Developing Medical Device Software with Recall Prevention in Mind

When companies design hearing aids or pacemakers, they have a lot of a different considerations to incorporate into their product development. What is the user experience? Does it function reliably in all scenarios? Is the device capturing data? If it is, what is it doing with that data?

Historically, functionality and compliance have been the two pillars. Now, the med device industry has to tackle the same security challenges common across the Internet of Things sector – but with HIPAA compliance and lives on the line. As the bar for comprehensive software quality continues to rise, medical device manufacturers have to adopt a process that prioritizes quality without sacrificing speed.

The State of the Industry & Key Trends

The medical device industry in 2017 accounted for $328 billion dollars in revenue.[1] Since 2016, it has grown by 10% YoY, which puts it on pace more with the Technology sector (11%) than the Healthcare (6%) sector. An expected 38% growth for home healthcare jobs indicates a key area of movement in the industry. Healthcare is moving more and more from the hospital to the home, from stationary to mobile. One cause is the availability of new types of medical devices.

The Expanding Digital Health Market

The very definition of a medical device is expanding. Digital Health tools and technologies can now offer consumers personalized health data in their pocket, from daily fitness statistics to genomic data and insights. Companies like Amazon, Apple, and Fitbit are now actively involved in the health tracking and care management fields. Right now, you can track and monitor your Diabetes with an app from Omada Health on an iPad.[2] You can send information from your FitBit to the app and then your Alexa in the Kitchen can make general food suggestions, taking into account your latest health data.

This movement started with personal fitness apps like Runkeeper, targeted for athletic individuals who just wanted to better measure their exercise performance.[3] Since those devices and apps first launched, the focus has started to shift toward new innovative solutions that are targeting specific healthcare needs. Additionally, pharmaceutical companies are now beginning to use apps to go beyond clinical trials and track real world results and symptoms. This Digital Health space is definitely an

area to watch. As mHealth applications develop more integrations with medical devices and wearables, there will be more data for physicians to diagnose and make care recommendations.

Class 1 Recalls on the Rise

As the industry shifts, there are certainly things to be concerned about. One of the most troubling issues is the recent jump in recalls, and Class 1 recalls specifically. The number of total recalls in 2003 was 604, and that steadily rose until it had doubled by 2012.[4] In Q2 of 2017, there were about 67.6 million units recalled.[5]

A study by Stericycle ExpertSolutions lists the average number of medical devices recalled per quarter in 2015 as 276,233. In 2016, it was 310,158. So far in 2017, it is 876,076.[5] While this is certainly concerning for patients, if this trend continues manufacturers could be buried in recall expenses. Manufacturers need to ensure that at quality-first approach is established in a programmatic way across all departments associated with product development.

What is behind this rise in recalls? The majority of units were marked due to sterility issues. These are typically the kind of units that don't have software as a component. For the rest of this paper, we are going to focus on the recalls that were triggered by quality issues and software issues. While software was the primary issue for only 1.9% of recalls, that still translates to over 1,280,000 units, and that number likely will rise because there is now an example of software vulnerabilities in medical devices being seen as a financial opportunity.

Surfacing Cybersecurity Threats

Normally, gaps or defects in device software are revealed through a process of testing authorized by the FDA or by the manufacturer. In 2016, Muddy Waters Capital hired MedSec, a cybersecurity penetration tester, to analyze a pacemaker produced by St. Jude Medical with the intention of finding a flaw, publishing that flaw, and winning a payout by shorting the manufacturer's stock. The net result has been lawsuits, counter-suits, and the FDA responding to understandable public pressure with a recall of 465,000 pacemakers in the US.[6] Unlike recalling a blender, it is not as simple as mailing it back. Everyone effected by this recall needs to make an appointment so that their doctor can update the device's firmware. Yes, you read that right. Doctors installing firmware.

After this unauthorized test by MedSec publicized a major hacking vulnerability, WhiteScope, a California-based security firm, conducted a study on devices from four pacemaker manufacturers. That study identified 8,000 bugs or hacking vulnerabilities, rooted in unencrypted patient information and software systems that hadn't been updated sufficiently. According to a Recall Index by Stericycle ExpertSolutions, 47.3% of the recalls in Q2 of 2017 were triggered by software defects and mislabeling.[5] Ultimately, the recent rise in recalls has illuminated an industry-wide issue and is forcing medical device manufacturers and their regulators to adapt to a new market landscape that include cybersecurity.

If you remember, back in 2016, there was DDoS attack that was able to take down sites like Netflix, Twitter, and Spotify.[7] It was able to gain such traction by leveraging the weak cybersecurity protections in IoT connected devices. As the trend towards Digital Health demands data interoperability, med device companies will need to invest as much in cybersecurity as any other initiative in order to ensure that personal health information isn't comprised.

A Look at the Industry's Standards Structure

There are a few key compliance standards in the medical device industry. ISO 9001, and specifically ISO 13485, set the requirements around quality management systems for medical device manufacturers. The ISO 9001:2015 standard is independent of any specific industry, but compliance demonstrates a formal process around quality management. For the medical device industry, ISO 13485 is the equivalent standard. It differs in two key ways.[8] There is no custom satisfaction component and no requirement for continual process improvement, just maintenance.

Specific to the development process, the FDA outlines expectations for electronic records and validation across the development lifecycle in Title 21 Code of Federal Regulation (CFR) Part 11. This regulation sets alignment expectations for how a team's digital process should interact with its respective quality management system.

This standard breaks out into these 5 sections:

1. Validation
2. Audit Trail
3. Legacy Systems
4. Copies of Records
5. Record Retention

Without diving into each, the impact that this standard has on a development team is that it prioritizes documentation across the entire development lifecycle, encompassing any parts of a process that could have a material impact on product quality. It also states that, "Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operation."[9] Essentially, whenever development teams are making changes, it needs to be easy to access retroactively by an auditor.

Medical Devices Manufacturers Can No Longer Afford to Be Reactionary

To prevent more recalls, the industry needs to take a more proactive approach to quality management that starts with the understanding that the product development lifecycle will most likely yield defects. If you start with that assumption, then it becomes much easier to implement the next steps:

- Identify and mitigate the highest-risk components and processes
- Drive quality through peer code and document reviews at every development stage
- Increase documentation and traceability across the communications thread

As a result of building risk assessments into the software design and development stages, manufacturers will need to be able to regularly foresee potential defects and fortify their review and testing processes accordingly. The best way to start strengthening quality throughout your development lifecycle is by empowering peer reviews. Every time that a section of code or a requirements document gets peer-reviewed, it sharpens the quality while also serving as a documentation event. The chaos of a recall is exponentially greater if there is no documentation around who worked on a trouble area, what the conversation was, and over what timeline the defect arose.

Building Quality into the Development Lifecycle

#1. Adopt a Fail Fast Mentality & an Ownership Culture

First off, quality can mean a lot of different things. For healthcare, a lot of product development comes down to asking the right questions early on. By bringing people and potential users into the product development process, you can achieve a design that yields an intuitive user experience and therefore, a better device. The end user should be at the center of the development process. The "Fail Fast, Fail Often" mentality is a parallel initiative that is often attributed to Agile development. Running many iterations and generating a minimally viable prototype allows for more functional testing and user testing. In order to fail fast, your team needs to know what failure looks like. Bringing in the end user throughout the development process helps to answer that question.

To be clear, moving to Agile isn't always the answer. Many organizations are just not configured to easily make the switch. Still, no matter what workflow your team is using, prioritizing individual accountability and regular collaboration will lay the

foundations for a successful team. In order to establish an ownership culture, team members need to share their work in a regular cadence.

One of the best ways to set up this culture in practice is a regular peer review process within and across teams. When feedback is exchanged on a daily basis, the skillsets & work for any team will actively improve. This frequent collaboration fosters skill transfer and a focus on quality. Additionally, if you utilize a review tool like our solution Collaborator, these peer reviews can standardize workflows and reviews across your software development lifecycle.

#2. Sew the Digital Thread Across Departments

In manufacturing right now, there is a lot of talk around the concept of a "Digital thread". Basically, a Digital Thread is a complete record of the communications and development processes that produce each part. When you create this thread, audit trails become more comprehensive and easier to follow, defects become easier to remedy, and process improvement gets more data-driven. The testing team should be able to have easy visibility into any conversations around software requirements, design documents, code reviews, and user stories. The benefit of cross-functional teams is that they allow you to iterate quickly. A lack of communication and transparency handcuffs team members to whatever silo they function in.

#3. Leverage the Right Tools & Workflows

So, we've established that teams focused on quality are iterating quickly and collaborating regularly. By opening up information on the development process, these teams are able to increase visibility and break down their functional silos. These two steps alone will set a team in the right direction, but how fast and far can a team go with a clunky workflow and insufficient tools? Bringing the right tools on board can unlock a better workflow that wouldn't have been possible before. These criteria can function as a rubric for evaluating new tools. Will your team need to adapt to fit the tool's requirements or can the tool adapt to fit your team's needs?

Evaluating Tools to Empower Your Development Process:

1. **Compliance with quality standards.** When adopting a new tool, compliance is critical. If a solution is not going to meet validation and verification steps reliably, it can become more of a burden than boon to your team.

2. **Supports team-designed rules and processes.** Forcing a team to fit the workflow of a tool can limit agility and productivity. For peer reviews for example, teams should be able to determine review intervals, workflows and specific tasks to be accomplished during the reviews. The tool should provide support for ideal workflows and manage adherence.

3. **Supports each team's preferred mode of interaction.** Whether side-by-side, remote real-time or asynchronous, or a combination, the communication capabilities of a tool are essential to driving adoption. The more contextual and flexible a tool can be, the better.

4. **Provides seamless integration with existing systems.** Most teams are using a stack of development tools to address unique needs. If your tools can connect and integrate effectively, it saves your development team time and confusion.

5. **Enables accurate reporting & performance metrics.** You could have a great development tool, but if you don't know how well your team is using it, then you don't know what you could be missing out on. For peer review solutions for example, use metrics can be used to gauge success towards review milestones and audit requirements. These metrics

could include man-hours spent dedicated to peer reviews, defect data, and lines of code inspected, as well as review approval and electronic signature status.

6. **Empowers cross-department communication.** As companies move towards establishing a Digital Thread across their product development, the ability for processes to be transparent, documented, and accessible will only be more critical.

In Conclusion

Peer reviews create an environment of shared understanding and collaboration. As developers review and comment on each other's code, whether in real-time or asynchronously, they all get better. In the end, the code review provides a platform for continuous process improvement, leading to improved standards, better developers, better efficiency, a higher quality finished product, and the peace of mind that comes from knowing the organization can prove compliance.

Collaborator | Robust Peer Reviews, Fast

Collaborator is the most comprehensive peer review solution on the market, designed with highly-regulated industries in mind. When code and design quality is critical and ISO compliance is on the line, Collaborator enables custom review workflows so your team can conduct code and document reviews specific to your development processes. With comprehensive integrations to data archiving, Collaborator makes peer reviews seamless and fast.
Start a free 30-day trial today.

Citations:

1. Kraft, C. (2017, July). Industry Trends by the Numbers. Healthcare Sales & Marketing, 35-36. Retrieved from http://www.hsandm-digital.com/hsandm/june_july_2017/?folio=35&pg=1#pg1
2. Digital Therapeutics for Chronic Disease | Omada Health. Retrieved December 27, 2017, from https://www.omadahealth.com/
3. Everyone. Every Run | Runkeeper. Retrieved December 27, 2017, from https://runkeeper.com/
4. Eisenhart, S. (2014, March 25). FDA Report: US Medical Device Recalls Up Nearly 100% Since 2003. Retrieved from https://www.emergogroup.com/blog/2014/03/fda-report-us-medical-device-recalls-nearly-100-2003
5. Recall Index – Q2 2017 [PDF]. (n.d.). Stericycle Expert Solutions.
6. Davis, J. (2017, January 10). St. Jude Admits Security Vulnerabilities in Cardiac Devices. Retrieved from http://www.healthcareitnews.com/news/st-jude-admits-security-vulnerabilities-cardiac-devices
7. Etherington, D., & Conger, K. (2016, October 21). Large DDoS Attacks Cause Outages at Twitter, Spotify, and Other Sites. Retrieved from https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/
8. International Organization of Standardization. (2016). Medical Devices – Quality management systems – Requirements for regulatory purposes (ISO 13485:2016). Retrieved from https://www.iso.org/standard/59752.html
9. U.S. Food & Drug Administration. (2003) Part 11, Electronic Records; Electronic Signatures – Scope and Application (21 CFR Part 11). Retrieved from https://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm

SMARTBEAR

About SmartBear Software

Supporting more than **seven million** software professionals and over **20,000 companies** in **194 countries**, SmartBear is the leader in software quality tools for teams. The company's products help deliver the highest quality and best performing software possible while helping teams ship code at nearly impossible velocities. With products for API testing, UI testing, code review and performance monitoring across mobile, web and desktop applications, SmartBear equips every development, testing and operations team member with the tools to ensure quality at every stage of the software cycle. For more information, visit: http://www.smartbear.com, or for the SmartBear community, go to: Facebook, Twitter, LinkedIn or Google+.