Unraveling the ERM Quagmire: Risk Identification - Utilizing the Risk Domains as a Process Model

Volume 1, Number 2

Authored by Caroline Bell, RN, BSN, JD, CPHRM, DFASHRM, founder & CEO of IERM (Integrated Enterprise Risk Management)

Suppose the chief physician of your hospital system’s family medicine department submits a proposal to implement the use of a digital health application (app) to monitor in real time the blood sugar levels for the pediatric and adult type I diabetes patient population. The chief physician explains that she intends to require all family medicine practitioners to use the app for every type I diabetes patient. She plans to implement the use of the app simultaneously with the new diabetes clinic that will be opened as a measure to address population health. What process is in place at your organization to identify each potential risk?

It will be difficult to conceptualize all of the risks and opportunities associated with the physician’s digital health app proposal without a panoptic discussion in a committee-based forum. Organizations that have implemented a fully functioning Enterprise Risk Management (ERM) program, which includes an ERM committee structure and standardized processes, will have the greatest success identifying and managing each potential risk and opportunity.

Let’s begin with a brief overview of ERM, then explore the mechanism by which the ERM committee can serve as a platform to generate comprehensive risk and opportunity identification.

ERM OVERVIEW

ERM is an organization-wide business model. According to the American Society for Healthcare Risk Management (ASHRM), “Enterprise risk management (ERM) in healthcare promotes a comprehensive framework for making risk management decisions which maximize value protection and creation by managing risk and uncertainty and their connections to total value.”[i]

According to the Committee of Sponsoring Organizations of the Treadway Commissions (COSO), organizations that integrate ERM throughout the entity can realize benefits, such as:

- Increasing the range of opportunities
- Identifying and managing risk entity-wide
- Increasing positive outcomes and advantage while reducing negative surprises
- Reducing performance variability
- Improving resource deployment
- Enhancing enterprise resilience[ii]

Contrast ERM with traditional risk management models, which are designed to preserve assets. COSO explains, “Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value.”[iii]

One of the Key goals of ERM in healthcare is to shift from traditional risk management processes that focus on the downside of risk (loss), to a more proactive risk management program that focuses on the upside of risk (opportunity) and processes to timely identify and proactively manage risk before harm occurs.

The basic elements of a successful ERM Program may encompass: • Goals that are consistent with the organization’s mission, vision, values and strategic goals. The ERM goals facilitate establishing the organization’s risk appetite and risk tolerance.

- A framework and supporting processes which provide the process to identify, analyze, evaluate, mitigate and monitor risk. One example is the ISO 31000 framework.
- A structure and function that supports the overall infrastructure for flow of information from the top down and bottom up, and across the organization. The ERM committee provides the infrastructure to accomplish organization-wide flow of information.
- A culture of accountability that extends from the governing board to frontline staff members. The organization’s ERM program must be leadership-driven. Otherwise, it is destined to fail.

The organization’s ERM committee structure and function can be one of the key drivers of the above listed success factors.

ERM COMMITTEE

The general structure of the ERM committee includes a working group and steering committee. Ultimately these committees report to the organization’s governing board.

- ERM working group: “[T}he ERM working group reports to the steering committee and is the group charged with day-to-day activities.”[iv] Include in the committee membership representation from each clinical and non-clinical department. The Committee members may include both internal and ad hoc external experts. The general role of the ERM working group committee is to proactively identify, assess, evaluate and manage risk. Risk identification should generate from internal and external data, and through committee discussions regarding proposals for new building, procedures, technology, and so on. The scenario above, regarding the chief physician’s proposal to implement the use of a digital health app in patient care, will be utilized as an example to discuss the ERM working group committee’s role in risk and opportunity identification.
- ERM steering committee: This committee serves as the oversight committee to the ERM working group committee. In general, it functions to guide and review organization’s ERM infrastructure,

including establishing a framework and setting goals.[v] Committee membership should include members of the c-suite and other executive leadership who collectively represent each clinical and non-clinical department within the organization.

The overall ERM committee function and processes extend beyond addressing only clinical/patient safety risks. It encompasses a variety of interrelated clinical, business, environmental, technology and people-centered risks. The eight fluid domains that have been adopted by ASHRM include:

- Clinical/Patient Safety
- Financial/Insurance
- Operational
- Strategic
- Legal/Regulatory
- Technology/Equipment
- Human Capital
- Hazard

The multi-risk domain process will be utilized as a guide for committee discussions to identify both threats (downside risk) and upside risk (opportunity) related to the scenario outlined in the beginning of this document. The process that will be described underscores the extent to which various risks associated with a single subject or event can be interrelated, and why it's important to include representation from all clinical and non-clinical departments in the committee membership.

This discussion is not comprehensive. Rather, it establishes a tone for the general thought process, discussion points, and it highlights certain ERM committee member experts who may be most useful under specific domains. Readers should consider the threats, opportunities, and internal and external experts within their own organization that would be pertinent to this process.

RISK DOMAINS

Clinical/Patient Safety Risk

Definition

The American Society for Healthcare Risk Management (ASHRM) has defined 'clinical/patient safety risk' management as, "Risks associated with the delivery of care to residents, patients and other healthcare customers. Clinical risks include: failure to follow evidence-based practices, medication errors, hospital acquired conditions (HAC), serious safety events (SSE), and others."[vi]

Context

Threats

A variety of clinical risks may arise through the use of digital health apps. Informed consent, proper patient selection, proper provider selection, and quality of care concerns, are among the clinical/patient safety concerns.

For example, committee experts may explore informed consent-related concerns by discussing what informed consent means when care is supplemented through the use of digital health apps. The committee may consider how the use of technology may impact the informed consent process and generate risk. Clinicians should follow existing guidelines for informed consent and revise the process as necessary to conform with the unique nature of incorporating technology into patient care.

There are multiple criteria related to informed consent that are applicable to this process including, but not limited to:

- Evaluating and documenting the patient's competence to understand and to decide, especially when pediatric patients are involved.
- Voluntary decision-making means the patient will not be coerced into using this technology. An alternative plan for obtaining and providing information from the patient to clinician should be in place for patients who do not want to engage in the process.
- Disclosure of material information is a key component of the consent process. The disclosure process should make clear what information will be shared with the patient's physician, how it will be shared, how the information will be used, and expectations by the patient and practitioner. It should be clear to the patient how the information gathered will be used in their treatment plan and publishing purposes, as applicable.
- The patient should expressly, in writing, authorize the plan. The plan should include when and how the patient should access the digital health app, and a process should be in place to follow-up with the patient to determine whether the patient has accessed the app at the designated time and whether the patient has been able to utilize the app as intended.

Quality of care issues may surface through improper patient selection. Patients who are not tech savvy or do not value the use of an app in their care will not be good candidates for use. The use of the app should be optional to preserve quality of care and optimal patient selection.

Opportunities

In terms of the upside of risk, and how the use of digital apps in patient care may drive value from the clinical/patient safety risk perspective, this technology has the potential to create an environment where patients receive care in real time. This may result in greater compliance and offer patients more control over their condition.

ERM Committee Member Experts

- Physician
- Physician office clinical staff
- Legal
- Medical staff office
- Patient safety
- Operations

Financial/Insurance Risk

Definition

The financial/insurance domain involves “Decisions that affect the financial sustainability of the organization, access to capital or external financial ratings through business relationships or the timing and recognition of revenue and expenses. Risks might include: costs associated with malpractice, litigation, and insurance, capital structure, credit and interest fluctuations, foreign exchange, growth in programs and facilities, capital equipment, corporate compliance (fraud and abuse), accounts receivable, days of cash on hand, capitation contracts, billing and collection.”[vii]

Context

Threats

The use of digital health apps may present an insurance risk, especially related to professional liability claims in the context of ‘standard of care’ in a legal proceeding. Technology naturally changes the watchfulness, attention, caution and prudence that a reasonable person in the same or similar circumstances would exercise.”[viii] It’s often a subjective issue upon which reasonable people can differ. If a person’s actions do not meet the standard of care, then his/her acts or inactions fail to meet the duty of care. The medical industry defines ‘standard of care’ as, “A diagnostic and treatment process that a clinician should follow for a certain type of patient, illness or clinical circumstance.”[ix]

According to the latter, digital health apps have the potential to change the standard of care. In broader terms, in the early 1990’s open cholecystectomies were the standard of care for all patients who needed to have their gallbladder removed. Patients were hospitalized for several days, were on IV fluids and were not permitted to eat for several days. Then technology advanced and laparoscopic cholecystectomies became the standard of care. Technology is constantly evolving and new ways of enhancing the quality and efficiency of patient care are being adopted across the globe.

Keep in mind, when the use of a digital health app is considered ‘experimental’ it may amount to an exclusion on a commercial insurance policy.

Opportunities
Market share growth and competitive advantage may be realized through the use of digital health apps in patient care.

ERM Committee Experts

- Captive administrator
- Legal
- Billing
- Insurance broker (external expert who may be invited to a committee meeting to contribute to the conversation)
- Physician

Operational Risk

Definition
According to ASHRM, “The business of healthcare is the delivery of care that is safe, timely, effective, efficient, and patient-centered within diverse populations. Operational risks relate to those risks resulting from inadequate or failed internal processes, people or systems that affect business operations. Included are risks related to: adverse event management, credentialing and staffing, documentation, chain of command, and deviation from practice.”[x] Operational risks may also refer to policies and procedures, and workflow.

Context

Threats
Operational risk can include the policies and mechanisms that are put in place to ensure safe usage of the app, and how the use of the digital app is protected from collateral threats. For example, risks can extend beyond the lack of direct security measures and hacks. In one case a cybersecurity start-up company pitched its software by showing to an outside organization how it worked within the network of a hospital that was a client.[xi] The company never had permission to use its customer’s data to provide presentations online and to other hospitals. In other words, the company selling security actually was giving outsiders an unauthorized look at information from inside its customer’s system. Procedures should be in place to prevent this type of occurrence.

Ensure that the app will perform the task that it is intended to do. Begin by researching whether the app does what it says it’s going to do. One organization learned this the hard way. The New York attorney general’s office settled with three separate health-related mobile app developers because they could have harmed patients by giving them wrong or misleading results. At least one of the apps claimed to measure vital signs and other key health indicators, but it was not backed by scientific testing, which could have caused significant harm.[xii] Developers should be able to provide information about testing and provide disclaimers that their apps are not medical devices and are not approved by the FDA, when applicable.

The use of digital health apps and any technology that requires an overhaul of existing processes and procedures also requires a process to evaluate and revise workflows. Well-designed policies may be developed to guide proper use of the app, including patient management guidelines. Organizations should already have in place a new equipment/new procedure process. Follow those same procedures when adopting digital health apps into patient care. If not already done, incorporate a mock trial run of a patient encounter utilizing the technology before it is actually incorporated into patient care. Mock demonstrations are extremely effective in identifying gaps in the process that can be proactively addressed.

Opportunities

The upside of risk that the organization may experience is the technology has the ability to expand patient-centered care efforts. Practitioners will have the ability to receive information regarding the patient's blood glucose levels in real time and provide more timely and customized and patient-centric care.

ERM Committee Experts

- Operations
- Clinical experts
- Biomedical
- Committee members who are also members of the organization's policy and procedure committee
- Information technology

Strategic Risk

Definition

Strategic risks are those risks associated with the focus and direction of the organization. Such risks may include competitive advantage, mergers/acquisitions/ divestitures, joint ventures, measures to adapt to changing times, health care reform, and other business arrangements.[xiii] Marketing messages should be consistent with the entity's mission, vision, and values. Strategic risks are measured by their applicability to the organization's mission, vision, values and strategic goals.

Context

Threats

The committee should consider how the use of the app furthers the organization's mission, vision, values and goals. For example, if the digital app is considered to be 'experimental' and the organization's mission

and vision is conservative and does not support experimental endeavors, then it will probably not be approved for use at the board level.
Marketing efforts should not over-promise. Collaborate with marketing and corporate counsel to ensure that marketing materials are consistent with applicable rules and do not over-promise cures or chronic disease control.

Opportunities
Adopting digital health apps is a measure to adapt to changing times and can provide a competitive edge. Align marketing messages associated with implementation and use of the app with the organization's mission, vision, and values.

ERM Committee Experts

- Marketing
- Operations

Legal/Regulatory Risk

Definition
Legal and regulatory risk relates to state and federal laws that impact hospital operations and the way care is delivered. It is not necessarily associated with medical malpractice/professional liability. According to ASHRM, "Risk within in this domain incorporates the failure to identify, manage and monitor legal, regulatory, and statutory mandates on a local, state and federal level. Such risks are generally associated with fraud and abuse, licensure, accreditation, product liability, management liability, Centers for Medicare and Medicaid Services (CMS) Conditions of Participation (CoPs) and Conditions for Coverage (CfC), as well as issues related to intellectual property."[xiv]

Context

Threats
There are several potential legal/regulatory risks associated with the use of digital health apps in patient care.

The committee members may consider whether the use of the app may be considered experimental. If so, the IRB rules according to Title 45 of the Federal Code of Regulations may apply.

Committee members may also discuss whether the technology is considered a medical device according to the FDA which may answer the question whether the issue of harm may be considered according to product liability versus medical malpractice principles. Sometimes an event can cross both lines. Many organizations, such as the FDA, are working in collaboration with other entities to drive safe usage of digital health apps in patient care.

Within the past few years, the Federal Trade Commission (FTC) cracked down on several high-profile health technology companies for deceptive marketing and claims, as well as delivering inaccurate results to patients. The FTC began to pay attention to the apps that lack scientific support to back up claims for products that purport to prevent or treat health or disease-related conditions. For example, a blood testing company claimed its technology was revolutionary, but investigators found serious deficiencies with its lab that posed serious health risks to patients.[xv]

State law can also impact the delivery of care through the use of digital health apps. Although state laws have yet to specifically address this space, organizations should follow state laws that address privacy, security, telehealth, geographical boundaries to providing care from the practitioner licensure perspective, and other applicable rules.

Committee members may also consider the federal anti-kickback rules. These rules prohibit "the exchange (or offer to exchange), of anything of value, in an effort to induce (or reward) the referral of federal health care program business."[xvi] The committee members may require from the physician additional information regarding the relationship with the vendor and whether payment or gifts have been offered.

Opportunities

Value may be realized when the committee proactively prevents practices that may violate laws in the first place. This can save the organization millions of dollars in fines and legal expenses.

ERM Committee Experts

- Legal
- Compliance
- Biomedical
- Billing
- Medical staff office
- Physician

Technology Risk

Definition

"This domain covers machines, hardware, equipment, devices and tools, but can also include techniques, systems and methods of organization. Healthcare has seen an explosion in the use of technology for clinical diagnosis and treatment, training and education, information storage and retrieval, and asset preservation."[xvii]

Context

Threats

Due diligence efforts would ensure that digital health apps would be provided through HIPAA compliant platforms and appropriate security measures would be in place. These include, but are not limited to the technology backbone and infrastructure to support the function, remote device integration with real-time data sharing, reporting and cross data correlation; interoperability, data analytics and big data management, and privacy and security.

Opportunities

The upside of risk in this context includes taking proactive measures to prevent technology-associated risks and maximizing best practices in patient care through the use of technology.

ERM Committee Experts

- Information technology
- Compliance

Human Capital Risk

Definition

ASHRM explains, "This domain refers to the organization's workforce. This is an important issue in today's tight labor and economic markets. Included are risks associated with employee selection, retention, turnover, staffing, absenteeism, on-the-job work-related injuries (workers' compensation), work schedules and fatigue, productivity and compensation. Human capital associated risks may cover recruitments, retention, and termination of members of the medical staff and allied staff.[xviii]

Context

Threats

In the scenario, the chief physician of the family medicine department indicated that all physician's will be required to utilize the app with all applicable patients. Proper physician/employee selection for use of the app will be important. Some physicians and employees may not be comfortable with the technology. Sometimes, this can ultimately cause harm in the delivery of patient care.

Opportunities

On the other hand, the use of technology may be a driver for staff retention. There has been much discussion recently on the challenges healthcare organizations face regarding staff retention, especially regarding retaining the millennial workforce. Millennials tend to be tech savvy. One source reported that "only 28 percent of millennials feel their current organization is making full use of their skills.[xix] Although this is only one factor related to millennial staff retention, one may surmise that they may be more content working in an environment that maximizes the use of innovative technology.

ERM Committee Experts

- Human resources
- Physician
- Clinical expert
- Frontline staff members

Hazard Risk

Definition

According to ASHRM, “This ERM domain covers assets and their value. Traditionally, insurable hazard risk has related to natural exposure and business interruption. Specific risks can also include risk related to: facility management, plant age, parking (lighting, location, and security), valuables, construction/renovation, earthquakes, windstorms, tornadoes, floods, fires.”[xx]

Context

Threats

Several hospitals have been victims of crypto-ransomware. The information technology systems of these attacks were infected with ransomware which encrypted files and made the system inoperable. The perpetrators demanded money to unlock the records and remove the malware.[xxi] The same type of threat could compromise the use of the app. The committee representative from the information technology department should take center stage on this portion of the discussion to describe the existing measures that are in place to prevent this type of occurrence. The committee as a whole may discuss which prevention measures or technology should be implemented to protect against this type of threat. The ERM steering committee will be responsible for allocating the resources necessary to implement such measures.

Opportunities

It may be wise for the committee to identify a team to conduct a proactive Failure Modes and Effects Analysis (FMEA) of the technology risks associated with the use of digital health apps in patient care. The findings of the FMEA will be valuable to consider for future plans to implement similar types of technology into patient care. This will ultimately save the organization time, money and resources.

ERM Committee Experts:

- Information technology
- Operations

NEXT STEPS

Once the ERM working group committee members have identified all potential risks, the next step is to analyze, evaluate, mitigate and monitor the risks. Committee members must be provided with the appropriate tools and guidelines to advance to the next steps in an expeditious, efficient and standardized manner. The ERM steering committee develops and guides these practices and provides the resources necessary to complete ERM working group committee tasks.

CONCLUSION

Healthcare organizations that have implemented a fully functioning ERM programs benefit from accelerated processes to proactively identify and manage risk. An ERM infrastructure also provides a platform to maximize opportunities. The entity's ERM committee structure, when properly functioning, can advance the organization's successful achievement of ERM.

This article is one of many in the *Unraveling the ERM Quagmire* series. Watch for additional issues on LinkedIn https://www.linkedin.com/in/caroline-bell-rn-jd-dfashrm-79a4877/ or register to receive a copy of these publications via our website https://i-erm.com/

ABOUT THE AUTHOR

Caroline has over 25 years of experience in the healthcare industry. She earned her Bachelor of Science in Nursing degree from Bowling Green State University and her Juris Doctor degree from Cleveland Marshall College of Law. As the founder and CEO of IERM (Integrated Enterprise Risk Management), she partners with health care leaders to achieve Enterprise Risk Management within their entity. Caroline has simplified the ERM process so that healthcare organizations can more easily integrate an effective, standardized and ongoing ERM infrastructure throughout the organization.

*Special thanks to AHRMNY for publishing this article in the *Risk Management Quarterly,* Volume I, pp. 4-8, 2018. Please contact Caroline.Bell@i-erm.com to publish this or related articles in your publication.

[i] American Society for Healthcare Risk Management, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, accessed 2/16/18.

[ii] Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management Integrating with Strategy and Performance Executive Summary," June 2017, pp. 3-4, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-withStrategy-and-Performance-Executive-Summary.pdf, accessed 2/20/18.

[iii] Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management Integrating with Strategy and Performance Executive Summary," June 2017, p. 3, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-withStrategy-and-Performance-Executive-Summary.pdf, accessed 2/20/18.

[iv] American Society for Healthcare Risk Management, developed by Roberta Carroll, "An Enterprise Risk Management Playbook: An Implementation Guide for Healthcare Professionals," 2015, p. 46.

[v] American Society for Healthcare Risk Management, developed by Roberta Carroll, "An Enterprise Risk Management Playbook: An Implementation Guide for Healthcare Professionals," 2015, p. 46.

[vi] ASHRM, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, 2016. 7 ASHRM, "Enterprise Risk Management,"

[vii] ASHRM, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, 2016.

[viii] The Free Dictionary by Farlex, https://legaldictionary.thefreedictionary.com/standard+of+care, accessed 2/8/18.

[ix] MedicineNet.com, https://www.medicinenet.com/script/main/art.asp?articlekey=33263 , accessed 2/8/18.

[x] ASHRM, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, 2016.

[xi] Kevin Townsend, "Tanium Blasted for Using California Hospital Network for Sales Demos," Security Week, 4/21/17, http://www.securityweek.com/tanium-blasted-using-california-hospitalnetwork-sales-demos, accessed 2/8/18.

[xii] Jonah Comstock, "New York Attorney General Settles with Three Mobile Health Apps," Mobi Health News, March 23, 2017, http://www.mobihealthnews.com/content/new-york-attorney-general-settlesthree-mobile-health-apps , accessed 2/12/18.

[xiii] ASHRM, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, 2016.

[xiv] ASHRM, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, 2016.

[xv] "Is it Fair to Call Digital Health Apps Today's 'Snake Oil?'" Fast Company, 6/21/16, https://www.fastcompany.com/3061125/is-it-fair-to-call-digitalhealth-apps-todays-snake-oil, accessed 2/12/18.

[xvi] "Anti-Kickback Statute," https://www.healthlawyers.org/hlresources/Health%20Law%20Wiki/AntiKickback%20Statute.aspx, accessed 2/12/18.

[xvii] ASHRM, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, 2016.

[xviii] ASHRM, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, 2016.

[xix] Patrick Thean, "Millennials in the Workforce – Engaging Them, Retaining Them," The Blog, Huffington Post, 4/2/15, https://www.huffingtonpost.com/patrick-thean/millennials-in-theworkfo_b_6994968.html, accessed 2/20/18.

[xx] ASHRM, "Enterprise Risk Management," http://www.ashrm.org/resources/pdf/ERM-Tool_final.pdf, 2016.

[xxi] Niam Yaraghi, "A Health Hack Wake-Up Call!" U.S.News, 4/1/16, https://www.usnews.com/opinion/blogs/policy-dose/articles/2016-0401/ransomware-hacks-are-a-hospital-health-it-wake-up-call, accessed 2/20/18.