VIEWPOINTS ON INNOVATION

VIEWPOINTS ON

Smart Connected MedTech

A KALYPSO PUBLICATION

Today's advancements in digital infrastructure make it easier and cheaper to build a robust smart connected architecture of medical devices, software applications, data, healthcare systems and services.

The promise of the Internet of Medical Things (IoMT) is tremendous, driving new business models via systems that can monitor, collect, exchange synthesize and deliver valuable insights like never before.

How can you build and enhance IoMT capabilities to drive value for your company while delivering better patient outcomes and decreasing the cost of care?

This compendium of articles offers practical advice in three key capabilities for smart connected MedTech: connected products, machine learning & advanced analytics, and closed loop quality & compliance.

Table of Contents

Connected Products

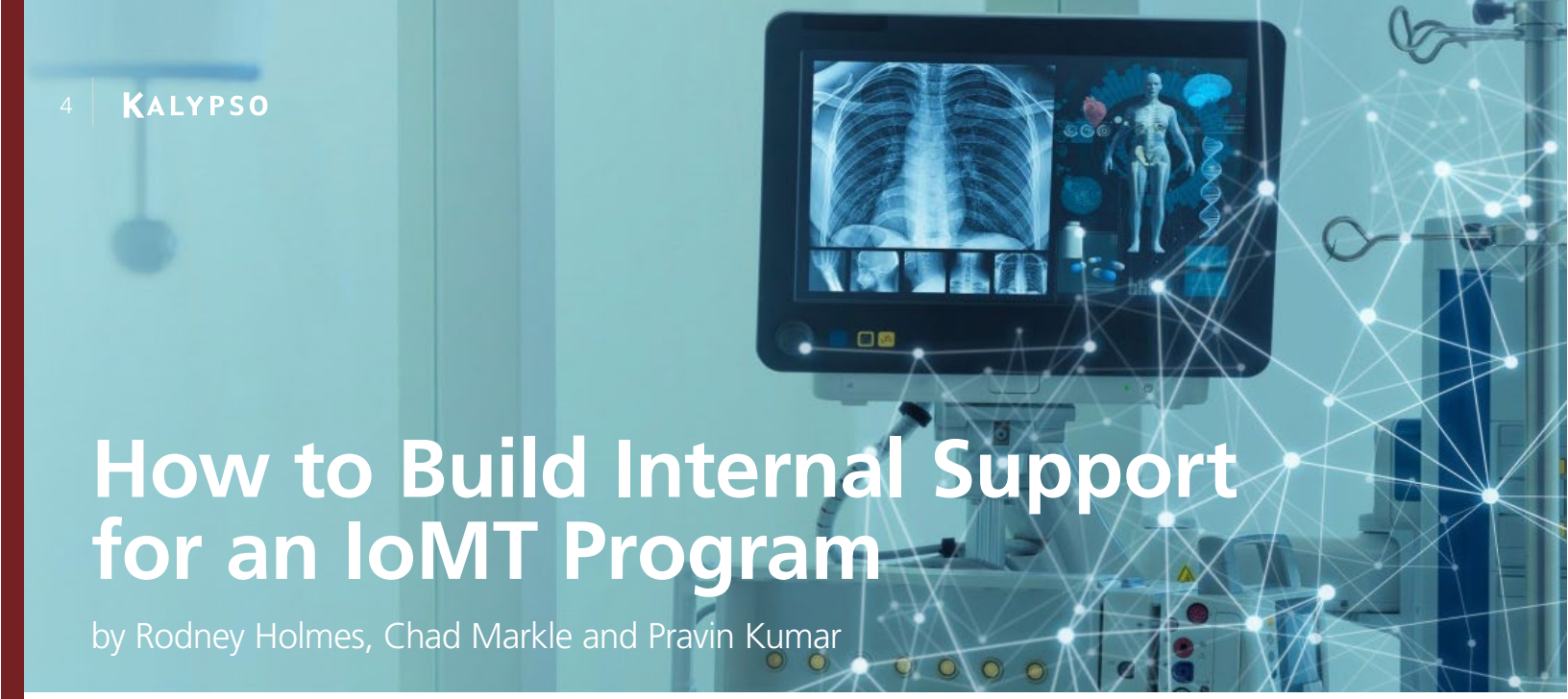
Leverage the power of IoT to generate valuable business insights.

Machine Learning & Advanced Analytics

Democratize analytics to build and adopt advanced capabilities with predictive analytics, machine learning and artificial intelligence. Apply AI and automation to extract meaningful insights from product data, formulate predictions, recommend improvements, and automate actions within systems and processes.

Closed-Loop Quality & Compliance

Leverage IoMT to enhance product quality and better navigate a complex regulatory environment. Harmonize and simplify internal processes that improve new product development transparency and product traceability throughout its lifecycle.



How to Build Internal Support for an IoMT Program

by Rodney Holmes, Chad Markle and Pravin Kumar

Healthcare is transforming as Internet of Things (IoT) technology advances and smart connected products are deployed into the hands of doctors, nurses, field technicians, caregivers and patients. This transformation has carved out its own subset of IoT, known as the Internet of Medical Things (IoMT).

The Internet of Medical Things (IoMT) brings together smart connected medical devices, advanced analytics and people (healthcare professionals, caregivers and patients). It's the network of a multitude of medical devices connected by communications technologies. When implemented correctly, the IoMT results in systems that can monitor, collect, exchange, synthesize and deliver valuable new insights like never before.

The IoMT provides a more coordinated, connected healthcare system where technology empowers providers to deliver better care to patients throughout their health journey and where better patient outcomes are delivered at increasingly lower costs.

But how do you get there? The opportunity is huge, and there are many potential starting points. If you're involved in medical device field operations and are responsible for IoMT strategy, we've got your back. Here's our advice for building a business case for IoMT initiatives, based on our experiences at the top medical device manufacturers in the world.

Four Essential Elements to Building Internal Momentum

Taking full advantage of all that IoMT has to offer requires changes in the way stakeholders use, manage and maintain smart connected medical devices. Unfortunately, large-scale change efforts fail more often then they succeed. So what distinguishes IoMT programs that have tremendous success? There are four essential elements.

1. **Tell a Compelling Story**

   First is a compelling story, because stakeholders must understand the rationale for IoMT and embrace it. One of our clients focused on communicating service response times and planned improvements; another focused on being a market leader with a modern servicing platform for a smart connected surgical robot.

2. **Role Model Desired Behavior**

   Next is role modeling, because stakeholders must also see leaders and colleagues they respect operating in new ways with IoMT. One Kalypso client used customer testimonials from a highly ranked hospital describing the results they saw from IoMT as a way to help encourage other customers in their adoption process.

3. Create Supporting Mechanisms

Third is supporting mechanisms, because processes, roles and incentives must be in line with the new IoMT program. A leading medical device company worked with Kalypso to create personas for each stakeholder in their IoMT program and then revised workflows to take advantage of new IoMT value.

4. Build New Capabilities

Finally, new capability building is required, because stakeholders must have the skills required to embrace the IoMT operating model. Companies we work with that leverage our compelling IoMT training and education, and that take ownership of the ongoing training requirements, always end up stronger and more capable.

As with any transformational initiative, the move to the IoMT has huge benefits, but many potential challenges along the way. With so many considerations, including infrastructure, interoperability, data privacy and security, it can be easy to lose sight of the bigger picture.

At the heart of this transformation is the desire to improve patient care. Companies that invest time and effort to build internal momentum will move faster and achieve much greater success.

Solution Architecture Strategies for IoT in Medical Devices

by Wayne Posner and Jordan Reynolds

Implementing an IoT solution can be a challenging initiative. Implementing an IoT solution within an industry bound by numerous rules, regulations, and restrictions can add significant levels of complexity.

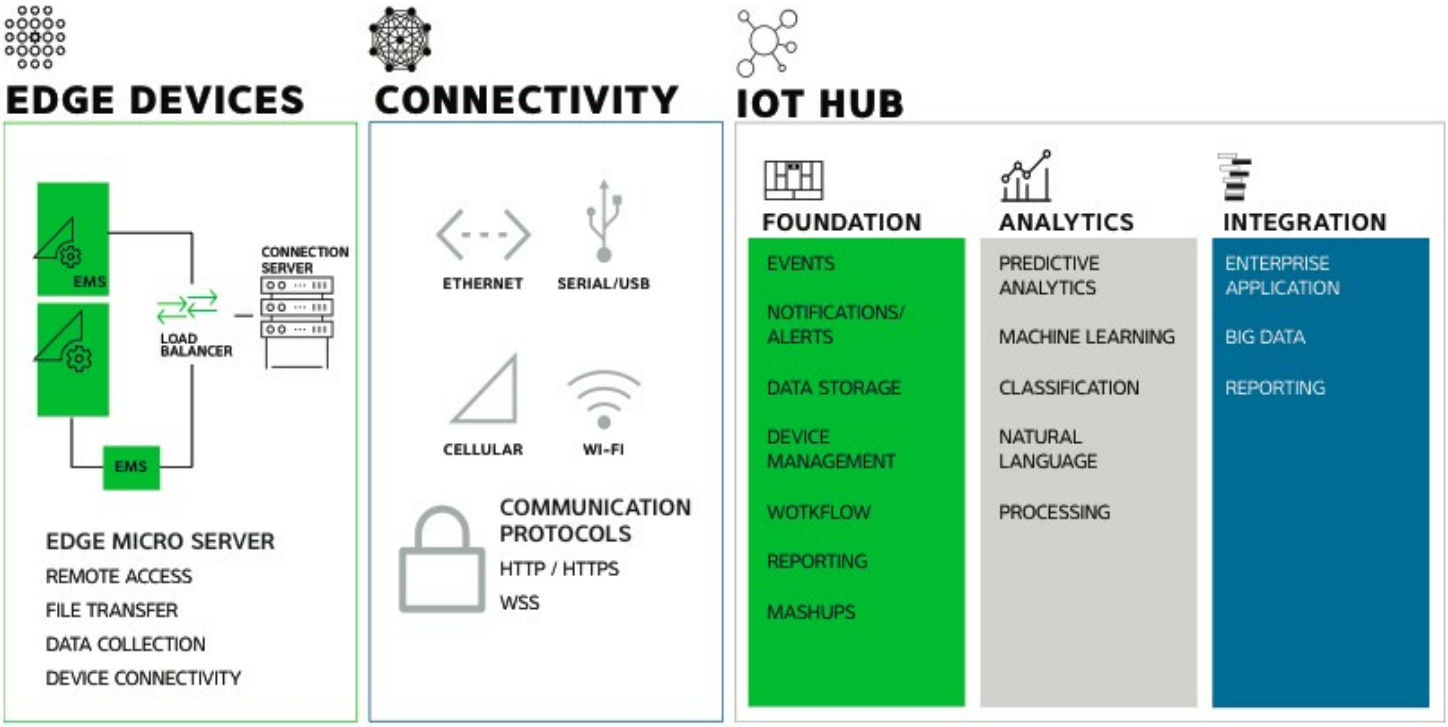
Fortunately, with a well-planned and carefully architected solution, an IoT initiative can be designed to work within the rules and regulations. This means that businesses, such as those within the medical device industry, can begin to realize the enormous benefits gained through this transformative strategy.

IoT Architecture

IoT solutions are generally defined by a three-tier architecture including:

- Private/public hosted IoT hub software solution, responsible for managing data received from remote IoT-enabled physical devices
- An edge gateway, to enable communication between the physical devices and the IoT hub
- Physical (edge) devices

Depending on the scale of the IoT implementation, there may be other architectural components such as load balancers and connection servers.



Medical Device Architectural Considerations

Within the medical device industry, there are additional architectural considerations.

- Does the device store patient data or can patient data be derived from examining device log data? If so, HIPPA compliance is a factor and must be addressed.
- Are there any legacy devices lacking networking capabilities?
- Does the environment in which the device is utilized implement any sort of network? If so, are there network security restrictions that preclude the device from connecting to the network?
- Are there government regulatory export restrictions that limit how where device data can be accessed? If so, a federated architecture with user location based security must be considered.

Security and encryption is always a key architectural consideration for any IoT solution. Many companies have strict constraints restricting specific data to users within specific organizations. Files transferred between the IoT hub and remote devices should be protected by strong encryption algorithms compliant with FIPS 104-2, while in flight, and validated against at least a CRC-256 checksum (SHA-256 hash is preferred), while at rest, to ensure malware has not been introduced.

Most medical devices deployed within a hospital environment are currently restricted from operating in an "always on" connectivity state. These devices operate in an "offline" mode. Working with these devices is a manual process. The typical use case for communicating with offline medical devices is that a qualified and/or authorized user will physically establish a connection between the device and a laptop or tablet.

The laptop or tablet will allow the user to interact with the device data using custom software. Finally, the laptop or tablet will sync the device data with a custom server solution once it establishes network connectivity.

IoT Solutions for Medical Devices Operating Offline

How can an IoT solution help to optimize this type of manual process? There are three possible solutions that work within the confines of devices operating in an offline mode.

Embedded Edge Micro Server

Install an edge micro-server directly on the device, provided the device has built-in networking capabilities; when a connection is required between the device and the IoT hub, temporarily enabling network connectivity is the only requirement. This solution is the most ideal and requires the least amount of customization; however, network security protocols must allow for medical devices to temporarily establish network connectivity when necessary.

Attached Edge Micro Server

Install an edge micro-server on a computer that is always connected or can quickly be connected to the device via a serial or Ethernet connection. Some medical devices may lack network connectivity or the additional resources required to run an edge micro-server, or may not run an operating system compatible with micro-server frameworks such as Java, C, or .Net. A small computer running Linux can be used to host the edge micro-server and establish a serial connection with the medical device. Like the first solution, network security protocols must allow for this computer to temporarily establish network connectivity so that it can communicate with the IoT hub.

Custom Software

Create/Update custom software running on the laptop and/or tablet to enable it as an edge device that communicates with the IoT hub while also adding enhanced cache management functions. This allows the IoT hub to automatically receive cached data from the laptops and tablets (with an active network connection) and push updates down to be cached until the laptop and/or tablet reconnects with the device. Of the three solutions, this is the most complex and time intensive due to the amount of required programming.

Implementing a robust and scalable IoT solution requires a well-planned and thoughtfully designed architecture. Highly regulated industries such as Medical Device have additional architectural requirements to be considered. Through careful design and thoughtful understanding of the governing rules and regulations, it is quite possible to introduce devices that regularly operate outside the IoT paradigm as part of an enterprise IoT solution.

Securing the IoMT – Nine Strategies You Can't Afford to Overlook

by Bryan Kissel and Chad Markle

The headlines are full of stories about companies that fail to live up to the expectations and legal obligations of information security. Compliance is complicated, and it changes a lot.

For medical device companies with an Internet of Medical Things (IoMT) strategy, it's even more complex. Combine recommendations and frameworks like ISO 27001 and the PCI DSS with regulations like HIPPA, GDPR and MDR, and the magnitude of the challenge becomes very clear.

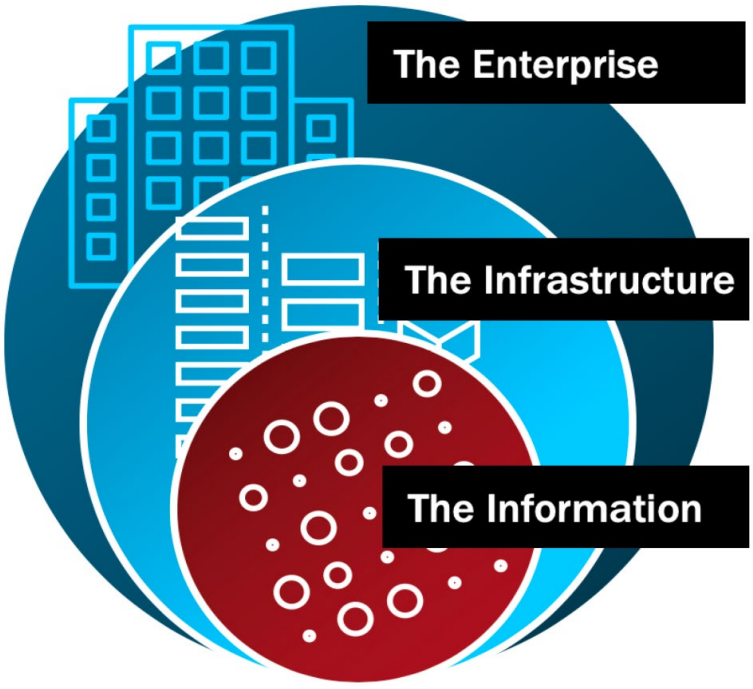
Companies are tasked with protecting both the connected devices in the field and the data they generate and transmit. So today's compliance strategies must include risk-based security practices protecting sensitive data and communications-based compliance practices around reporting, recording and archiving sensitive data.

Protecting devices in the field requires an innovative approach to comprehensive information security, along with compliance practices that can evolve alongside changing formfactors, design principles, connectivity solutions and management strategies. And on top of all this, interoperability and legacy device support is an ongoing, pressing need.

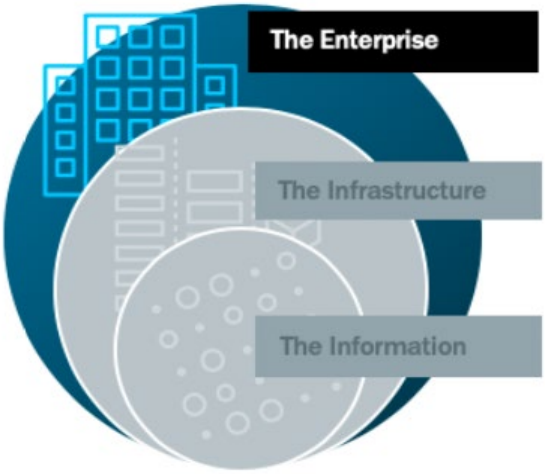
Nine Strategies to Secure the IoMT

When physical security experts secure a house, they think in terms of concentric circles. The tree line or fence would your outer-most ring - whatever constitutes the perimeter. Next would be the front door and anything on the inner-perimeter, like cameras, a storm door or window locks. The inner-most ring would then be a panic room or secure space within the home. Each ring poses a more significant barrier than the last until you ultimately have your human assets within the inner-most ring protected by the increasing degrees of scrutiny as you move inward.

IT and Security professionals should approach security in much the same way. As you move closer to the center of the concentric rings, security controls should become increasingly strict, impeding risk vector access within each ring.



Securing the Outer Ring (The Enterprise)



In the outer-most ring is the true first line of defense – the policies and education practices of the enterprise. Enforcing strong, secure policies should be a part of any company's DNA, but here are a few strategies that must apply to this ring.

1. **Use 'exceptionally' strong passwords**

   Eight-character passwords and mnemonic devices have led to many breaches, and most incidents are still user-related. Phishing, weak credentials and lost devices… we can do better.

2. **Avoid common, shared accounts**

   Shared access, passwords on Post-It notes and 'admin/password' accounts represent the old ghosts of information security risk management. Don't sacrifice security in the interest of deadlines or ease of use.

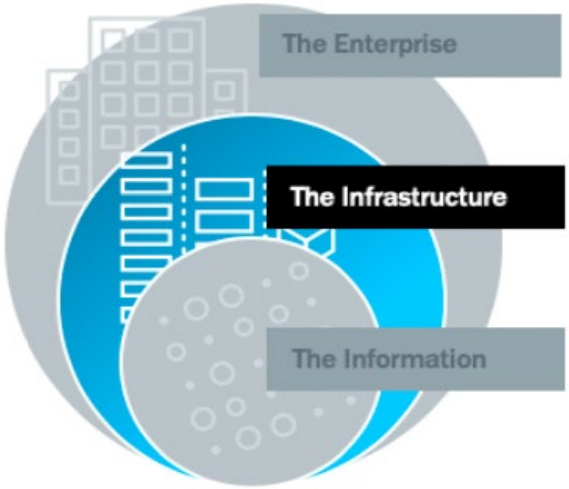
3. **Have a Data Privacy Officer (DPO)**

   Some companies try to put DPO responsibilities on the CISO or a System Admin, but there's enough strategy, policy and education required to justify this role. Plus, GDPR actually requires businesses to have a named DPO responsible for managing Personally Identifiable Information (PII) and protected health information (PHI).

4. **Enforce education, policy and values**

   Educating the workforce must evolve to create a culture of compliance at every level of operation. A clean desk policy is no longer enough, and users that access data in any form have a duty to protect that data and use it appropriately. The enterprise (led by the DPO) must deploy strategies that educate the workforce, monitor for user compliance and report incidents in real-time.

Securing the Inner Ring (The Infrastructure)



The inner ring represents the infrastructure – the hardware that supports applications and devices, secures pathways and manages traffic to assets. Innovation in this ring is critical to the longevity of connected medical devices and the operability of legacy devices still in use. There are many security strategies that apply specifically to this ring – here are some of the most important.

5. **Innovate encryption strategies for micro-formfactor devices and implantables**

   Some of the most common medical devices, like implants and wearables, are the most vulnerable. Tiny Encryption Algorithms (TEA), system-derived passwords and self-encrypting devices are some options on the bleeding edge of device security, since many of these devices are too small to handle large encryption schemes.

6. Encrypt all the blind spots on the information superhighway

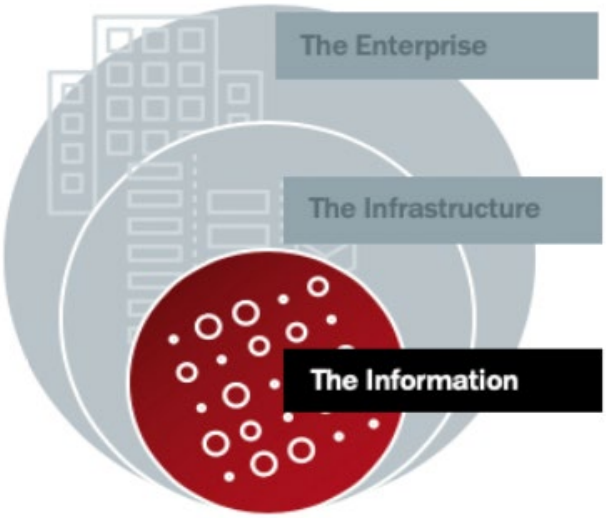
As more and more industries move toward cloud-based solutions and services, data managers must ensure that data is fully protected at every point in its lifecycle. Each system, node and relay must be demonstrably 'as-safe' as the last, from end to end.

7. Secure development of the entire IoMT ecosystem

A secure network or secure out-of-the-box solution is insufficient today. The complete ecosystems that support devices must be implemented with mature information security policies, governance, role-based access controls (RBAC) and deep documentation to ensure compliance across operational regions. Design with security in mind to always be 'audit-ready.'

Securing the Center Ring (The Information)

The center ring protects the most important asset at the heart of the IoMT – the data. Security at this level should be a nearly impenetrable shield of role-based access, attribute-based asset control, data type-specific archiving and retrieval, and comprehensive records retention.



8. Evolve and mature records management practices

Identifying and organizing data is the first and most important step to achieving compliance in any regulated industry. In the US, companies are tasked with securing data according to the risk associated with a breach. Considering the life or death implications of some connected medical devices and the truly personal nature of the data these devices generate, the medical device industry should expect the highest degree of scrutiny from auditors, legislators and even patients. New practices for records management – including documenting design, solution, architecture and audit materials – allow the DPO to demonstrate a reasonable and proactive approach to data security and privacy that lays the foundation for achieving compliance.

9. Manage the data like the high-value asset that it is

Insights gleaned from advanced analytics are the main ROI opportunity. To capitalize on this, data must be managed as a high-value asset. Protected health information and personally identifiable information should be considered as precious as secret business data, proprietary CAD elements, or IP.

In the age of Ransomware and PHI sales on the dark web, the question is no longer when a breach will occur, but how much an eventual breach will ultimately cost. As the IoMT evolves, isolated information security practices are a liability. Interoperability and security practices must extend to every point of the data lifecycle and be capable of growing alongside a maturing and ever-changing device landscape. As data privacy and information security continue to become almost inseparable, the offices of the CISO and DPO must evolve together, presenting a unified front against digital threats and a cooperative partnership in support of audit and compliance operations.

As medical device companies build and evolve an IoMT strategy, these efforts can help minimize risk while fostering a culture that mitigates information security risks, improving overall operational effectiveness, compliance posture and audit readiness.

New Frontiers for Medical Device PLM Systems: Leveraging the Power of Machine Learning

by Dave Hadfield and Jordan Reynolds

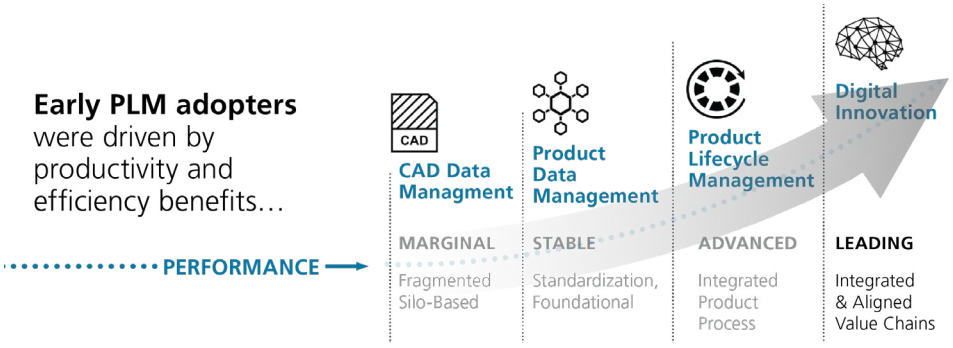
Medical devices are essential to our modern society. They give us healthier, more productive, and more independent lives. But the companies who make them face many headwinds; adhering to strict regulatory standards, proving that their benefits outweigh risks, and achieving efficacy and safety standards. To succeed, they must constantly innovate, drive down costs and navigate complex regulatory pathways.

All of this has been the driving force for medical device manufactures to automate and integrate disparate engineering, quality, regulatory, manufacturing and post-market capabilities into a single consolidated product lifecycle management (PLM) system.

Building on a PLM Foundation

Adopting PLM remains a missed opportunity for much of the medical device industry, with the potential to drive long term transformational success. But we're rapidly approaching a time when PLM alone is not enough.

Early PLM adopters were driven by productivity and efficiency benefits…



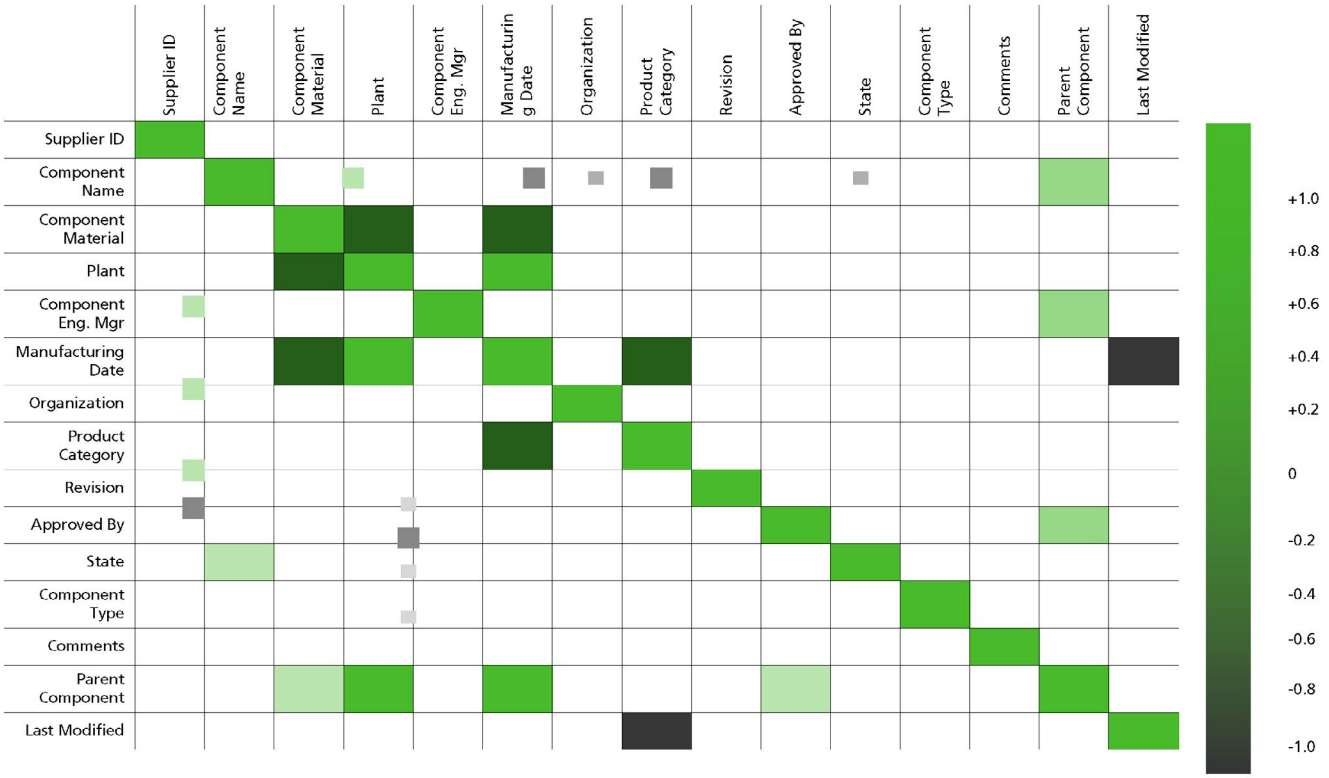
The product lifecycle is captured as data – including at its heart, a three-dimensional math-based model of the product. Companies can extend and gain new insight about these product models using new digital technologies, including machine learning, the Internet of Things (IoT), and augmented reality. These technologies have made extraordinary progress in the past few years. By evolving PLM to embrace digital tools, companies gain strategic insights while facilitating the creation of breakthrough products and services.

Machine Learning and PLM

In a typical medical device company, research, engineering, quality engineering, supply chain, operations planning, and post-market surveillance activities produce large sets of structured and unstructured data. Intersections of those data sets can produce over 750 potential points of data correlation. These large, complex, dynamic sets of data are exactly what machine learning analytics algorithms were built for. Any large, mature PLM system with robust processes and data has almost countless applications to drive value from machine learning techniques.

Potential Applications of Machine Learning to PLM

Apply Machine Learning to PLM Data to Improve Product Development Results



PLM provides the potential to gather large amounts of structured product data, and integrate it with data about post-market quality issues. This gives valuable information to improve products, accelerate the resolution of issues and improve quality outcomes.

But even with advanced integrated and automated processes, it's not easy to identify potential correlations across multiple related data sets. With machine learning performing advanced analytics on PLM data, companies can predict outcomes and improve product development results by understanding the causes behind non-compliances, problem reports, product failures and quality issues.

Understand the Nature of a Product's Evolution using Natural Language Processing

Any given product may go through thousands, even tens of thousands, of iterations with each change recorded in PLM. By parsing language inside changes (tapping into the same type of technologies that make Siri and Alexa successful), we can understand the historical nature of product improvements and draw insight. This can be helpful in new product development efforts, shaving off design cycles and driving innovation.

Find Winning Product Features

What conclusions can we draw from on market sales to identify correlated user experiences? By combining part sales information (say by region) with PLM feature information, we can zero in on market success and tie it to specific product attributes.

Suggest Parts without a Search

Use machine learning to suggest parts based on specification data, and present them to the user. This is similar to how Google Search works when you enter a search term. But this goes beyond search and uses machine learning to identify potential candidates.

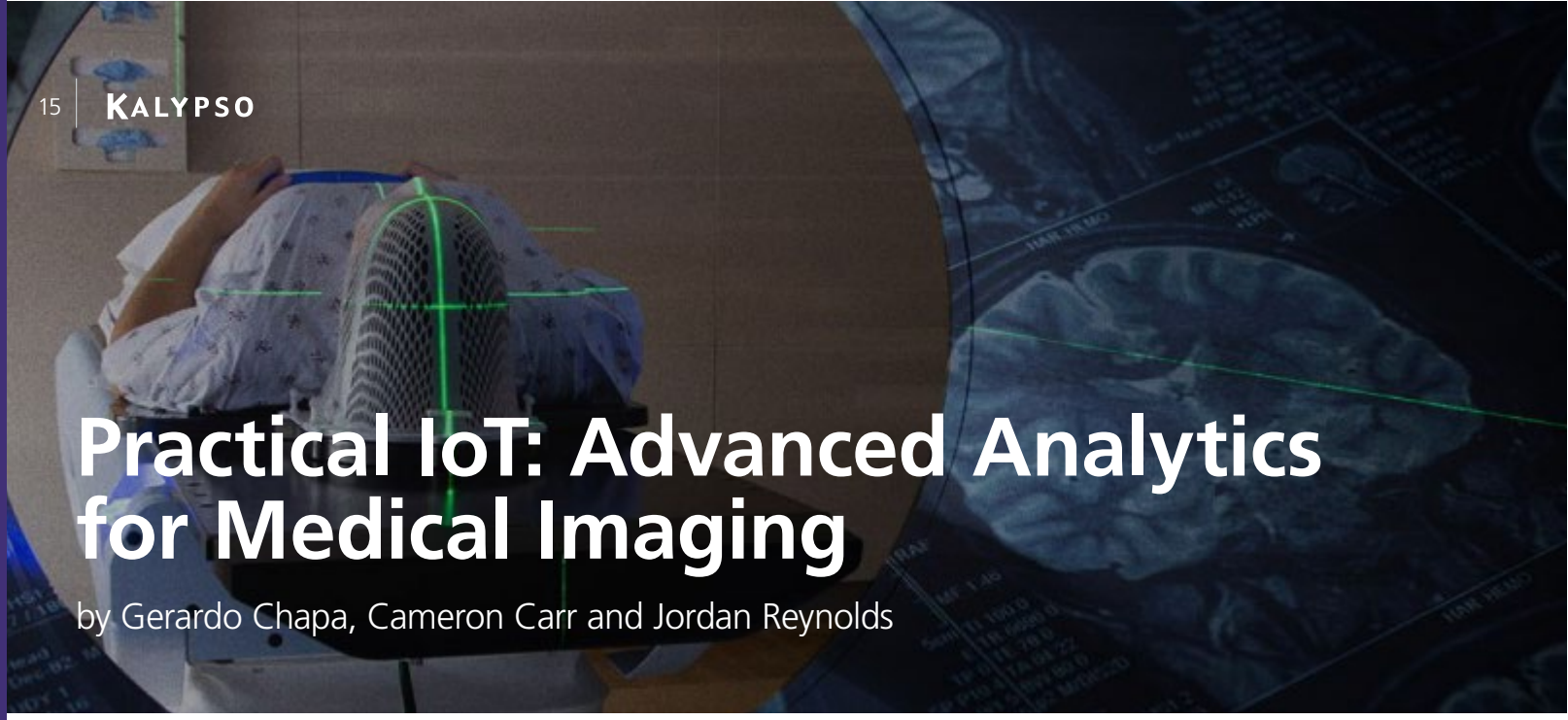
Drive Lean Processes

The system can learn process and corresponding workflow behaviors over time and by user, site, division, product, etc. From this it can identify points of delay and recommend potential process optimizations. Combined with flexible PLM applications, users can apply optimizations that are sensitive to cultures, locales, product types or even individuals to help processes like change, New Product Development (NPD) and Corrective and Preventive Action (CAPA) run more effectively.

Think Forward. Act Now.

Medical device companies have unique challenges. As they strive to differentiate themselves with new and innovative products, they can get benefit from a strong PLM foundation. With PLM, medical device companies collect large quantities of diverse data as they develop products. But PLM alone can't provide true insight from this data.

To accelerate results in a digital world, medical device manufacturers need to think forward and act now. Those who identify opportunities to apply machine learning and advanced analytics to PLM will unlock new insights to outpace their competition.



Practical IoT: Advanced Analytics for Medical Imaging

by Gerardo Chapa, Cameron Carr and Jordan Reynolds

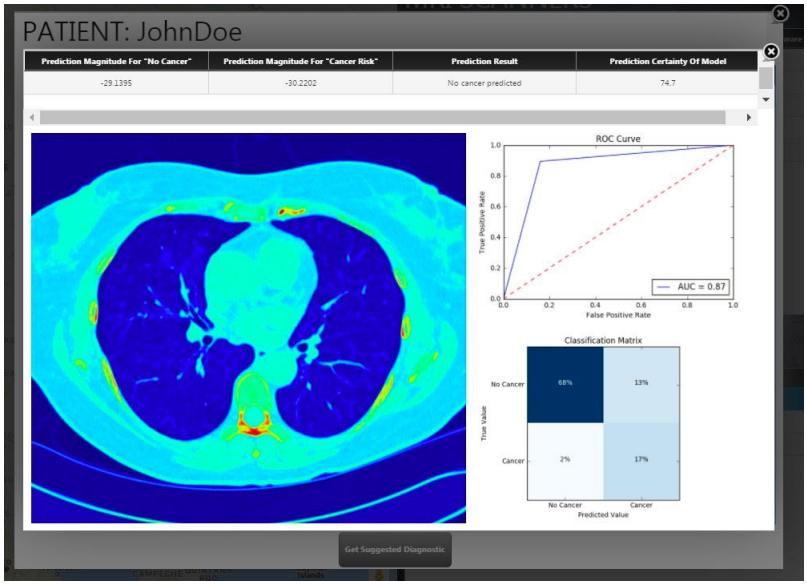
Early detection is a key indicator for a patient's five-year prognosis when treating cancer.

Time matters. The faster and more accurately a doctor can analyze the image of a tumor, the quicker treatment can begin and the sooner patients are on their way to recovery.

Imagine if doctors could quickly compare and contrast images of a tumor with hundreds of thousands, or even millions, of other tumor images while diagnosing and treating cancer. With advanced Internet of Things (IoT) techologies and new deep learning techniques, doctors could do exactly that.

Request a Suggested Diagnosis Using Machine Learning

In a single year, a leading cancer research hospital in Texas generated more than half a million medical images in their fight against cancer[1]. With so many images to analyze, harnessing the power of an IoT and analytics platform to analyze rich multimedia data – such as medical images – could improve patient prognoses with earlier cancer detection and, more importantly, treatment. Leveraging the advanced analytics capabilities of PTC's ThingWorx platform, we built a use case that uses images produced from smart connected CT scanners, and a set of processes for understanding and analyzing digital images, known as computer vision.



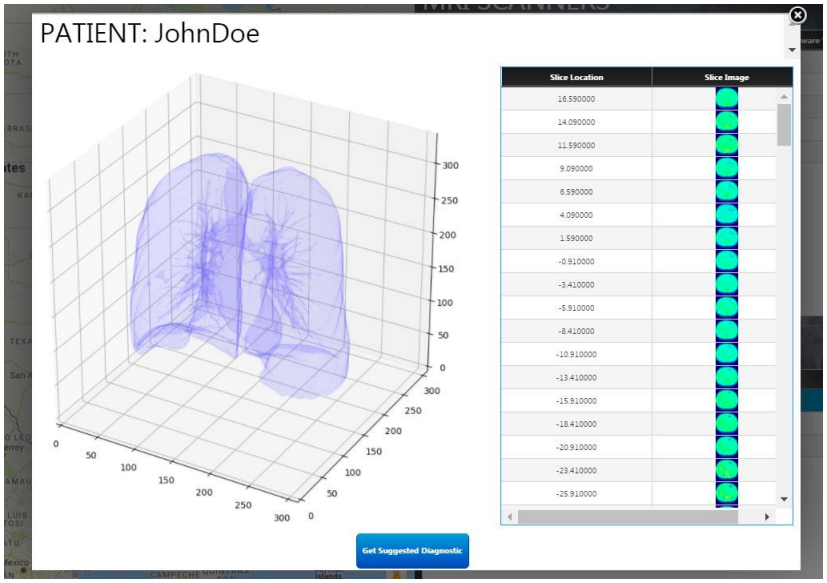
For example, a smart connected CT scanner can send data directly to an IoT cloud. Thanks to the new technologies provided by deep learning algorithms like neural networks, the system can interpret one medical image based on what it's learned from hundreds of thousands of others, and identify indicators of cancer that would otherwise remain undetected. The results are almost immediate, and are readily available for the doctor to use in diagnosing and treating patients.

1 https://www.mdanderson.org/documents/about-md-anderson/about-us/facts-and-history/quick-facts.pdf

Improve Accuracy and Patient Outcomes with Scale

Deep learning and other machine learning techniques improve as more data is collected. This means the system's accuracy of detecting tumors could increase over time due to the ever-growing database of medical images being fed into the cloud by smart connected medical imaging devices.

A smart connected CT scanner has the potential to not only provide life-saving images for a single patient, but to continually provide quality data to support the analysis that could save others in different facilities and locations altogether.



PTC's ThingWorx Analytics platform can act as the hub for medical images and enable the medical device industry to harness the power of the Internet of Things, cloud computing and machine learning to improve the quality of diagnosis and treatment of cancer and other diseases.

This technology has not been validated or approved by the FDA or other international regulatory agencies as a saleable medical device. However, given the success of this capability, we believe smart connected medical devices like this present many opportunities to increase effectiveness and reduce costs.

Potential Business Model Innovation for Medical Device Manufacturers

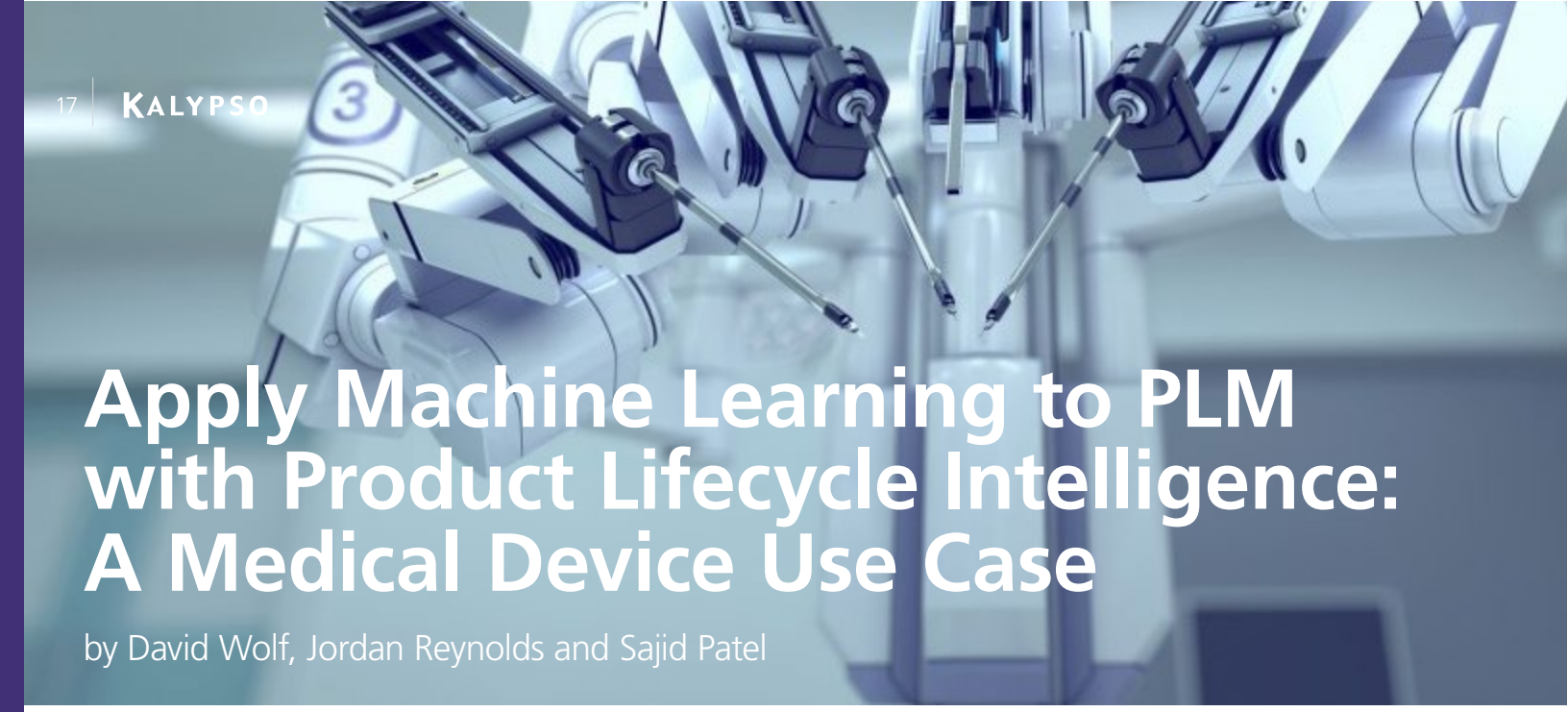
Smart connected technologies like the one discussed in this article will also allow medical device manufacturers to innovate on their business models. Integrating smart cloud platforms to medical devices they bring to market and licensing cloud analytics capabilities to their customers as a premium service. Subscription based cloud analytics services for medical diagnosis has the potential to drastically improve radiology workflow by allowing for faster, more accurate cancer diagnosis.

From predictive maintenance and smart software updates to using advanced analytics on rich multimedia data, smart connected medical devices have the potential to fundamentally change the future of healthcare.

Think Forward. Act Now.

If your business goals include reducing cost and increasing effectiveness, now is the time to take the next step towards smart, connected products. Reap the benefits of IoT analytics with rich multimedia data analysis — not just text or numbers — to improve patient outcomes. Replace downtimes and maintenance costs with predictive maintenance and automatic software updates to invest in the future.

Accelerate innovation results in a digital world. Think forward. Act now.



Apply Machine Learning to PLM with Product Lifecycle Intelligence: A Medical Device Use Case

by David Wolf, Jordan Reynolds and Sajid Patel

Worldwide regulations are changing at an alarming rate. One way for global medical device manufacturers to remain competitive is by optimizing change notice lead times. Today, the ability to apply machine learning to Product Lifecycle Management (PLM) systems can help them better understand and drive insights from product data that has been collected over many years.

Product lifecycle intelligence (PLI) is an evolution of PLM that applies artificial intelligence and automation to help PLM users extract meaningful insights from product data, formulate predictions, recommend improvements, and automate actions within systems and processes.

The potential value is immense because with PLI and machine learning, medical device manufacturers can proactively prevent delays and failures.

This article details how one manufacturer addressed their global challenges with a unique three-phase approach, driving measurable business results.

The Company and the Business Challenge

A top medical device manufacturer wanted to enhance transparency of the change control data stored in their PLM system. The process required a transformation to how they aggregated and displayed data such as aging and cycle time throughput. The organization used PLM dashboards, spreadsheets and shared hard drives to analyze their change control data; a process plagued with common data replication issues. The problem was intensified by the fact that there was no easy way to perform analytics on data without a massive effort and an extensive approval process - which is typical with traditional Master Data Management (MDM) and Business Intelligence (BI) solutions.

Although PLM systems store change data that may be used for auditing purposes, the core platform does not provide advanced analytics capabilities – like machine learning – that can aid in predictive analytics, root cause analysis and discovery activities.

The company decided to execute a proof of value with a role-based application that used a state-of-the-art app to aggregate data and optimize change notice lead times. Just like many medical device manufacturers, the company hoped to optimize their change management process and predict the likelihood that a product would fail or succeed in production.

A Strategic Three-Phase Approach

To address the challenge, the company used a strategic approach based on Kalypso's hands-on experience helping global medical device organizations benefit from emerging technologies. The three-phase approach is designed to drive maximum value from digital initiatives both in the near-term and for future growth, with an iterative crawl-walk-run cycle.

Phase 1: Start with a Proof of Value Workshop

This phase starts by defining a small scope of business objectives (engineering change cycle time, rejection/rework rate, etc.) The company provides data extract from PLM and Kalypso demonstrates a high-value use case leveraging PLI to drive insights from the data. With a clear link to a strategic business objective, it's easier to show results that help obtain executive sponsorship for the next phases.

Phase 2: Test a Minimum Viable Product (MVP) Pilot in Production

This phase builds on insights generated from connected systems, leveraging machine learning and artificial intelligence to proactively predict and prescribe actions that prevent future crises.

Phase 3: Scale Pilot to other Business Units and Manufacturing Sites

In this phase, knowledge is transferred from the first two phases, enabling multiple use cases, while leveraging medical device connectors, role-based apps and advanced analytics. It is the phase at which the enterprise-wide business value is realized, and the benefits of a strategic digital program start to accrue.

Phase 1 Results

In less than six weeks, Kalypso addressed phase 1 with a medical device role-based app solution using the ThingWorx platform to capture and aggregate real-time data related to the change management process. An analytics engine was used to create a change management algorithm, providing immediate insight into lead time variation within the product and proof of value for leadership support.

This is just the start. In addition to optimizing cycle time, PLI can predict the rate of approval from the implementation board based on the tasks and rework cycles within the change implementation plan. The company could reduce costs from poor quality through the ability to simultaneously optimize cycle time, streamline the change process and remove bottlenecks before they occur. As a result, the company could expect to provide consumers with a safer and more effective products, resulting in positive brand reputation and increase in market share.

It's important to recognize that using machine learning with artificial intelligence allows an effortless change management process, significant error-reduction and protection of data integrity.

Mergers and acquisitions are commonplace in the medical device industry. For this company, ThingWorx smart connected systems and PLI can eliminate siloed environments, secure data and help prevent quality events.

Maximizing the Value of PLM

PLM can do a great job of managing product data through rapid change, but it's not perfect at putting that data to work through datamining and analytics. For many discrete manufacturers, this means they are sitting on months or even years of untapped R&D product data. By combining PLM with product lifecycle intelligence, companies can bridge the gap in PLM analytics capability today, allowing them to understand current performance, historical averages, and the variances across different business units and functions.

These insights can help them develop more meaningful customer experiences, while driving business and product value. As an organization iterates through product development efforts, their database grows to be robust and the value of PLI grows accordingly.

Companies that continuously strive to maximize the value of PLM – by pursuing PLM system consolidation, looking for more opportunities to leverage insights from data using PLI, and expanding the use of apps to augment consolidation strategies – will continue to expand the return on investment.

Streamlining Your EU MDR Compliance Journey

by David Wolf

The European medical device industry is undergoing a transformation as the new European Medical Device Regulation is set to replace Medical Device Directives (93/42/EEC) and Active Implantable Medical Device Directive (90/385/EEC) by 2020. The European Union Medical Device Regulation (EU MDR), which was published in the Official Journal of the European Union on May 5th, 2017, is aimed at restoring confidence in the European regulatory system after widespread safety issues and corrupt Notified Body engagements. These regulations are directed to increase postmarket surveillance, expand the use of Unique Device Identifiers and provide better oversight of Notified Bodies.

Medical device companies in the EU market are under additional pressure to remain competitive while preparing for the EU MDR, which does not allow the grandfathering of previously approved medical devices. As companies rethink their current strategies amidst the evolving regulatory landscape, they're able to take market share from competitors by becoming an EU MDR compliance pioneer. Those organizations that are non-compliant will be unable to participate in the EU market until they are certified. The market opportunity across EU's ten largest economies, plus Switzerland, is estimated to be $16.469 Billion!

Key Compliance Challenges faced by Organizations:

- EU specific Unique Device Identification (UDI)
- Reclassification of products based upon risk
- Mandatory product liability insurance
- Reprocessing of single use devices
- Technical File updated requirements
- Clinical evaluation and evidence standards
- Tightened Vigilance Reporting and Post Market Surveillance
- Enhanced transparency by utilizing the EUDAMED database
- End to end traceability with labeling and supply chain systems

PTC provides a world class PLM system that acts as the product quality and compliance backbone, which helps facilitate an organizations compliance journey. Thingworx allows companies to mashup data from multiple systems ten times faster than traditional integration methods. Axeda supports remote service strategies and gathers run data files from the device that help identify the root cause(s) and critical usage patterns. PTC executives Kevin Wrenn and Kathleen Mitford recently discussed the "Innovation Gap" in the medical device industry and the importance of closing the loop on quality. PTC has specialized offerings for medical device clients, enabling them to expedite regulatory submissions and incorporate postmarket surveillance into product design to ensure competitiveness and compliance.

Kalypso created a purpose-built Regulatory Information Management (RIM) solution that helps organizations track the status of worldwide product registrations. It fully integrates Regulatory and Product Development landscapes as well as processes. RIM can be integrated with ERP systems so shipping controls are harmonized with product change control. The International Medical Device Regulatory Forum (IMDRF) Table of Contents is dynamically linked to the Design History File (DHF) for traceability over the entire product lifecycle. Use of advanced searching, reporting and auditing features allow organizations to analyze cycle times, spot key trends and identify problems in their infancy stages. RIM is a great starting point for organizations beginning their EU MDR journey and helps foster an environment that can be easily expanded to incorporate Design Controls, Document Controls, Supplier Controls and Quality Management.

Kalypso's Product Lifecycle Intelligence (PLI) solution can be utilized for a variety of use cases to help augment an organization's EU MDR journey. Regardless of their existing systems, PLI can be used in a software agnostic setting to generate a compliance cost model based upon existing compliance gaps using advanced analytic algorithms. Not only will this aid in determining which product lines to update or retire but also more accurately identify the true root cause(s) of the problem. Once integrated to existing systems, PLI can be used to prevent issues from escaping the factory or occurring in the first place, thus saving companies significant amounts of money that are otherwise lost due to the Cost of Poor Quality (CoPQ). Lastly, PLI can be used to tightly integrate and control the Supply Chain, which is frequently managed in another system such as ERP.

Recommendations for companies pursuing the EU MDR Compliance Journey:

- Don't wait - Develop and implement a proactive EU MDR strategy right now
- Run a mock audit to access the product portfolio and understand the cost of compliance
- Create a team of cross functional SME's that will be responsible for specific processes and user adoption
- Pick your Notified Body and schedule your EU MDR certification based upon your portfolio strategy
- Get involved with groups like MedTech Europe and partner with experienced professionals to help guide you through your EU MDR compliance journey
- Perform Quality System and Data Management system infrastructure gap assessments
- Identify a data migration strategy and start moving on it now

14 Reasons to Unify Regulatory Information Management with PLM

by Sajesh Murali and Nate Reisch

Medical device companies have many unique challenges, including rapid growth by acquisition. As product portfolios expand, they must efficiently manage information on new and existing products, all while considering stringent regulatory requirements and global distribution challenges.

In many cases, these manufacturers don't know every place where products are registered or need to be registered. They also struggle to provide international affiliates or divisions with all the information they need to register products.

When regulatory and product development information are not aligned, there are numerous financial and quality impacts, including loss of international sales, increased regulatory risk like recall notices or unauthorized shipments, and a strain on resources due to the manual effort required to collect information to support the regulation needs.

But it doesn't have to be like this. By aligning regulatory information management (RIM) with product lifecycle management (PLM) systems, companies can gain significant benefits, reduce regulatory risk and improve international sales.

A Quick Refresher on PLM and RIM

PLM, at its core, is more than just a software system or solution. It's a set of unified business processes that interconnect all of a product's data from the time of conception until obsolescence. The benefits of a global PLM solution, driven by leading practices, are numerous and well-documented. Importantly for this discussion: with a PLM system in place, the foundation for RIM system is already laid.

RIM, at its core, is a unified process of handling product development data that is required to register a product that complies with regulations of every country or region where it will be sold.

From strong governance to high data quality, a global PLM system provides visibility across the entire product lifecycle. When connected to a RIM system, companies gain visibility to the regulatory ecosystem in the same way.

14 Benefits of Unifying PLM and RIM

System Improvements

1. Consolidate Systems

In general, it's a well-understood leading practice to consolidate data between systems. Benefits include lower cost of ownership, easier transfer of information across business processes, and common user experiences.

Statistical Improvements

2. Reuse Product Master Data

Leverage a single source of truth for all product data - from early design throughout the lifecycle - for easy re-use in design dossiers and submission packages.

3. Increase International Sales

Register products in more international markets, with greater speed and less effort. Easily maintain registration status and expiration notices on an ongoing basis.

4. Improve Regulatory Support of Business Planning

Gain global visibility to registration information (status, plans, etc.) to help the business drive decisions and to support better collaboration and alignment between business and regulatory planning.

5. Streamline Submission Package Management

Enable easier creation and management of submission packages (510k, tech file, etc.) with all the data integrated in one place. It's easier to maintain technical files and international submission packages even as product data changes, because it's directly linked to the master source.

6. Reduce Manual/Duplicate Effort

Reduce time spent finding and communicating registration information across many different functions. Reduce redundant efforts between countries, ensuring proper communication and availability of the right information at the right time. For example, clinical trials performed for one country may be shared with another country for reuse.

Procedural Improvements

7. Reduce Unauthorized Shipping

Integrate registration within the design, commercialization, and distribution processes. This reduces the risks and regulatory penalties that occur when products are shipped to countries where they are not registered, or where the registration is not active.

8. Improve Planning and Communication

Limit the number of review cycles and changes to improve global submission planning and communications across different functions.

9. Share Country Requirements during Product Development

Enable design teams to understand and plan to meet all the different country requirements during the product development process.

10. Notify of Country Requirement Changes

Notify design teams of country requirement changes that might impact products. Help plan the changes accordingly to reduce delays in renewals and time back to market.

11. Plan for Product Obsolescence

Enable better obsolescence planning by taking related registration information into account and ensuring there are no active products in the field at remote locations.

12. Faster Regulatory Affairs Resource Planning

Achieve more accurate and faster planning by giving regulatory affairs groups full visibility to upcoming registration activities.

13. Enable International Change Notifications

Enable more efficient and integrated processes for notifying international teams of design changes by broadcasting a message to all countries.

14. Change Impact Assessment

Give design teams full visibility to assess if and how a design change will impact compliance. With an integrated change process, international regulatory affairs groups are notified and engaged earlier.

Which Comes First - PLM or RIM?

First, your starting point doesn't greatly affect the expected outcomes or benefits. Companies can start with RIM or PLM and still expect similar results.

However, implementing a RIM system alone will not deliver transformational results. Companies must also address organizational (people), statistical (data), and procedural (process) dimensions to fully realize the potential of a comprehensive regulatory information management solution.

It's also important to not think about RIM and PLM as individual functional areas, business process, or systems. Break down the old school, siloed school of thought. Approach both regulatory and product lifecycle information management from a holistic perspective focusing on the interactions between the two and the areas where they have traditionally broken down.

Getting Started: Key Questions and Guidance

Do your organization's current RIM and PLM processes use an integrated approach to sharing information or a "throw it over the wall" approach, where the two groups don't collaborate or interact during the commercialization phase of the product lifecycle?

Most companies still operate with a "throw it over the wall" approach, which wastes time when people must re-find or re-create information that already exists. By collaborating at the right time and with the right data, time-to-market and regulatory filing errors can be drastically reduced.

Does your company currently use common and consistent roles between RIM and PLM processes?

Functional areas should not have largely standalone functions that have no connection or place in the greater organization. Roles and skill sets should be consistent across the organization. The greatest improvements to innovation results often come from cross-collaboration with employees working outside of their standard, boxed-in ways of thinking.

Is your organization ready to fully integrate RIM and PLM into a single system?

Depending on your organization's current maturity level and strategy related to mergers and acquisitions, now may not be the right time to invest in a single platform for all functions. But companies can gain benefits and reduce costs by first defining integrated people and process strategies prior to fully integrating the systems. And when the time is right, the integration will be faster and cheaper with this pre-work complete.

Final Thoughts

Today's regulatory submission process is complex, but with integrated PLM and RIM solutions, companies can implement inter-connected processes and share information through product development and all the way to the distribution cycle. Companies that do this well focus not only on the systems and data in the merging of these processes, but also on managing people and change.

And all the effort is worth it. Embracing this transformation and embedding safety and compliance into every step of the medial device innovation process, will ultimately lead to better results for patients.

Leading Practices for EUDAMED and Basic UDI

by David Wolf and Erin Halleran

Big regulatory changes are coming to the way medical device companies sell their products in the European Union (EU). Previous product management strategies are becoming antiquated with exponentially increased risk. The changing landscape demands urgency and comprehensive strategies based on informed opinions.

As a part of the changes in the EU, Unique Device Identification (UDI) and Basic UDI (BUDI) will be a requirement for medical devices. The new regulatory initiative falls under the EU Medical Device Regulation (MDR) and supersedes the Medical Device Directive (MDD), which previously had no provisions on traceability of medical devices, so the steps necessary for compliance are completely new for the EU market.

As deadlines to comply quickly approach in Spring of 2020, let's explore the context, basics, and best practices to adapt to this new normal across the industry.

How Did We Get Here?

To better understand the context of Basic UDI, it's important to understand the origin of UDI in the United States. UDI first came into use in 2007, when the US Congress passed legislation directing the Food and Drug Administration to develop regulations establishing the UDI system for medical devices. In an interview on July of 2013, a Senior Adviser for Patient Safety at the Center for Devices and Radiological Health stated that the underlying issue was the lack of a consistent, standardized way to identify devices. There was no explicit device identification for use in adverse event reporting or post-market surveillance. On September 24, 2013 the final FDA rule took effect in the US.

In the case of the FDA, UDI is the link that connects FDA-regulated medical device products and tracks critical quality characteristics over the entire product lifecycle. UDI aids in digital product definition and makes it possible to perform advanced analytics when scoring vendors in the FDA's Case for Quality initiative. There's no doubt that the FDA UDI regulation serves as a blueprint for the EU and other evolving regulations expected to be released in China, Brazil, Australia, Japan, etc. However, each is expected to introduce new attributes according to specific intentions, and we see this in the EU.

The Basics of Basic UDI (BUDI)

In addition to implementation of their own UDI, EU MDR went one step further with Basic UDI-DI, the key identifier in EUDAMED. Basic UDI-DI is defined as "the primary identifier of a device model. It is the DI assigned at the level of the device family. It is the main key for records in the UDI database and is referenced in relevant certificates and EU declarations of conformity." [MDR 2017/745, Annex VI, Part C]. So the DI improves the traceability of a family of medical devices over their product lifecycle.

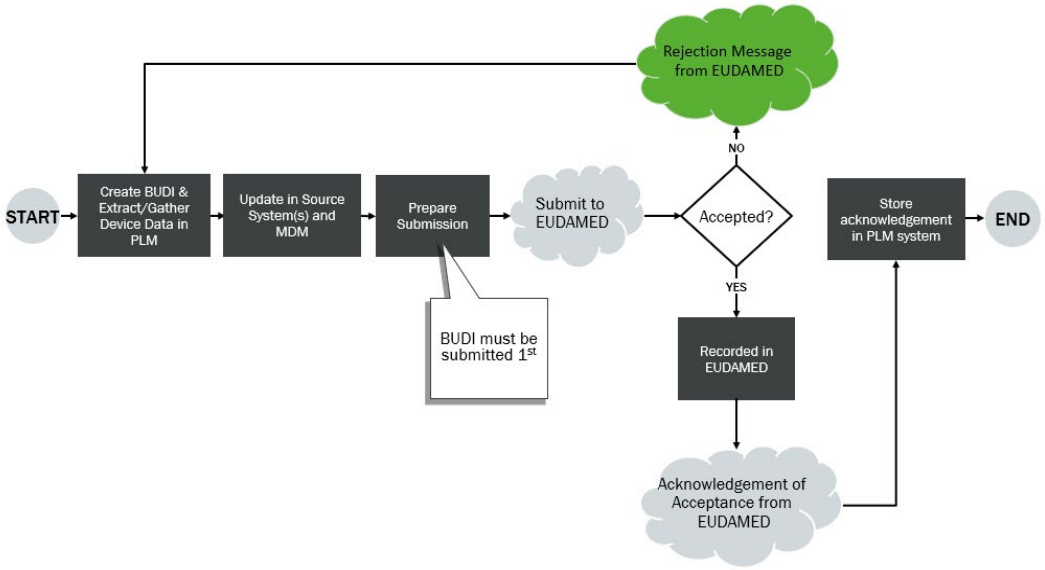
The improved oversight will enable BUDI to act as the glue for improving safety and efficacy, making the well-being of the customer or user more transparent and the ultimate priority. For this reason, a main priority within BUDI is the identification and grouping of products. There is no stringent clarification about the size or specification of categories. A default option seems to be grouping based on already-established product families or franchises, which could result in benefits for different groupings, and more clarity around the consequences of categories. By grouping products effectively, adverse event reporting limits further harm of associated products that could have similar risks.

Practical Tips for BUDI Submissions

There are many interdependencies between other EUDAMED components and the BUDI. Based on EUDAMED requirements, a BUDI can be initiated using a Manufacturer Single Registration Number (SRN). An SRN is generated by EUDAMED once a manufacturer is registered in EUDAMED as an Economic Operator. Approved certificated information must be added to the submission package before a BUDI can be submitted for approval to EUDAMED.

Sample Workflow to Create, Store, Submit BUDI UDI Device Data

The image to the right represents a sample workflow for using a product lifecycle management (PLM) system to address BUDI creation, storage, and submission.



Master data management (MDM) provides a common definition of an asset and all its data properties to eliminate ambiguous or competing data policies, and to give the organization comprehensive stewardship over its data. MDM provides mechanisms for consistent use of master data across the organization and is designed to accommodate and manage change. Many larger life sciences organizations use MDM as their data hub to support UDI/BUDI, but it's not mandatory. Most small- to medium-sized businesses use alternative solutions for their data hub needs.

The Basic UDI-DI will not be labelled on packaging or in the supply chain; instead it is a regulatory identifier used in the Declaration of Conformity (DoC), technical documentation, Free Sales certificates, and in the Summary of Safety and Clinical Performance (SSCP).

EUDAMED will be the EU MDR-specific database, centrally collecting information about medical devices. In addition to the Basic UDI-DI, there are also the device identifier (UDI-DI) and production identifier (UDI-PI). A single Basic UDI-DI can be linked to multiple UDI-DIs, while a UDI-DI can be linked to only one Basic UDI-DI.

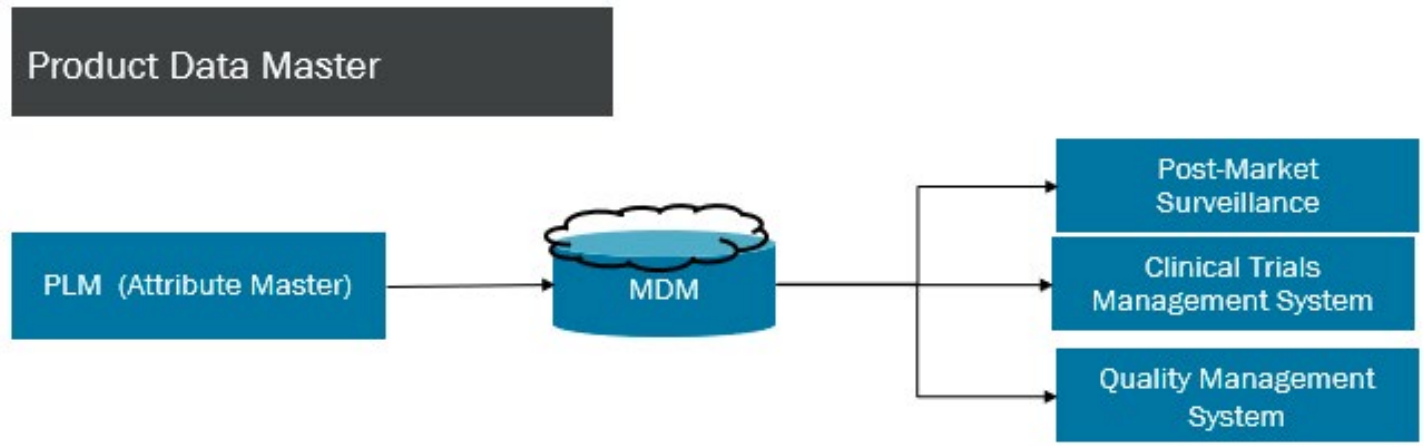
The Basic UDI-DI will connect relevant medical device information and provide a single source of truth for patients, healthcare professionals, notified bodies, competent authorities and the supply chain. The UDI-DI is to be included in the labelling and in the EUDAMED database. Device identifier is specific to manufacturers and device. Any lack of complete clarity requires a new unique UDI-DI. In addition to the UDI-DI, the UDI-PI is to be included in the labeling and if applicable, in the implant card. Production identifiers identify unit of device production.

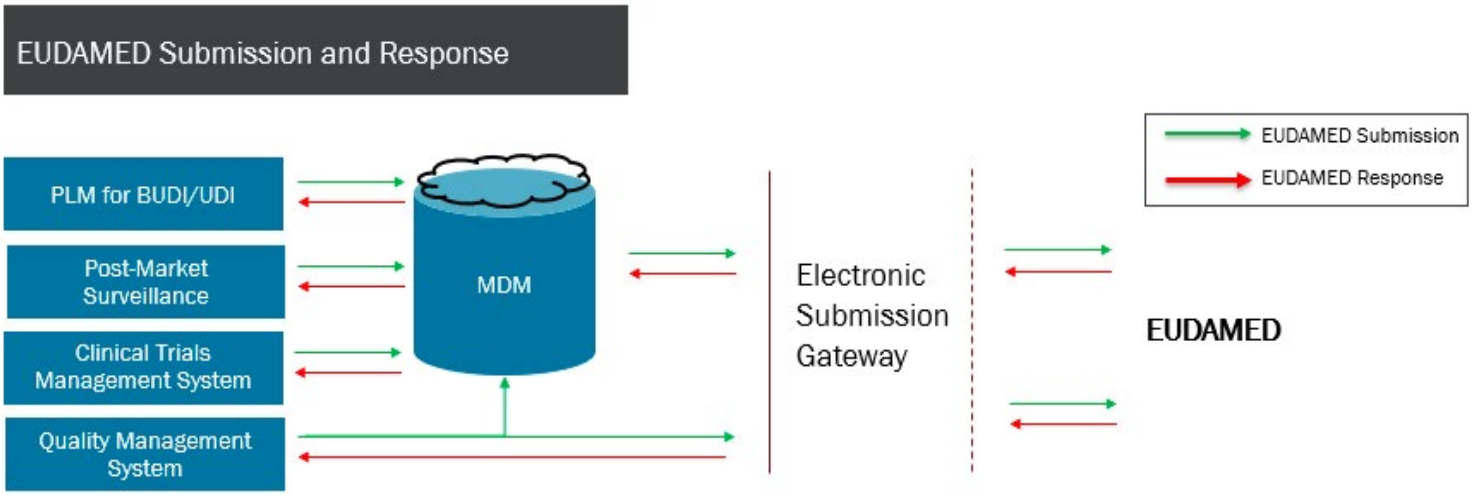
The Broader Initiative for Regulatory Information Management

Since tech doc submissions and certificate management is also a critical part of EU MDR, Regulatory Information Management (RIM) systems and processes have also become critical to efficiency in compliance towards EUDAMED. RIM systems manage regulatory data and documents throughout the product lifecycle. RIM is more focused on technical documentation than BUDI, and BUDI does need to be referenced across UDI-DI, product registrations, technical documents/certifications/DoC, the SSCP, or in vigilance and post-market surveillance. Therefore, BUDI should be registered as a precursor to all the other processes. BUDI has its own submissions and lifecycle that trigger submission to EUDAMED.

Companies that maintain their product data in a PLM system, and who may have associations that represent product families, should implement a workflow process that can be kicked off to start the BUDI request procedure. As an alternative and a part of the device identification process, a regulatory team can identify and associate a BUDI to a product, and then trigger a workflow for approval and subsequent submission.

The following images show solution architecture and product master data infrastructure that directly address submissions to EUDAMED by strengthening initiatives around data management.





The Bottom Line

As a guiding document, the final regulations will be subject to the interpretation of the Court of Justice of the European Union. With so much at stake and a lack of precedent, organizations must focus on risk mitigation through improved processes.

The question then becomes around the alignment of this BUDI process in Europe. EUDAMED requires about 50 attributes in approved submissions for the product family BUDI registration listing storage and approval; are these submissions going to be unique?

> ***Soon there could be hundreds of attributes required for an international organization. Already, we expect 350+ new UDI attributes to be required (future and present) with the six pending UDI initiatives in 28 EU countries.***

To address the growing challenges of regulatory warnings while maintaining profitability and global competitiveness, medical device manufacturers are leveraging a variety of initiatives. These include a focus on the FDA case for quality, strategic integration of current and planned systems to normalize metadata, and efficiently and effectively tracking worldwide product submissions and registrations (with RIM). For all of these initiatives, a strong PLM backbone improves success, and opens opportunity for future initiatives including digital app connectors, machine learning and predictive analytics.

Unlock Innovation with Smart Connected MedTech

Leveraging the power of IoMT expands opportunities for new functionality, far greater reliability, much higher product utilization, and capabilities that cut across and transcend traditional medical device product boundaries.

Companies are driving value through:

- **Reimagining** how value is created and captured through new medical technology use cases, value chains and business models
- **Engineering** "smart" components such as sensors, microprocessors, data storage, software, embedded operating systems and enhanced user interfaces
- **Connecting** disparate devices and applications to enable access to multiple data sources
- **Building** complete IoMT solutions and Augmented Reality (A/R) experiences quickly and easily
- **Analyzing** complex device data for real-time insights, predictions and recommendations
- **Experiencing** and engaging with devices in a more contextualized, actionable way
- **Managing** the performance of smart connected devices, processes and systems
- **Servicing** equipment remotely, speeding up resolution time and eliminating the costly field service technician visits
- **Accelerating** time-to-value and return on investment (ROI) of IoMT initiatives

KALYPSO

Wherever you are in your IoMT journey, Kalypso can help you develop a business case, define a strategic roadmap, build new offerings and/or enhance existing capabilities to quickly capture business value. We have deep experience combining new product development expertise with digital technology to drive transformation and enable value-based healthcare.

We work across the full healthcare ecosystem including provider groups, medical device suppliers, pharma/ biotech companies and payers, bringing unique insights and extensive domain expertise to our clients.

Let's accelerate your Connected MedTech capabilities.

Learn more at kalypso.com/IoMT

kalypso.com