Risk Management in EHR Implementation

Save to myBoK

By Tiankai Wang, PhD and Jackie Moczygemba, MBA, RHIA, CCS, FAHIMA

Risk management is defined as “the act or practice of dealing with risk, which includes planning for risk, assessing, identifying and analyzing risk areas, developing risk-handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program.”[1] The goal of risk management is to lower the probability of risk and alleviate risk impacts. Health information management (HIM) students need to be able to analyze risk management scenarios in various HIM practices to control or prevent risk where possible. The authors reviewed current textbooks and journal articles and did not find sufficient practical examples for student use. Addressing this lack of information, this article describes and illustrates how to apply the risk management tool failure mode and effects analysis (FMEA) with risk register

Risk Management in Healthcare

Several tools are available in risk management, including root cause analysis, FMEA, and risk register. FMEA is used to identify the location, cause, and consequences of potential failure, for the purpose of reducing the chance of failure.[2] While the origin of FMEA can be traced back to the 1970s, FMEA was gradually adopted for the healthcare industry by the American Hospital Association (2002) and The Joint Commission (TJC) at the turn of the century.[3] Use of FMEA in healthcare is growing, particularly since a requirement was added to the Joint Commission standards that healthcare facilities identify and conduct at least one FMEA on a high-risk process every year.[4] FMEA has been used by hundreds of hospitals in a variety of healthcare programs. For example, the Institute for Healthcare Improvement’s (IHI) Idealized Design of Medication Systems (IDMS) team used FMEA to evaluate the medication-dispensing process. The team identified and analyzed seven critical steps that usually occur in a dispensing process. The team reviewed these steps for failure modes and assigned a risk priority number (RPN) to each step. Following FMEA, IHI proposed an activity list which is used to improve the process for dispensing medications.[5]

The methods of FMEA vary in different texts. One approach, published in the *AORN Journal*, proposes a critical index score, which is calculated as follows:[6]

Critical Index (CI) score = Severity × Probability × Detectability

For each of the factors, a scale of numbers ranging from 1 to 5 is assigned. Thus, the most severe, most probable, and least likely to be detected potential error event is the highest ranked event. The Joint Commission proposes a risk priority number (RPN) method, which is the same as the CI score described above, except that the scale for each factor ranges from 1–10.[7]

Yet another approach, published by Mike W. Schmidt in Medical Device and Diagnostic Industry, argues that detectability in risk assessment is suitable in manufacturing, but detection of a hazard during use of a particular device does not ensure the harm will be avoided.[8] Therefore, in recent healthcare studies the risk score contains only two factors.-[9,10] For example:

Risk score = Severity × Probability

Just as the methods of FMEA vary in different texts, there is currently no standardized process in actually conducting the FMEA process. The Veterans Affairs National Center for Patient Service (VA NCPS) interpreted the TJC requirement in the Leadership 5.2 standard as needing five steps:[11]

1. Defining the FMEA topic
2. Assembling the team
3. Graphically describing the process
4. Conducting a hazard analysis
5. Actions and outcome measures

To further illustrate differences in conducting the FMEA process, Darryl S. Rich, the surveyor of TJC, specifies the following six steps:[12]

1. Constructing a detailed flow chart of the process
2. Determining each step that can "fail" and how it can "fail"
3. Determining the "effect" of each possible "failure"
4. Determining how serious the possible effect(s) can have on the patient—criticality
5. Conducting root cause analysis of top failure modes
6. Brainstorm actions that could reduce the criticality index

Healthcare managers can be flexible in deciding on the FMEA process steps based on the process under review. Regardless of the differences, both of the two methods require the key technical parts in FMEA which include conducting a workflow process, assigning the scales to the risk factors, determining the risk score, and providing actions to improve the process. Below, the authors use an arbitrary example of electronic health record (EHR) implementation to illustrate the application of FMEA in risk management.

Applying FMEA in EHR implementation

After the Health Information Technology for Economic and Clinical Health (HITECH) Act was promulgated in 2009, EHRs were more widely adopted. Many healthcare organizations are undertaking EHR implementation projects or updating information technology processes. Risk management is needed for EHR systems so that undesirable events can be ruled out and prevented whenever possible.

Choosing the EHR implementation process is an ideal example to illustrate the application of FMEA. Using the process proposed by VA NCPS, the first three steps are assumed. The topic is identified and a team is in place. An analysis of workflow has been completed because EHR implementation projects are generally led by a professional project team. The team will usually consist of a project manager, sponsors, and representatives from each department/unit. To illustrate FMEA, this article will focus on the next steps in the analysis, which consist of risk assessment and control.

First, what are the risks in EHR implementation? Risk identification methods include brainstorming, Delphi technique, interviews, root cause analysis, SWOT analysis, and experience. The risk management team can use any method to identify the risks. The team will assign each risk factor a rating for severity and probability. In practice, one risk item will impact several aspects of the project, including cost, time, scope, and quality, which are the key criteria to assess the implementation success. Therefore, it is more complicated than calculating one single risk score. To analyze the complexity, the following tables were created.

Table 1: Risk Assessment Table

Severity	**Probability**			
	Low (1)	**Medium (3)**	**High (7)**	**Very High (9)**
Cost (2)	insignificant	<5%	<10%	>10%
Time (3)	insignificant	< one month	< 3 months	>3 months
Scope (5)	insignificant	no business impact	some business impact	Definite business impact
Quality (2)	insignificant	no anticipated problems	potential for problems	Definite problems

Ranking: High > 75, Medium > 50, Low < 50

According to the above table, the risk management team can assess each risk item's probability, then risk score. For example, the risk score of inadequate training is found in Table 2.

Table 2. The Risk Score of Inadequate Training

Inadequate Training

Severity	Probability	Risk Score = Severity × Probability
Cost (2)	High (7)	14
Time (3)	High (7)	21
Scope (5)	Low (1)	5
Quality (2)	Very High (9)	18
	Total Risk Score	**58**

The ranking legend below Table 1 is used to decide whether this risk item is assessed as high, medium, or low risk in the EHR implementation project. According to the ranking legend, inadequate training is assessed as medium risk.

Monitor and Control Risks with Risk Register

The purpose of risk management is to reduce the chance of failure. Therefore, assessing the severity and probability of each risk item with FMEA is the identification and assessment segments of risk management. Once FMEA is completed, the healthcare management team is able to create the risk register to monitor and control risk as much as possible. In the case illustration of EHR implementation, the root cause of inadequate training is examined as one risk included in the risk register (shown in Table 3). For this risk factor, the cause may be simple—insufficient training due to neglect on the part of management.

The next step is to take action to monitor and control risks. The risk management team should pay more attention to risk factors assessed as high to medium to alleviate its impacts. Actions include avoiding, transferring, mitigating, and accepting a risk. Avoiding a risk is to ensure the risk will not happen by changing the plan or process. For example, to address inadequate training, managers can prepare in advance by requiring more training from the vendor and providing additional on-site or on-line assistance.

The most common form of transferring a risk is to purchase insurance. For example, in an EHR implementation project, purchasing additional billing insurance can alleviate the potential negative impacts due to billing errors during use of the new EHR system. Outsourcing is another popular approach in risk transferring. If the hospital has limited experience in data conversion during EHR implementation, it can contract out this work to a data conversion specialist. If there is no way to avoid or transfer risk, then mitigating the risk is needed. For example, with system incompatibility, the organization can allocate more capital resources to replace obsolete systems. This will require mobilizing the contingency plan for extra resources, such as labor and cost. Finally, if nothing can be done, the organization will have to accept the risk.

The next step involves the development of a risk response plan for each of the risk items. Each risk item has its critical date, such as with EHR implementation, where some risk items are approaching, while others are not urgent. The risk team needs to assess all risk items and input them into the risk register, as illustrated in the following table.

Table 3: Risk Register

Risk Item	Risk Score	Risk Management Strategy	Critical Date	Current Status
Increased workload	Low	Accept, or mitigate depends on contingency budget	Month 1	Increase scrutiny
Network capacity	Medium	Mitigate: upgrade current network with contingent budget approval.	Month 2	Continue to review
System incompatibility	High	Mitigate: replace obsolete systems with contingent budget approval	Month 3	Continue to review
Inadequate training	Medium	Avoid: require more training from vendor, and provide more on-site and online assistance, and contingency of $50,000 approved by the Committee.	Month 3	Solved, not an issue now

Unexpected expenses	Low	Mitigate: depends on contingency budget	Month 3	Continue to review
Data Privacy Compliance	High	Transfer: outsourcing	Month 6	n/a
…				

It is important to note that the team will need to continue monitoring and updating the register weekly or monthly. Some risks, such as data privacy compliance, will not influence the project for 6 months, so the current status may be noted as “not applicable” until further information is obtained and the timeline is reached. In addition, during the risk monitoring, the project team needs to watch for new risks, especially when the project scope, schedule, or environment changes.

Summary

Risk management is a required curriculum competency by CAHIIM. This article illustrates how to conduct risk management with the popular risk management tool FMEA and create the risk register, utilizing EHR implementation as a case illustration. In addition to this case illustration, risk management knowledge is needed in loss prevention and reduction (clinical and non-clinical), claims management, risk financing, patient safety, and regulatory and accreditation compliance as a risk manager. Health information management practitioners can master the knowledge and fundamentals from this example and utilize the risk management tools in other HIM practices.

Notes

[1] Spath, P. L. *Introduction to Healthcare Quality Management.* Health Administration Press, Chicago, IL: 2009.

[2] Ibid.

[3] Joint Commission on Accreditation of Healthcare Organizations. *Hospital Accreditation Standard*, LD 5.2. 2002.

[4] Kelly, D. *Applying Quality Management in Health Care: A Systems Approach.* 2nd edition. Health Administration Press, Chicago, IL: 2007.

[5] Institute for Healthcare Improvement. “Improve Core Processes for Dispensing Medications.” http://www.ihi.org/resources/Pages/Changes/ImproveCoreProcessesforDispensingMedications.aspx. 2015.

[6] Spath, P. L. Using failure mode and effects analysis to improve patient safety. *AORN Journal.* 78(1), 16-37. 2003.

[7] Joint Commission Resources. *Excerpts from Failure Mode and Effects Analysis in Health Care: Proactive Risk Reduction*. 3rd Edition. 2013. http://2013.march.qualityandsafetynetwork.com/downloads/JCR3_13_Risky_Business.pdf. [content no longer available at this link]

[8] Schmidt, Mike W. “The Use and Misuse of FMEA in Risk Analysis. Medical Device and Diagnosis Industry.” March 2004 issue. p. 56. Retrieved on 4/17/2014 from http://www.mddionline.com/article/use-and-misuse-fmea-risk-analysis.

[9] Reiling, J. G. et al. “FMEA – the Cure for Medical Errors.” *Quality Progress* 36(8), 67-71. 2003.

[10] Win, K. T. et al. “Electronic health record system risk assessment: a case study form the MINET.” *Health Information Management*, 33(2), 43-8. 2004.

[11] Veterans Affairs National Center for Patient Service. *The Basics of Healthcare Failure Mode and Effect Analysis.* 2001. http://www.patientsafety.va.gov/docs/hfmea/HFMEAIntro.pdf.

[12] Rich, D. S. Complying with the FMEA Requirements of the New Patient Safety Standards. 2001. http://www.fmeainfocentre.com/presentations/fmea_requirements.ppt?.

References

American Hospital Association. “Strategies and Tips for Maximizing Failure Model and Effect Analysis in Your Organization.” *Journal of Healthcare Risk Management* 22(3), 9–12. 2002.

Department of Defense. *Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis*. 1980. http://www.sre.org/pubs/Mil-Std-1629A.pdf.

Tiankai Wang, PhD, is associate professor and Jackie Moczygemba, MBA, RHIA, CCS, FAHIMA, is associate professor and chair in the health information management department at Texas State University.

Original source:
Wang, Tiankai; Moczygemba, Jackie. "Risk Management in EHR Implementation" (Journal of AHIMA), May 2015.