Advancing Regulatory Science through Comprehensive, Rational Risk Management

Fubin Wu *is cofounder of GessNet Risk Management Consulting and Solutions in Sacramento, CA. Email: fubin.wu@gessent.com*

Edwin L. Bills, *RAC, CQE, CQA, CQmg, is principal consultant of ELB Consulting in Overland Park, KS. Email: elb@edwinbillsconsultant.com*

Jessica Eisner, *MD, is principal consultant with PharmBio Consult in Boston, MA, Email: jeisnermd@gmail.com*

Editor's note: This article is the first installment in a semiregular department providing analysis and insights on matters affecting the regulation of health technology. If you are interested in contributing, please contact the editor at jsheffer@aami.org.

Regulatory science involves the development of tools, standards, and approaches to assess the safety, efficacy, quality, and performance of Food and Drug Administration (FDA)-regulated products. In efforts to improve and advance regulatory science, the FDA frequently cites risk-based approaches for the development of strategic plans, premarket review guidance, and compliance inspection manuals.

A lack of common ground in understanding the FDA's approach toward risk can be a source of controversy and confusion. Risk-based approaches may be inconsistently interpreted or implemented. With the complexity of today's connected healthcare ecosystem, key risk management principles can be overlooked, inconsistently followed, or even misused.

With the complexity of today's connected healthcare ecosystem, key risk management principles can be overlooked, inconsistently followed, or even misused.

What Is Risk?

The confusion surrounding risk management begins with inconsistent definitions of the term "risk."

Historically, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have jointly developed standards, such as ISO 14971,[1] that were less prescriptive and allowed for the rapid development of new technologies in healthcare. Both ISO 14971, (a medical device risk management standard) and ICH Q9[2] (pharmaceutical risk management guidance) define risk as "the combination of the probability of occurrence of harm and the severity of that harm." ICH Q9 defines harm as "damage to health, including the damage that can occur from loss of product quality or availability," while 14971 defines it as "physical injury or damage to the health of people, or damage to property or the environment."

Other uses of the term "risk" appear in IEC 60812.[3] This standard explains the failure modes and effects analysis (FMEA) tool, which often is used to provide input into risk analyses by identifying effects of failures that might lead to hazardous situations and, ultimately, to harm. Unfortunately, this standard does not actually define risk. Further variation in the use of the term can be found in ISO 31000,[4] which only defines risk as "risk-uncertainty on objectives."

When ISO 13485[5] was updated in 2016, it was thought that additional clarity would be achieved. However, although the standard adopted the definition of risk from 14971, it did not include a definition of the term "harm," which completes the definition of risk in 14971. Indeed, ISO 13485 muddied the waters by stating, "When the term 'risk' is used, the application of the term within the scope of this international standard pertains to safety or performance requirements of the medical device or meeting applicable regulatory requirements."

Risk also has been addressed in standards related to biocompatibility, software, clinical trials, usability, and, recently, cybersecurity. Biocompatibility standards developers incorporated risk instruction in ISO 10993-1,[6] while software standards developers provided risk guidance in IEC/TR 80002-1.[7] Usability standards developers incorporated the concept of risk with informational annexes in IEC 62366-1,[8] and clinical trials standards developers addressed it in ISO 14155.[9] Each of these standards addresses how it interfaces with 14971—the one medical device risk management standard. The ISO healthcare cybersecurity standards committees continue to work on the interface between their documents and 14971.

Risk Management Principles

Application

Emphasis on safety. The healthcare industry needs to recognize that product safety should be emphasized over business, compliance, and other project priorities. If products are not safe to use, they must not be placed on the market. It is interesting to see that regulators spent considerable effort in revising 13485 to include regulatory risk; however, the difference between regulatory risk and product safety risks remains somewhat unclear, and even 13485 does not explicitly state which is more important.

Vigilance throughout the product life cycle. Risk management needs to be vigilant and iterative throughout the product life cycle. Premarket risk management reflects decisions and conclusions based on information and knowledge known at the time. Even with clinical study results (for certain devices), this information and knowledge during the premarket phase may not be complete or completely correct. Continuously seeking real-world evidence to validate the decisions made and monitor evolving use conditions in a timely manner to identify and manage potential changes in risk or emerging new risks (e.g., cyberthreats) is crucial.

Up until recently, the pharmaceutical industry has focused on applying risk management to the manufacturing processes of drugs, while the medical device industry has placed the majority of its focus on design and development processes. Neither industry has carefully considered monitoring and feedback processes.

The next version of 14971 is set to be released in late 2019. It is expected that extensive information will be provided in the accompanying technical information report, ANSI/AAMI/ISO TIR24971,[10] on the use of postdevelopment information to improve the risk profile of healthcare products through connection to the monitoring and feedback phases of the product life cycle. Currently, the monitoring and feedback processes are covered in the corrective and preventive action processes described by the Global Harmonization Task Force.[11]

System-level risk management. Risk management needs to be performed at the system level, in the context of evolving use conditions and environments of the healthcare ecosystem. Of important note, in addition to potential harm to patients, risk includes "damage to the health of people." This may include health professionals, other caregivers, device servicers, or other people who come into contact with the device. For health safety risk, the system begins where the basic causes of potential hazardous situations are identified and finishes with the patient or end user. During this continuum, other medical systems or applications, organization processes, clinical workflows, and conditions/events may influence risk (Figure 1[12]).

Risk for a medical application needs to be analyzed, assessed, and controlled using this

In addition to potential harm to patients, risk includes "damage to the health of people." This may include health professionals, other caregivers, device servicers, or other people who come into contact with the device.

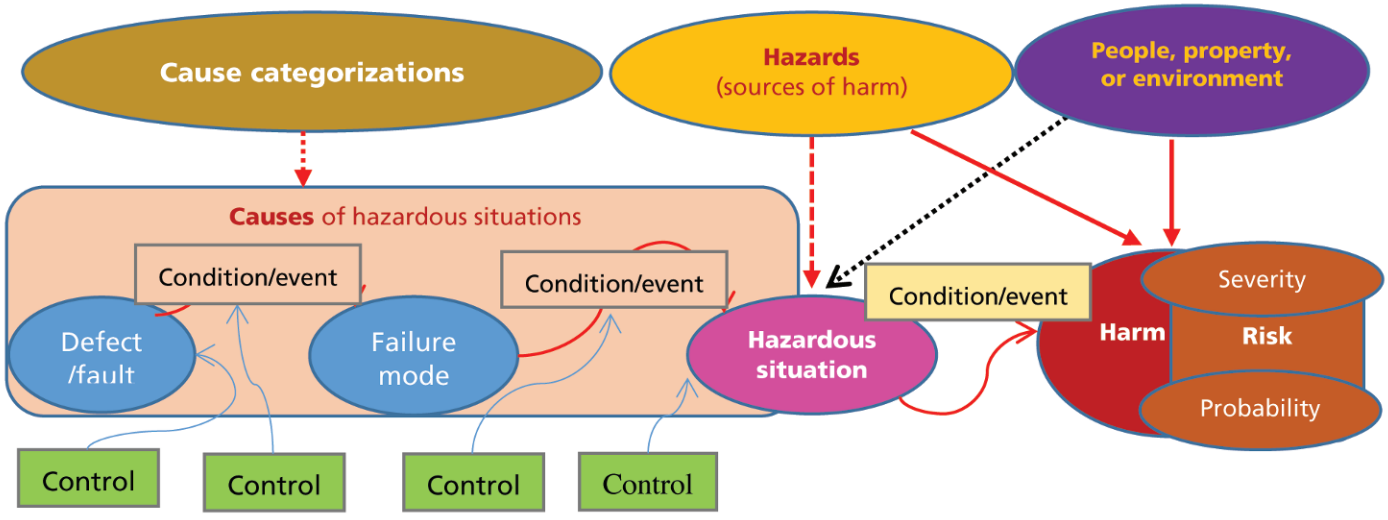

Figure 1. Risk analysis taxonomy and causal chains[12]

end-to-end system standpoint. Following this principle, one can see risk comprehensively and keep it in perspective. However, risk principles can be overlooked or improperly executed in a number of ways.

Pitfalls

Not considering other factors. Risk analysis should include analysis of the potential failures of medical devices, with adequate consideration of whether certain device functions can lead to a hazardous situation *in the absence of failures*, as well as other factors (e.g., evolving use and environment conditions) that can influence or introduce new risks.

For instance, some developers still use FMEA exclusively rather than supplementing it with other risk analysis techniques. This results in inadequate top-down system analysis (including preliminary system hazard analysis and fault tree analysis) to identify hazardous scenarios contributed by normal functions, system-level conditions, and events. Another example would be the development of a drug delivery device that is designed for specific drugs but also used broadly for delivering other drugs or solutions, without considering new or different risks potentially resulting from interactions among device, drug, and use conditions. A recent FDA safety communication[13] is a good reminder that using a device to deliver medications for which the device was not designed and approved can pose significant risk.

Not analyzing foreseeable use conditions. Classifying or evaluating a device based solely on risks associated with its categorical intended functionality—without adequate analysis of foreseeable use conditions specific for the device—is another pitfall.

For example, this risk management peril can emerge for medical device data systems (MDDSs) and mobile medical apps (MMAs). In general, MDDSs and MMAs tend to have lower risk compared with traditional medical devices. However, for a given MDDS or MMA, the specific risk profile can be very different from the general risk profile, particularly with the current complexity of digital health, mobile device technologies, and network connectivity.

For example, if an MDDS is connected to and used by another device that delivers therapy or performs critical diagnosis directly, then—just as with any physical medical device—a failure, malfunction, or cybersecurity vulnerability associated with the MDDS could lead to patient harm.

Although MDDSs and certain MMAs are subject to less vigorous regulatory oversight from the FDA, risk analysis itself should never be discounted or ignored. It is exciting to see companies such as Google, IBM, and Apple participating in the advancement of healthcare and medical applications. However, it remains vitally important that these fast-moving, high-tech entities have comprehensive risk management programs in place to inform what would be a suitable quality system for their medical applications. It is a significant risk for regulators to create a compliance scenario based on an application's intended functionality without requiring the developer to perform adequate risk management.

It is a significant risk for regulators to create a compliance scenario based on an application's intended functionality without requiring the developer to perform adequate risk management.

Inappropriate assumptions. Another pitfall is classifying risk based on the inappropriate assumption that the rest of the healthcare delivery ecosystem will detect errors before the patient is harmed.

For example, at one time, drug dosage calculator software was proposed as being in a low-risk device class because the software does not directly touch the patient and downstream clinical processes (e.g. patient or caregiver review and an insulin delivery device) and "safety checks" exist to protect the patient. Although these downstream systems may catch dosage errors before they reach patients, a patient, caregiver, or delivery device maker could assume that the software, as a dosage calculator, will provide the right dosage and not perform additional checks of its accuracy. In that case, a dosage error by the software can result in a hazardous situation similar to the type of dosage error that can occur within an infusion pump. In fact, performance-based research

suggests that medical apps, such as insulin dosage calculators, may place patients at risk of catastrophic overdose, as well as at risk of more subtle harms resulting from suboptimal glucose control.[14] Thankfully, medical apps such as insulin dosage calculators continue to be regulated as high-risk devices.

Effective Risk Management

Effective risk management is not about completely eliminating all risks. As stated in the introduction to 14971, "use of a medical device entails some degree of risk."[1] Effective risk management is about identifying and differentiating high and low risks, as well as making risk control choices and decisions that are balanced with consideration of benefits. Advances in science, technology, and healthcare connectivity have increased the difficulty in risk management decision making. Many decisions are subjective within certain contexts or rely on certain assumptions. Without proper context or rationale, risk management decisions and conclusions are challenging for internal or external reviewers to follow.

As stated in AAMI TIR38:2014,[15] "a challenge with ANSI/AAMI/ISO 14971 is that it does not require a formal, organized summary of why the device is safe for its intended use. While 14971 requires a series of discrete analyses and reports, there is no overview document that provides a roadmap to product risk ... and does not *tell the story of safety*. A reviewer is often faced with thousands of pages of design documentation, with no overall summary as to why the designers believe the product is safe. Additionally, if the reviewer is interested in a particular issue, there is no roadmap to finding that issue within the design documentation."

Safety assurance cases have been used by some European countries for mission-critical systems and for U.S. defense and aviation projects. The FDA has formally introduced the assurance case method to the medical industry through its guidance in 2014.[16] According to the FDA, a safety assurance case (or safety case) is a structured argument supported by a body of valid scientific evidence that provides organized information that a medical device adequately addresses risks associated with its intended use within its environment of use. The assurance case method requires elements of context, assumption, argument, and evidence, thereby providing an intuitive way to capture typically undocumented safety-critical information, knowledge, and rationale. In addition, when constructing and developing an assurance case in parallel with product development, the questions (and answers) of, "Why these hazards, why these causes, why these risk controls, why these specifications, and why this testing?," are constantly being exercised at the time decisions are made. This provides effective checks and balances to help developers make better, safer decisions.

The AAMI Infusion Devices Working Group has developed TIR38 with detailed instructions on how to construct safety assurance cases for medical devices. As explained by Eagles and Wu,[17] from a methodology perspective, assurance cases can address a number of limitations in risk management practices. Years of experience with infusion pump safety assurance cases have also revealed that in addition to providing better quality information for internal and external reviewers, assurance cases help manufacturers identify and address shortcomings in existing risk management practices. This results in improved risk analysis, risk control measures, design reviews, and risk control verification and validation. The FDA, however, has not extended the requirement of safety assurance cases for other devices than infusion pumps.

Similar to any other engineering method, incorrect or superficial implementation of the assurance case method will result in a "paper exercise" with little or no value to product safety. Getting the assurance case right requires an open mind and willingness to improve practices among those in healthcare. Tools for developing assurance cases have advanced significantly; some can even draft assurance cases automatically based on ongoing risk management results, then prompt users to provide additional information needed to complete the cases. This greatly reduces manual work, which is a concern of many in the industry.

Similar to any other engineering method, incorrect or superficial implementation of the assurance case method will result in a "paper exercise" with little or no value to product safety.

As medical devices and our healthcare systems rapidly and continuously advance, and therefore become more complicated, integrating assurance case method into risk management offers a great opportunity to advance regulatory science.

Regulatory decision making requires application of the best available science and tools to keep pace with healthcare advances, support innovation, and protect and promote the public health. However, implementing these measures requires adequate understanding of risk within the context of our evolving healthcare ecosystem, as well as continuous, candid communication among engineers, clinicians, and regulators. Understandably, decisions at a policy level are difficult, as regulators do not have visibility into technical risk management documentation unless and until the products are received for review. As such, it is important for regulatory policy to require and promote good risk management practices for individual medical application developers to proactively perform adequate risk analysis, rationalize risk-level conclusions, and justify the adequacy of corresponding quality management systems.

Implementing these measures requires adequate understanding of risk within the context of our evolving healthcare ecosystem, as well as continuous, candid communication among engineers, clinicians, and regulators.

Comprehensive and rational risk management is an essential tool in the design and development of medical devices and a cornerstone for advancing regulatory science.

References

1. ANSI/AAMI/ISO 14971:2007/(R)2016. *Medical devices—Application of risk management to medical devices*. Arlington, VA: Association for the Advancement of Medical Instrumentation.
2. ICH Q9:2005. *Quality Risk Management*. Geneva: International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.
3. IEC 60812:2018. *Failure modes and effects analysis (FMEA and FMECA)*. Geneva: International Electrotechnical Commission.
4. ISO 31000:2018. *Risk management–Guidelines*. Geneva: International Organization for Standardization.
5. ANSI/AAMI/ISO 13485:2016. *Medical devices—Quality management systems—Requirements for regulatory purposes*. Arlington, VA: Association for the Advancement of Medical Instrumentation.
6. ISO 10993-1:2018. *Biologic evaluation of medical devices—Part 1: Evaluation and testing within a risk management process*. Geneva: International Organization for Standardization.
7. IEC/TR 80002-1:2009. *Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software*. Geneva: International Organization for Standardization.
8. IEC 62366-1:2015. *Medical devices—Part 1: Application of usability engineering to medical devices*. Geneva: International Organization for Standardization.
9. ISO 14155:2011. *Clinical investigation of medical devices for human subjects—Good clinical practice*. Geneva: International Organization for Standardization.
10. ANSI/AAMI/ISO TIR24971:2013. *Medical devices—Guidance on the application of ISO 14971*. Arlington, VA: Association for the Advancement of Medical Instrumentation.
11. Global Harmonization Task Force. *Quality management system—Medical Devices—Guidance on corrective action and preventive action and related QMS processes*. Available at: www.imdrf.org/docs/ghtf/final/sg3/technical-docs/ghtf-sg3-n18-2010-qms-guidance-on-corrective-preventative-action-101104.pdf. Accessed Dec. 14, 2018.
12. Wu F, Kusinitz A. Best Practices in Applying Risk Management Terminology. *Biomed Instrum Technol*. 2015;Spring(suppl):19–24.
13. Food and Drug Administration. Use Caution with Implanted Pumps for Intrathecal Administration of Medicines for Pain Management. Available at: www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm625789.htm. Accessed Dec. 18, 2018.
14. Huckvale K, Adomaviciute S, Prieto JT, et al. Smartphone apps for calculating insulin dose: a systematic assessment. *BMC Med*. 2015;13 106.
15. AAMI TIR38:2014. *Medical device safety assurance case report guidance*. Arlington, VA: Association for the Advancement of Medical Instrumentation.
16. Food and Drug Administration. Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff. Available at: www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf. Accessed Dec. 18, 2018.
17. Eagles S, Wu F. Reducing Risks and Recalls: Safety Assurance Cases for Medical Device. *Biomed Instrum Technol*. 2014;48(1):24–32.

Starting a company is risky enough. Let us help.

Premarket Risk Management for New Medical Device Companies

The guide you need to succeed in today's market.

For more information and to order, please visit **www.aami.org/store.**

Product Code: PRM and PRM-PDF

www.aami.org

AAMI
Advancing Safety in Health Technology