**Supplemental Materials for *Health Law Connections* (March 2021) Feature Article: *And Then Came COVID . . . One Health Care System’s Journey to Develop and Sustain an Enterprise Risk Management Program***

Contributed by Eva J. Goldenberg and Sheilah O’Halloran, Atlantic Health System

**ENTERPRISE RISK MANAGEMENT POLICY**

**SECTION 1. Purpose**

The purpose of this Policy is to establish the standards, processes and accountability structure to identify, assess, prioritize and manage key risk exposures across Atlantic Health System and its subsidiaries (the “System”) through an Enterprise Risk Management (“ERM”) program. Through a comprehensive risk identification, assessment and prioritization process, the System can identify risk accountability and response. This ensures that the most appropriate and optimum level of resources is assigned to the areas of greatest risk. The ERM program is intended to enable executives and managers at all levels of the System to systematically and continuously evaluate the implications of decisions and actions to the highest priority goals and objectives of the System and to effectively manage a broad array of risks in an informed and strategic manner within an acceptable risk-tolerance level.

The ERM program is designed to support the System’s mission, vision, strategic plan and guiding principles.

**SECTION 2. Scope**

This Policy applies to all plans, activities, business processes, strategies, goals, policies, procedures, individuals, entities and property that make up the System.

**SECTION 3. Statement of Policy**

The System engages in a wide range of clinical and business activities, all of which give rise to some level of risk. It is the policy of the System to:

1. Embed risk management into the culture, goals and operations of the System through establishment of an ERM program.
2. Integrate ERM into strategic and business planning and review, policy development, performance management and resource allocation decisions.
3. Designate individuals with full accountability, appropriate skills and adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and how risks are being managed.
4. Regularly reassess the System’s risk profile and the effectiveness of its risk response in the context of its integrated strategic and financial plan.
5. Anticipate and respond to changing social, technological, environmental, government and market requirements.

**SECTION 4. Definitions**

**Enterprise Risk Management** is a structured, consistent, and continuous process across the whole System for identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect the achievement of the objectives of the System.[[1]](#endnote-1) ERM takes an enterprise-wide, holistic approach by considering the potential impact of *all* types of risks on all processes, activities, stakeholders, products and services by looking at both upside risk (opportunities) and downside risk (potential losses or damages), assessing risk and opportunity in the context of strategic objectives, enhancing existing strategic planning and budgeting processes and engaging “risk owners” or subject matter experts to address and manage risk.

**ERM Audit** is a systematic, independent and documented process for gathering evidence and evaluating it objectively in order to determine the extent to which the risk management framework, or any selected part of it, is adequate and effective.

**Risk** is the chance that an event, trend or course of action will have either a positive or negative effect on the System’s ability to meet its strategic, financial or operational objectives.

**Risk Analysis** is the process of determining the likelihood of a particular event, trend or course of action occurring and the impact of the occurrence on operational or strategic objectives.

**Risk Appetite**, also known as **Risk Tolerance**, is the amount and type of risk that the System is willing to pursue or retain.

**Risk Assessment** is the determination of the quantitative or qualitative value of risk related to a concrete situation and a recognized threat.

**Risk Controls** are the measures used to modify risk to keep it within the System’s Risk Tolerance for that risk and include acceptance, mitigation, transfer, avoidance or exploitation of an event, trend or course of action.

**Risk Evaluation** is a process of comparing the results of the risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

**Risk Identification** is a process of finding, recognizing and describing risk. Risk Identification involves the identification of risk sources, events, their causes and their potential consequences.

**Risk Impact** measures the effect on the System of the occurrence of a risk and ranges from very high to high to moderate to low to very low.

**Risk Likelihood or Risk Probability** measures the chance of an occurrence and ranges from very high to high to moderate to low to very low.

**Risk Management** is the process of identifying and assessing internal and external risks, determining appropriate risk response, creating policies and procedures, controls, systems and accountability to support risk response, communicating risks and mitigation plans and monitoring the effectiveness of mitigation efforts.

**Risk Management Process** is the systematic application of management policies, procedures and practices to the activities of identifying, analyzing, evaluating, treating, monitoring, reviewing and communicating risk.

**Risk Matrix** is a tool for ranking and displaying risks by defining ranges for consequence and likelihood.

**Risk Owner** is the person or entity with accountability to manage a risk.

**Risk Rating** is the priority level assigned to an identified risk based on a combination of the Risk Likelihood and the Risk Impact.

**SECTION 5. Roles and Responsibilities in the ERM Program**

ERM is the responsibility of every System team member.

The System’s Board of Trustees (the “Board”) oversees the ERM program and has delegated its oversight responsibility to the System’s Audit & Compliance Committee. The Audit & Compliance Committee will regularly review the effectiveness of the ERM program and may engage outside auditors and other consultants to assist in its review.

The System’s President & Chief Executive Officer (the “CEO”) is ultimately responsible to the Board for and assumes ownership of the ERM program. The CEO provides Risk direction and ensures that strategic, clinical, operational, legal, financial and compliance Risks are effectively managed. The CEO holds management accountable for managing enterprise Risk.

The System’s leadership, including Senior Vice Presidents, Vice Presidents (including the Presidents of the System’s hospital campuses), directors and managers supports and communicates the System’s Risk Management philosophy, promotes compliance with the System’s Risk Appetite and a sound culture of Risk awareness, manages Risks within its scope of responsibility consistent with the System’s Risk Tolerance and ensures the accurate, timely and consistent flow of Risk Management information to the CEO and Board. The System’s Vice President, Corporate Compliance & Internal Audit and the System’s Senior Vice President, Legal Affairs & General Counsel (the “ERM Executives”) are designated as the leadership executives who manage the ERM program and connect leadership responsibilities to CEO and Board reporting.

All System team members are responsible for integrating risk management into their day-to-day activities in accordance with established directives and protocols. This includes implementing delegated action plans to address identified risks, informing management of new risks and significant changes in known risks and cooperating with others in the Risk Management Process by providing information as required.

**SECTION 5. ERM Framework**

Under the direction of the ERM Executives, who may convene a committee of senior leadership to assist, the System will engage in an ongoing ERM process that includes the following steps:

1. Establishing the Context. The ERM Executives will review with senior leadership the System’s strategic and financial objectives, taking into consideration the System’s clinical and business activities, annual goals and the regulatory, competitive, social, technological, reputational and other environments in which the System operates. This review will form the basis for risk identification, measurement and prioritization.
2. Identifying and Measuring Risks. The purpose of this step is to develop an understanding of Risks or opportunities in order to have an informed evaluation and decision of whether a response is required. In this step, the ERM Executives and senior leadership will engage in a Risk Analysis in order to generate a comprehensive list of threats and opportunities based on events that might enhance, prevent, degrade, accelerate or delay achievement of strategic, financial and operational goals and identify sources, causes and potential consequences. The ERM Framework focuses on the following risk categories, which may change as needed:
3. Clinical
4. Physician Enterprise
5. Medical Staff
6. Lab
7. Research
8. Financial
9. Community
10. Legal/Regulatory
11. Compliance/Internal Audit
12. Technology
13. Human Capital
14. Facility & Safety – Construction Project Management
15. Supply Chain
16. System Development/Strategy
17. Governance
18. Reputation
19. Ambulance Services

The Risk Identification summary will be periodically reviewed and updated by management under the leadership of the ERM Executives.

1. Determining Risk Response and Control Activities. The purpose of this step is to determine which Risks and opportunities require a response, the extent to which the identified Risks are currently controlled, current risk management and mitigation tactics and future risk management and mitigation tactics. Risk Control will be categorized as potentially over controlled, adequately controlled, potentially poorly controlled or poorly controlled. Risk Controls may include preventive controls, detective controls, corrective controls, management controls, administrative controls, accounting controls and information technology controls.

Risk Owners will identify current tactics, future tactics and how they will monitor and report on Risk Management. Risk Owners will also report on new risks identified. An accountability leader will be identified for each risk category. The information received during this step will be available electronically to the System’s leadership to share the information with its directors and managers. The ERM Executives will meet at least semiannually with each accountability leader to receive a report on progress made toward mitigation of identified risks and identification of new risks. The ERM Executives will report to the System’s Audit & Compliance Committee at least annually on ERM activities.

1. Communicating Risk and Response. The accountability leaders will submit the results of their ERM activities to the ERM Executives at least semiannually. The report shall contain at a minimum the summary of material risks, a highlight of all risks that exceed the System’s Risk Tolerance, timeframe and status of Risk Management activities or responses for each Risk, Risks that are increasing, success of mitigation tactics and Risks that require additional activities, highlights of any new Risks including their Risk Assessment and mitigation activities, highlights of untreated Risks and Risk mitigation tactics that are overdue along with the Risk Owners, material emerging Risks and summary of exceptions to established policies or limits for key Risks.
2. Monitoring Effectiveness of Risk Responses. Risks and Risk mitigation activities will be monitored through an ERM Audit by the responsible accountability leaders and the ERM Executives to ensure that significant Risks remain within acceptable Risk Tolerance levels, that emerging Risks are identified and that Risk mitigation activities are effective and appropriate. This will be accomplished through at least semiannual meetings between the accountability leaders and the ERM Executives. The System shall regularly verify that the criteria used to measure Risk and its elements are still valid and consistent with the mission, vision, business objectives, strategies, guiding principles and policies of the System and that changes to the business context are taken into consideration during the Risk Management Process.

The System Audit & Compliance Committee will conduct, or cause to be conducted, regular assessments of Risk Management Processes to identify opportunities for improvement, Risk Management standards used in like providers to ensure this policy reflects contemporary best practices and performance measures with regard to Risk Management related to the strategies and financial and operational performance of the System.

1. Source: Institute of Internal Auditors [↑](#endnote-ref-1)