PARAGON CONSULTING PARTNERS

PCPIMAGING.COM

The Innovator's Guide to Health IT

Top considerations for entering the healthcare market

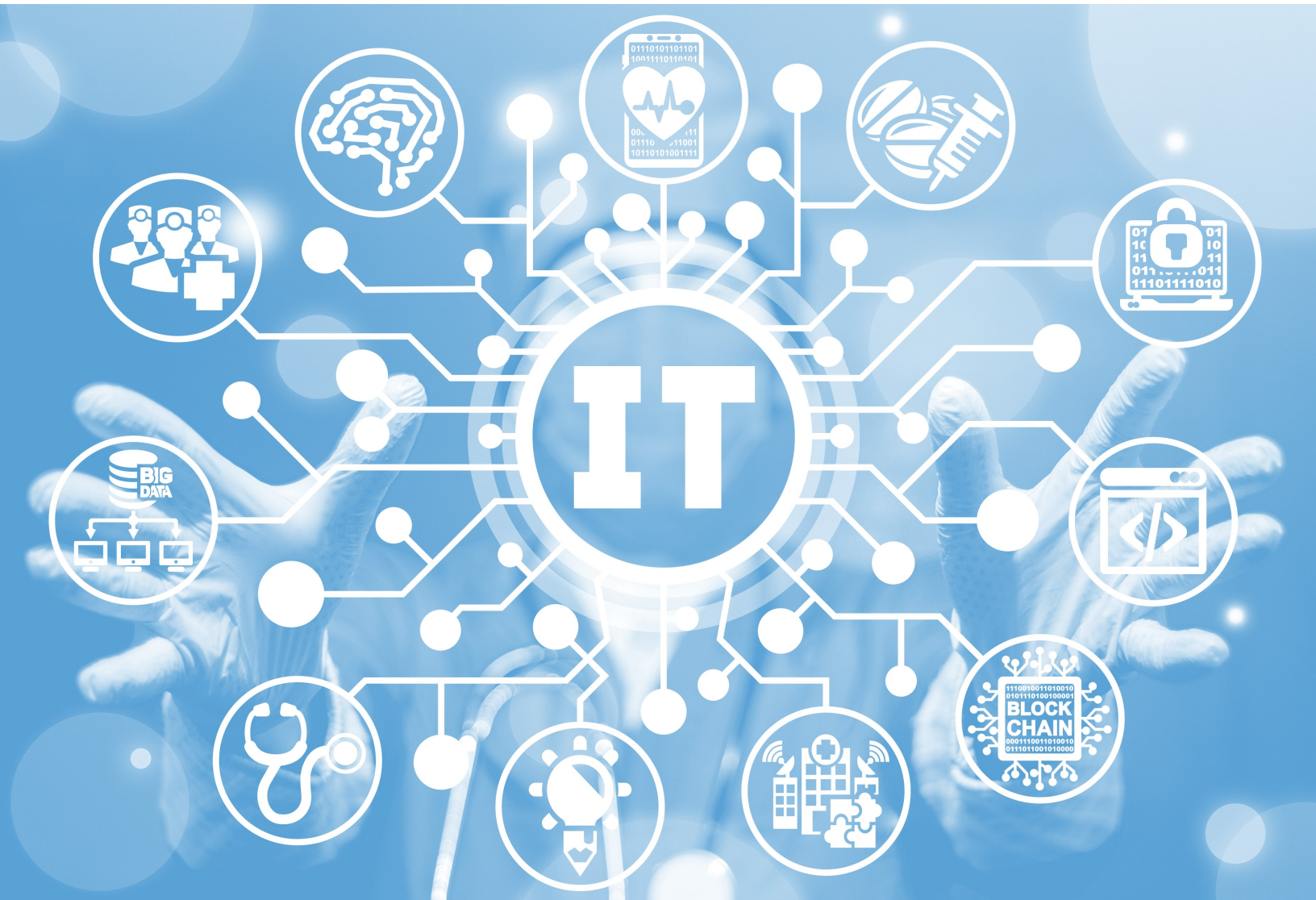


Table of contents

Introduction

In today's rapidly evolving digital landscape, where technologies such as data lakes, blockchain, artificial intelligence, machine learning, and IoT devices continue to emerge, the opportunities for health innovators to develop and launch new products with the potential to improve healthcare for consumers and providers alike seem limitless. However, unlike the consumer sector where such products have already gained a foothold, the healthcare market presents a unique set of requirements and challenges that Health IT innovators must face before their promising applications can be brought to market, adopted, and used in clinical settings.

The first step is ensuring your innovation is well designed to address your target market's top priorities – whether they be health consumers, independent providers or facilities, or large healthcare systems. As well, since your innovation will be managing personal health information you must be familiar with and adhere to all applicable privacy requirements and regulations – whether government or customer driven. Finally, if your innovation will be considered a medical device (and even if it's not), you must ensure appropriate processes and controls are in place to guarantee that your product will be safe, effective, and secure once it is released into the hands of health consumers and care providers.

Marketing to discerning healthcare organizations

Three things are particularly important in the healthcare market. First, healthcare executives and providers are busy. Very busy. Second, they are almost always budget constrained. A common saying in the healthcare industry, albeit painfully overused, continues to hold true – healthcare providers are constantly being called upon to do more with less. Finally, no two healthcare organizations are the same. For healthcare innovators hoping to gain a foothold in the market this means that you need to know your audience, demonstrate value (what's in it for them), and be flexible.

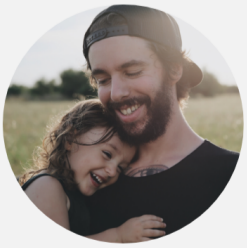
Know your audience

Successfully introducing a new innovation into a healthcare organization typically requires buy-in from a variety of different stakeholders across business, technical, and clinical roles. These stakeholders carry varying degrees of influence on their organization's decision-making process, therefore a savvy Health IT innovator will get to know each one so that they can better understand their unique needs, their role in the decision-making process, and how much influence they bring to bear on whether or not the innovation will be adopted.

The examples below provide a starting-point for persona development, including what type of information should be included. When defining your own personas, be sure to identify the specific needs and challenges that your innovation is meant to address and include a concise list of its specific benefits for each persona. To get the most out of this activity it is important not to over-generalize; each persona is unique and should be treated as such – take the time to really understand how each behaves, what motivates them, what frustrates them, how will they measure success, etc. In doing so, you will be in a better position to tailor your messages and pitches in a way that will really resonate (more on that later).

Health Consumer

Dan is a single working dad. When he's not working his day-job, he's driving his two daughters to dance classes and hockey practices. Dan tries to encourage a healthy lifestyle for his family but being on-the-go so often makes this challenge.



Goals:

- Keep his family healthy
- Access care that is reliable and convenient when its needed for himself or his daughters
- Stay on top of his family's health information so he can easily share it when needed with care providers or specialists

Challenges:

- Maintaining a healthy lifestyle for himself and his daughters
- Scheduling appointments around his busy schedule
- Knowing where to find, or how to access his family's up-to-date health information

How can you help?

Family Physician

Dr. Grace runs her own family practice, sometimes seeing ~100 patients per week ranging in age and complexity of care. Dr. Grace wants to be there for every patient – and as a result typically has a very demanding schedule and sometimes struggles with burnout.

Goals:

- Keep all of her patients healthy and happy by being available, attentive, and proactive
- De-burden local emergency rooms and clinics by ensuring her patients are able to be seen in a timely manner when needed
- Reduce wait times and congestion in her office by staying on-schedule
- Improve her work-life balance

Challenges:

- Documenting and tracking her patients' health information in a way that is quick and accessible by herself and her patients
- Gaining access to health data that wasn't initiated from her office (i.e. lab tests, imaging results, hospital visits, etc.) for her patients
- Staying in-the-loop with outside care providers or specialists regarding her patients' health

How can you help?

Hospital CTO

Richard is responsible for the development, maintenance, and support of the IT infrastructure and software applications for a growing hospital system.

Goals:

- Ensure all hospital IT systems are available and performing well
- Protect the security and privacy of all protected health information
- Identify new and innovative ways to improve care delivery and reduce costs through IT
- Effectively manage rapid growth from service line expansions and facility acquisitions

Challenges:

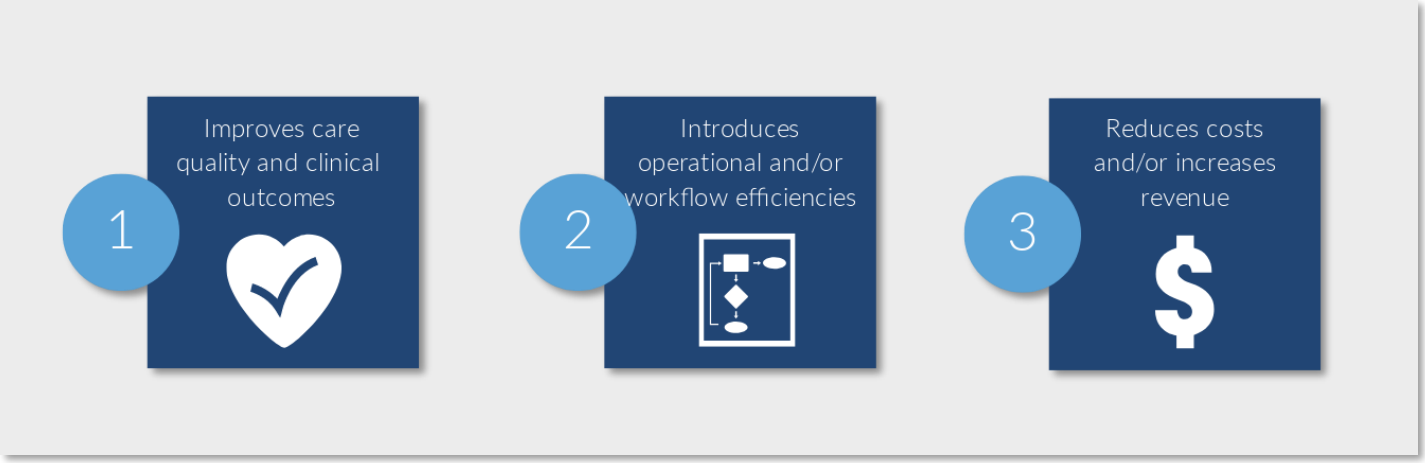
- Managing a diverse array of legacy systems, with varying degrees of interoperability
- Obtaining budget for capital and operational IT improvements and enhancements
- Gaining buy-in and budget dollars for new IT project initiatives

How can you help?

Demonstrate value

Introducing a new innovation into a healthcare environment is no easy task. Healthcare organizations and providers are notoriously resistant to change – and for good reasons. First, change often carries risk, and risk is to be avoided at all costs when a patient's comfort, health, or life is on the line. As well, care providers are busy, and are only getting busier as demand for care services continues to out-grow supply (i.e. physicians, diagnostic equipment, hospital beds, etc.). Finally, most healthcare organizations are budget constrained, tasked with providing high-quality care to a growing number of health consumers while simultaneously having to cut costs wherever possible.

First and foremost, for Health IT innovators this means that your product needs to deliver tangible and measurable value that ultimately provides one or more of the following:



To convince a care provider that your innovation will deliver a sufficient return on investment you need to be able to quickly and effectively communicate how your technology will deliver some or all of the aforementioned benefits and head-off potential concerns about risk to patients, operations, or the bottom line. Remember that each persona has different challenges and motivations, so tailor your messages accordingly using concepts and terminology that they can relate to and understand. The following list provides some tips on how to create effective and compelling messaging:

Focus on the benefits, not the features:

While your innovation may have tons of cool features, focus on evangelizing the benefits they provide. Customers often become overwhelmed and confused with lengthy feature lists and can quickly lose interest. Focusing on the benefits will more effectively capture their attention.

Identify your key messages:

Map your product's distinct benefits to the needs of each individual persona and use these to create concise and targeted statements that can be used on their own, or as the foundation for a variety of marketing content.

Use vivid imagery:

Spicing up your content with relevant imagery helps you to stand out, capture and keep your audience's attention, and is proven to aid in memory retention. Keep in mind, images don't always have to be literal – be creative!

Tell a compelling story:

Describe what the world looks like today without your innovation and why it needs to change – use a real-life story if you can. Then, describe what the future could look like with your innovation adopted; what's different, and why is it better?

Back up your claims:

Anyone can make statements promising vast improvements – but referencing quantifiable statistics or qualitative testimonials such as client quotes or case studies where your innovation was used successfully will bring added credibility to your message and your innovation. For brand-new innovations that have not yet been deployed in a live environment consider internally generated performance statistics or information about any outside providers or organizations with whom you have been collaborating as an interim substitute.

Be flexible

Every healthcare organization is unique – while they share common goals, and sometimes even tools, there are always variations in clinical workflow steps and data management and utilization policies and practices. This means that very few, if any, Health IT solutions will work 'out-of-the-box', and to be successful in this diverse landscape Health IT innovations must be able to flexibly adapt to their environment. The table below outlines the top areas that should be considered:

Configurability	How easily can your product be configured to accommodate variations in clinical workflow processes or user preferences?
Interoperability	Does your innovation adhere to the relevant industry standards and/or best practices for integration and information exchange (i.e. IHE)? Does your innovation offer advanced programming interfaces (APIs) for advanced integrations? How accessible is the data generated and/or stored within your product to other integrated systems? Conversely, how easily can your product access and leverage outside data?
Extensibility	How easily can new functionality be added to or extended upon within your innovation? How agile are your development practices, and how adaptable is your technology platform? How easily can extended functionality be validated to ensure it is safe and effective?
Scalability	How easily and cost effectively can your innovation scale to accommodate organic or rapid growth (i.e. due to acquisitions or system consolidations)? How are system performance and business continuity assured during periods of growth?

Offering an even deeper level of agility, the concept of Innovation Procurement, which involves healthcare organizations evaluating Health IT vendors based not only on their current capabilities but also for their potential as innovation partners for collaboratively designing new or better solutions, is becoming increasingly popular among academic and forward-thinking institutions. This approach calls for

innovators to be nimble and transparent in their product design and future roadmap, and in-turn offers several advantages including the ability to iterate and validate ideas with representative end-users before incurring the cost and effort of commercialization, and providing a competitive edge when vying for deals against larger, more established (and less nimble) vendors.

To learn more about Innovation Procurement, check out this Primer on Innovation Procurement.

Want to know more about Health IT marketing?

Our team is well-versed in Health IT product development and marketing (both upstream and downstream) practices, including persona profiling, requirements definition, strategic roadmap planning, content development, communications, and sales strategy. If your organization could use some help with your Health IT marketing strategy or execution contact us for a free consultation.

The implications of managing health information

Most Health IT products deal with some form of protected health information (PHI), which is any information about a person's past or present health status, provision of care, or payment for health services that is generated by a healthcare provider, organization, or one of their business associates (such as a Health IT vendor, for instance). This means that any software application that generates, stores, or accesses this type of information must adhere to the federal privacy and security regulations that are designed to protect this sensitive data.

What are HIPAA and PIPEDA?

In the North American market there are two laws which govern the protection and management of health data; the US Health Insurance Portability and Accountability Act (HIPAA) and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). Which one(s) your innovation must adhere to is based on where it is marketed and sold. While there are differences between the two, they are largely similar, outlining the following macro-level requirements:

Physical safeguards	• Physical access controls for facilities where health data is stored (i.e. data centers) • Physical access controls to locations where health data can be accessed (i.e. via a workstation) • Policies about the appropriate access and use of PHI for anyone who has access to health data (i.e. software engineers or support specialists)
Technical safeguards	• Data encryption • Unique user identifiers (i.e. no shared logins) • Strong password policies • Audit logging and reporting for all instances where health data was accessed, altered, or deleted
Data Integrity safeguards	Business continuity controls to protect against the loss or destruction of health data (i.e. system redundancy, backup and recovery, etc.)
Security safeguards	Protect against unauthorized access to health data (more on that in the section below)

It is important to note that each state or province may have its own unique extensions to the above requirements. For example, whether or not health information can be transmitted and stored outside of the country, or even state/province where it was generated, as is often the case in cloud-based deployments. Thus, it is important to become familiar with the regulatory environment in each region where your innovation will be offered to ensure conformance.

How does this apply to consumer generated data?

One of the most notable differences between HIPAA and PIPEDA – particularly for consumer-focused IoT or mobile health applications and devices – is the way each approaches data that is uploaded by health consumers themselves, such as health statistics from an Apple Watch, FitBit, or other consumer wearables or apps. Under HIPAA, this information is not viewed as PHI and is therefore not subject to the same security and privacy regulations. PIPEDA, however, is more stringent and applies to all personal information, health or otherwise. Therefore, businesses managing consumer generated data are held to the standards as healthcare organizations and their associates.

Do we need an ISO 27001 certification?

> The Industry Organization for Standardization (ISO) 27001 certification defines the best practices for an information security management system (ISMS) to govern PHI access, handling and storage.

The focus of ISO 27001 is not on the PHI itself, but on the physical systems and policies that organizations put in place to ensure secure infrastructure and protect data. While it is not mandatory under HIPAA or PIPEDA, it is typically requested and required by healthcare organizations who are purchasing IT systems, as it ensures that

their technology vendors have the necessary controls in place to guarantee safe handling of any PHI that will flow through their system or be handled by their employees.

Want to know more about managing health information?

For more information about HIPAA, check out HIPAA for Professionals. For more information about PIPEDA, check out Privacy Laws in Canada. For more information on ISO 27001, check out SO/IEC 27000 family - Information security management systems.

Our team has decades of hands-on experience in medical device software engineering, including the implementation of HIPAA, PIPEDA, and ISO 27001 compliant systems, policies, and audit processes. If your organization could use some help with your ISMS contact us for a free consultation.

Security: a top-of-mind concern

Security has always been a top-of-mind concern for healthcare organizations because of the critical and confidential nature of the information they generate and house. Recently security has become a hotter topic than ever due to the surge in ransomware attacks worldwide, but also because of the growing volume of data and the increasing complexity associated with the web of systems and devices generating and accessing it.

For instance, while Wifi or Bluetooth enabled medical equipment can simplify and improve patient care for clinicians, if an intruder were to gain control of a life sustaining system, such as a wifi-enabled drug infusion pump, there could be very serious safety ramifications. Similarly, while mobile and IoT applications can provide 'anytime, anywhere' information capture and viewing capabilities that are invaluable for closing the information gap, those with weak and inconsistent security controls can expose health networks to vulnerabilities – in fact, nearly half of U.S. firms using such devices are reported to have experienced a security breach as a result.

Emerging threats and vulnerabilities

Unfortunately, hackers recognize the value of the information contained within patient health records, making healthcare the largest target for ransomware attacks compared to any other industry. Not only are covered entities subject to financial penalties under the Health Insurance Portability and Accountability Act (HIPAA) for breach of protected health data, but even worse - such records can be rendered inaccessible by attackers, who can withhold critical life or death information from care providers until a ransom is paid. The result is significant fiscal and clinical implications for providers and patients.

There are many methods available for resourceful attackers to wreak havoc on an unsuspecting healthcare organization. In addition to the popularized ransomware attacks, other potential breaches could include brute force attacks, where attackers attempt to decipher valid user credentials in order to gain access to the system – either to access protected data, or to install malware.

Yet another example, Distributed Denial of Service (DDoS) attacks take a different brute -force approach, inundating systems with repeated requests that overwhelm servers and prevent legitimate traffic from making it through – effectively rendering the system unusable.

Safeguarding your Health IT innovation

This is by no means an exhaustive list, rather it is merely a few examples of the potential threats that exist. To mitigate these and other vulnerabilities requires a multi-faceted approach. The table below outlines some tangible safeguards that can be implemented to protect against vulnerabilities and improve the security of your Health IT innovation.

Strong passwords	If your innovation doesn't leverage an integrated, secure user management system such as AD/LDS then ensure your application enforces strong passwords that are at least 6 characters in length and contain a combination of upper- and lower-case letters, numbers, and special characters or symbols – and enforce regular updates.

Two-factor authentication	Add an additional protection layer beyond the username/password combo, such as physical or biometric controls (i.e. swipe cards, security tokens, finger print scanners, facial recognition, etc.)
Encryption in transit	Provide secure encryption for your data whenever it is transferred from one location or system to another to prevent unauthorized interception and access (i.e. SSL, TLS, HTTPS, SSH, etc.)
Encryption at rest	Provide secure encryption of idle data in storage to provide an additional layer of security that would prevent a would-be intruder from deciphering or distributing the data in any meaningful way, even if they were to gain access.
System hardening	Only install and activate the operating environment services, packages, and add-ons that are necessary for your product, and always test your innovation against the latest updates and patches to reduce your exposure.
Maintain secure backups	In the event a security breach occurs, ensuring a reliable backup copy of your system and data is available, and a well-tested recovery plan is in place, can minimize the impact and allow operations to continue with minimal, if any, interruption in care delivery.
Security monitoring and alerts	Consider integrating with tools that monitor system access and utilization patterns for your product and provide notifications whenever suspicious activity is identified.

Want to know more about security?

Our team has decades of hands-on experience in designing, developing, and deploying diverse Health IT technologies in a wide array of healthcare settings across North America, and are well-versed in security requirements for vendors and provider organizations. If your organization could use some help with your security strategy contact us for a free consultation.

45% of ransomware attacks in 2017 targeted healthcare organizations

The cost of an average cyber attack now exceeds **$5million**

- Beckers Hospital Review, 2018

Is your innovation a medical device?

If your innovation is brand new and yet to be launched to market, an important consideration will be whether or not regulatory bodies such as the FDA or Health Canada will consider your product a medical device. If so, there are some very important processes and documents you will need to have in place before you can even think about selling – let alone going live – in a regulated healthcare environment.

What is considered a medical device?

The FDA and Health Canada consider any product that is used in the treatment, mitigation, diagnosis, or prevention of disease or abnormal physical condition[1,2] to be a medical device. This includes a wide array of things like tongue depressors, syringes, imaging modalities, software applications that manage patient data, surgical tools, implants, and more. In order to separate the most basic, low-risk medical devices from those that are more complex and inherently carry higher risk for patients medical devices are divided into classes, which determines the regulatory requirements they must adhere to.

[1] https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices.html
[2] https://www.fda.gov/medicaldevices/deviceregulationandguidance/overview/classifyyourdevice/ucm051512.htm

Most IT-based medical devices fall into one of the first two categories, based on the degree to which they alter data or inform diagnosis or treatment for patients. For example, an application that is simply used to collect, store, and display information to a care provider would be considered a Class I device, whereas an application that can change the structure or content of clinical data and/or use it to inform clinical diagnosis or treatment falls into the Class II category.

Class	Risk level	Applies to
Class I	Lowest risk	Non-diagnostic mobile apps, EHR applications, clinical analytics applications, workflow engines, basic archives (non-transformative), etc.
Class II	Low – Medium	Diagnostic imaging software and viewers, computer-aided diagnosis or artificial intelligence tools, implant templating software, data warehouses (transformative), clinical decision support systems, etc.
Class III	Medium – High	X-Ray and ultrasound imaging modalities, respirators and ventilators, limb prosthetics, etc.
Class IV	Highest Risk	Orthopedic implants, pacemakers, cardiovascular stents, etc.

The category to which your innovation belongs and federal regulations will determine the regulatory requirements you must adhere to before you can market and sell your product.

If your innovation is a Class II medical device or higher then you will be required to register your product with federal regulatory bodies (i.e. the U.S. Food and Drug Administration (FDA) or Health Canada) and obtain a license. This process requires that the medical device manufacturer demonstrates that they have a thorough quality management system (QMS) that will ensure the products they release will be safe and effective. In Canada this means obtaining an International Organization for Standardization (ISO) 13485 certification. In the U.S. ISO 13485 is foundational to the FDA's own quality

requirements, however is not (yet) a formal requirement – although this is anticipated to change in the near future[3].

However, even if your product is a Class I medical device it is still a good practice to obtain your ISO 13485 certification, or at least follow the ISO 13485 QMS best practices. Not only will it provide you with a proven framework for delivering high-quality healthcare technology to market, it will also make it easier for you in the future should you choose to expand your product to include regulated use cases.

What is an ISO 13485 certification?

Both the U.S. FDA and Health Canada require companies that produce medical devices – in physical or digital form – to obtain an ISO 13485 QMS certificate. This ensures your business has the proper policies, procedures, and documentation in place to ensure and prove that your final product is safe and effective, and therefore can be trusted by care providers and their patients to do what it is intended to do.

Intended Use: a statement that must clearly define the functions for which your product is (and is not) meant to be used.

Indications for Use: outline the precise situations and conditions within which your product should be used.

To that point, the first step in the ISO 13485 certification involves defining your medical device's **intended use** and **indications for use**. In both cases be specific – do not include forward-looking things it could do, only what it will do when it is released. These will serve as the framework for your QMS and will be used by auditors when performing their conformance evaluation. At a high-level a conformant QMS must include the following:

[3] https://www.iso.org/news/ref2318.html

Functional requirements definition and documentation	What problems and use cases is your product meant to address, and for whom?
System architecture and design documentation	How will you implement technology to deliver the aforementioned functionality and features?
Risk identification and mitigation	Ensure you proactively identify and document the potential risks associated with your product's use in a healthcare environment, including the related adverse outcomes that could occur. Identify how you intend to eliminate or mitigate these risks through preventative measures.
Internal testing procedures, test cases, and test evidence	How will your team thoroughly test and prove that your product functions as expected, and is free of critical defects in a controlled environment?
External validation by qualified experts	How will your team thoroughly test and prove that your product functions as expected, and is free of critical defects in a clinical environment?
Post-market surveillance and reporting	What channels and resources do you provide to address any issues or defects that arise when your product is live in the field? What about critical defects that could impact patient safety – how will you communicate with your customers and regulatory bodies? How will you undertake corrective actions to ensure the issue is quickly and effectively resolved?

This is by no means an exhaustive list; however, it provides a good overview of what will need to be in place for you to obtain your ISO 13485 certification. The mantra you should live by when designing your quality management system is "documentation, documentation, documentation". There must be a comprehensive set of documentation that clearly outlines your policies, procedures, and work instructions for every participating role in your company – including engineers, validation specialists, documentation authors, support personnel, and others.

Want to know more about regulatory requirements?

For more information about ISO 13485, check out ISO 13485 Medical Devices: A Practical Guide.

Our team has decades of hands-on experience in medical device software engineering, including the design, documentation, and implementation of quality management best practices. If your organization could use some help with your quality management system contact us for a free consultation.

Scratching the surface

While these topics provide a great overview and starting point for innovators seeking to enter the Health IT marketplace, they merely scratch the surface of what is required to be successful in the challenging – yet highly rewarding – healthcare industry.

Our team has decades of hands-on experience in clinical, technical, and business health IT settings and bring an unrivaled depth of knowledge and expertise ranging from pre-market strategy, design, regulatory, and product marketing considerations to launch and post-market activities including marketing communications and sales strategy, deployment and project management, and training and support methodology.

If you would like to learn more about the topics covered in this white paper, or if your organization could use some help in bringing your innovation to market or improving your market position, contact us for a free consultation.

About Paragon Consulting Partners, LLC

We are a team of passionate healthcare professionals with more than 100 years of collective clinical, technical, and business leadership experience within the healthcare IT and imaging fields. Each partner contributes a unique set of skills that together guide collaborative efforts to unify and improve healthcare delivery alongside our care provider and vendor partners.

Offering a wide variety of advisory, consultative, and professional services for healthcare organizations and industry vendors our experts can bring relevant experience to your unique situation to augment your team, accelerate success, and increase your return on investment.

PCPIMAGING.COM

PARAGON CONSULTING PARTNERS

Contact Us

500 Capitol Mall, Suite 2350
Sacramento, CA 95814
916.382.8934
info@pcpimaging.com
pcpimaging.com