Medical Device Cybersecurity & Privacy:

Medical Device "Frameworks and Standards"

This is the second offering in our series on cybersecurity and privacy impacting medical devices and medical technology. Stay tuned for more on emerging trends, opportunities, and challenges. For additional information, contact a member of our life sciences cybersecurity services team.

No need to wait as frameworks and standards are known and generally accepted.

Effective cybersecurity, privacy, and risk management are top priorities for medical device manufacturers (MDMs) and providers. However, some have struggled with where to start and to what extent to commit their finite resources. The Food and Drug Administration (FDA) is expected to help with that effort in the near future by progressing from pre- and post-market recommendations[1] based on industry standards to specific directives and requirements that companies must follow.[2] We expect other regulators across multinational jurisdictions to follow suit, and for a convergence in medical device cybersecurity and privacy requirements to materialize.

In the final versions of both the pre- and post-market guidelines, the FDA recommends using a number of industry accepted frameworks and standards and standards to model enhanced cybersecurity, privacy, and risk management programs. Requirements have not been finalized, though MDMs and providers should not wait as frameworks, standards, and capabilities are generally agreed. Organizations should work proactively and design, build, implement, sustain, and govern improved cybersecurity and privacy practices.

The following is a recommended framework and a few of the standards that, in our professional experience, are critical for MDMs and providers to consider. It is equally important to consider how to apply your organization's selected framework and these standards (1) throughout different stages in a device's life cycle, and (2) in accordance with your organization's cybersecurity and privacy program maturity.

NIST Framework for Improving Critical Infrastructure Cybersecurity

The NIST Framework for Improving Critical Infrastructure Cybersecurity is an executive order that calls for the development of a voluntary risk-based cybersecurity framework to help organizations that are part of critical infrastructure, such as MDMs and providers, allocate resources to manage cybersecurity based on identified risks.[3] The FDA, in their post-market guidance, encourages MDMs to use and adopt this framework in order to provide a common mechanism for incorporating foundational cybersecurity, privacy, and risk management concepts into each respective program. The framework describes the full cybersecurity risk management process and how it can be used to manage cybersecurity risk by focusing on critical services within an organization.

Whether or not your organization decides to adopt NIST or another cybersecurity framework, the important variable is to select a framework that clearly articulates risk and defines a target operating model.
The NIST framework includes an extensive list of proposed cybersecurity controls. Organizations must select specific controls that align with their own unique processes and associated risks. By choosing from a pool of common controls from your chosen framework, MDMs and providers can be confident that they are implementing controls that are common across industries, and are speaking in commonly understood terms.

Cybersecurity would not exist without privacy.

Your organization's selection of a cybersecurity framework, should also include selection of a privacy framework as part of this process. Generally Accepted Privacy Principles (GAPP)[4] facilitate management of privacy policies and programs on a local, national, and international level. Cybersecurity and privacy practitioners, among other professionals, face a number of differing privacy legislation and regulations. The GAPP offers a comprehensive framework for designing an effective privacy program that can be applied within the MDMs and provider industries and professions.

[1] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," accessed February 13, 2017, FDA Web site.
[2] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," accessed February 13, 2017, FDA Web site.
[3] "Cybersecurity Framework," accessed February 10, 2017, NIST Web site.
[4] "Cipp Guide of Generally-Accepted-Privacy-Principles," CIPP Web site

GAPP is a principles based framework that should be considered when designing, building, implementing, and governing privacy related standards, controls, and expectations. This framework allows organizations to establish the building blocks of privacy and helps achieve the varied privacy requirements defined across legal jurisdictions.

ISO standards

The FDA's finalized pre- and post-market guidelines reference and recognize a large number of International Organization for Standardization (ISO) standards. While each standard provides unique and relevant guidance on how organizations can integrate cybersecurity practices, the following three are most pertinent to medical devices, and offer an opportunity today to start designing, building, and implementing cybersecurity and privacy improvements. Understanding and introducing changes in accordance with established industry standards can launch your medical device cybersecurity, privacy, and risk management programs today in advance of requirements.

ISO 14971:2007, Application of Risk Management to Medical Devices

The ANSI/AAMI/ISO 14971:2007/(R)2010 International Standard (ISO 14971) specifies a process for MDMs to identify the hazards associated with medical devices, to estimate and evaluate the associated risks, to implement controls to mitigate these risks, and to monitor the effectiveness of these controls.[5] This standard's scope includes all medical devices, including in vitro diagnostic medical devices. Requirements of this standard must be applied to all stages of the life cycle of a device, from the initial concept and design straight through to end of life and disposal. By following recommended standards such as ISO 14971, and aligning with its intent, MDMs will be able to establish a solid foundation for controlling risk. It should be well noted that compliance does not translate into security. Organizations must perform additional assessments and develop device profiles, a target-state operating model, and a medical device cybersecurity road map, as well.

As defined within ISO 14971, management must take ownership of the process by carefully documenting a risk management and cybersecurity plan. Every time a new medical device enters the design phase, it must have a documented risk management plan included in its overall risk management file. The plan must be submitted to the FDA as part of the 510(k) or premarket approval (PMA).[6] The PMA defines the scope of all activities, includes a detailed technical risk assessment, and describes the plan for vulnerability and other technical testing at every stage gate of the design process. It is management's responsibility to ensure that the risk management process has sufficient resources, including qualified personnel. Finally, management must provide a documented and defendable review cycle of the entire risk management process, so that iterative improvements can be identified and implemented.

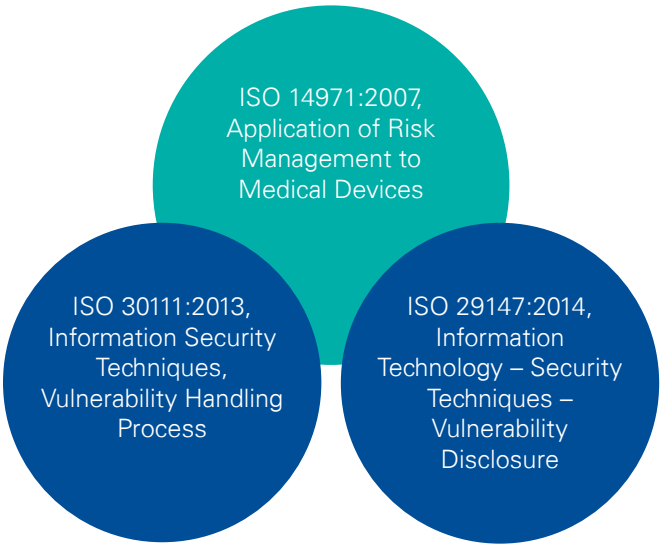
ISO 14971 provides all the guidance necessary to implement risk management processes that align with leading industry practices. If MDMs do not already have risk management processes in place, then they must do so in the interest of complying with future standards and soon to be released requirements. For MDMs with existing risk management processes in place, we strongly recommended that your organization benchmark existing processes against ISO 14971 to ensure that they are in alignment with leading practices.

ISO 30111:2013, Information Security Techniques, Vulnerability Handling Process

The ISO/IEC 30111:2013 International Standard (ISO 30111) provides guidelines on processing and resolving potential vulnerabilities discovered in a product or online service. While ISO 30111 is intended for all organizations, MDMs and providers can leverage the standard to elevate their cybersecurity profiles and overall security posture.

ISO 30111 is not tied to any one source of vulnerability reports, e.g., an organization's own security, development, or testing teams, outside vulnerability researchers, or an Information Sharing Analysis Organization (ISAO), such as the FDA-endorsed National Health Information Sharing & Analysis Center.[7]

Risk Management and Mitigation



[5] "ISO 14971:2007 Medical Devices – Application of Risk Management to Medical Devices," accessed February 10, 2017, ISO Web site.
[6] "Premarket Notification 510(k)," accessed February 20, 2017, FDA Web site.
[7] "Postmarket Management of Cybersecurity in Medical Devices," accessed February 3, 2017, FDA Web site.

ISO 30111:2013, Information Security Investigations, Triage, and Resolution of Vulnerabilities

ISO 30111 describes how organizations can better handle internal investigations, triage, and resolution of vulnerabilities.

MDMs must update their vulnerability management processes to integrate with, as well as meet the needs of, the early phases of their SDLCs. Early detection and remediation of vulnerabilities can significantly reduce the probability of a cybersecurity incident. The International Cost Estimating and Analysis Association (ICEAA) has shown that early testing through each phase has a positive impact, significantly reducing the total cost of ownership (TCO)[8] by avoiding late-stage changes as well as costly emergency updates and patch distributions once devices are in service.

To complement vulnerability detection, internal development processes must be continually updated and strengthened so that high-risk vulnerabilities are prioritized for prompt remediation. A common mistake is to have inadequate budget and resources earmarked for post-production fixes and related support.

ISO 29147:2014, Information Technology – Security Techniques – Vulnerability Disclosure

The ISO/IEC 29147:2014 International Standard (ISO 29147) addresses the interface between organizations and external parties who either discover vulnerabilities or use devices and/or products that are affected by vulnerabilities. ISO 29147 covers actions including reporting, publishing information about a vulnerability, and steps for resolution.

The standard provides guidelines on how to effectively take in vulnerability reports from outside parties (independent researchers, end users, other MDMs, providers, integrators, etc.) by setting up a secure communication channel where outside parties can submit vulnerability reports, while keeping sensitive information private. The standard also addresses how to disclose vulnerability information to device users, including guidance on timing, information that can be shared, and information that must be kept private. Finally, the standard outlines how to report vulnerability findings to other MDMs, providers, etc., either privately or through an ISAO.

MDMs and providers must define and implement a vulnerability disclosure policy and associated procedures. It is customary for organizations to limit the release of vulnerability information to situations where there is a prescribed remediation plan. However, it should be noted that high-severity vulnerabilities that are being actively exploited must be disclosed immediately.

MDM and provider leadership must assume positions of leadership within the industry. This includes taking an active and participating role and become invested and engaged, as well as encouraging other leaders to remain open to sharing vulnerability information with the greater community. The first step is to actively participate in the FDA-endorsed ISAO and the National Health Information Sharing and Analysis Center.[9] Sharing threat vulnerability information within the community will help strengthen the security and privacy posture of the industry as a whole. In this manner, organizations are constantly made aware of the current threat landscape and active threats that other organizations are experiencing.

Cybersecurity and Data Privacy Around the World[10]

This thought leadership paper is topical and offers guidance in response to medical device cybersecurity and privacy. This is real-time and we encourage a principles based approach to this subject. As such, we would like to profile the recently released guidelines and cybersecurity laws from China within this paper.

The China Food and Drug Administration (CFDA) has issued guidelines to implement China's new Cybersecurity Law (CSL) in the administration of medical devices in China. This is very similar to the pre- and post-market guidelines from the U.S. FDA over the past few years. This development is a clear indicator that Chinese regulations intend to focus on and enhance both cybersecurity and privacy protection in the healthcare sector. The CFDA guidelines and CSL further reinforce KPMG LLP's positions on the need for a global focus and collaboration across this industry sector. This includes your organization's selection of a framework, related standards, and a principles-based approach to medical device cybersecurity and privacy.

The new registration requirement, CFDA guidelines, and CLS all have major implications to MDMs. As cybersecurity threats and related cyber risks may lead to the violation of patient privacy, or a network breach may pose risks including injury or the potential for loss of life from operational malfunctions, MDMs need to pay close attention to these issues throughout the devices' system development life cycle. Applicants need to be aware that while the CFDA Guidelines are not mandatory obligations, the failure to meet the requirements can potentially delay the product registration. In simple terms, noncompliance with this process can have a negative impact of the success and timing of launching and rolling out a new medical device product in China. Organizations should expect to see similar guidelines and expectations from other Countries over the coming months.

8. "Postmarket Management of Cybersecurity in Medical Devices," accessed February 3, 2017, FDA Web site.
9. "Postmarket Management of Cybersecurity in Medical Devices," accessed February 3, 2017, FDA Web site.
10. http://www.bakerinform.com/home/2017/4/3/new-china-cybersecurity-guidelines-for-registration-of-networked-medical-devices

Conclusion: Using frameworks and standards moving forward

MDMs should immediately review the recommended NIST framework and the ISO standards highlighted in this paper. The framework and standards provide guidance for the development and/or transformation of medical device cybersecurity, privacy, and risk management programs, as well as related processes so that MDMs and providers alike, comply with the finalized FDA guidelines (and regulations) and align with leading industry practices. Taking these steps now will better prepare MDMs and providers for imminent mandatory standards and regulations, and situate each in a position of strength in comparison to their peers.

Transformations of this nature and magnitude take time, so MDMs and providers must begin selecting a framework and applying these standards—now. KPMG, LLP has helped organizations transform their cybersecurity risk frameworks and related processes in line with leading practices, including the NIST framework and ISO standards outlined above. Our cross-functional teams have both the broad industry understanding and deep technical experience to successfully implement these leading practices in the medical device industry, as well as provider communities.

Contact:

Larry Mraz
Director, Advisory,
Medical Device Cybersecurity Lead
T: 973-912-6161
E: lawrencemraz@kpmg.com

David Remick
Partner, Advisory,
Life Science Cybersecurity Lead
T: 404-222-3138
E: jremick@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia