

Contact Information

References

Policy Approval

The Compliance Department will review and update this Policy when necessary in the normal course of its review of the Organization's Compliance Program.

Version History

Date	Author	Revisions
		Initial draft completed. Original date of issue.