Yalantis

Make sure your medical IoT device is ready for a wide audience: Follow the checklist comprised by the industry expert

Responsible for this issue:
Artur Shevchenko, Director of Engineering at Yalantis

“Testing healthcare solutions is a highly responsible and complex task. It is necessary to thoroughly analyze the system architecture, track all integrations, all third-party dependencies, and clearly understand how data flow processes occur.

After analyzing the architecture, it is always necessary to ask the question "WHAT IF?": what if something goes wrong, what if the response from a third-party comes in a different way than expected, what if the middleware fails...

If there are also IoT devices in your system, then you need to pay a lot of attention to testing the integration of the IoT device with the system using not only emulators or simulators of this device, but also a real device.”

— **Artur Shevchenko,**
Director of Engineering at Yalantis

Testing medical IoT devices is a mandatory procedure that requires a lot of effort, expertise, and experience with real devices, not just simulators. In this guide, together with Artur Shevchenko, we will tell you what you should never forget about when testing medical IoT devices, namely:

TABLE OF CONTENTS

LEGACY SYSTEMS INTEGRATION AND COMPATIBILITY

- **Assess compatibility**
  Evaluate how the IoT solution interacts with existing legacy systems to ensure seamless integration.

- **Legacy protocols and standards**
  Ensure support for protocols and standards used by legacy systems, facilitating smooth communication and data exchange.

- **Testing for coexistence**
  Conduct thorough testing to confirm that the IoT solution and legacy systems can operate concurrently without interference or performance degradation.

REGULATORY COMPLIANCE TESTING

- **Certification requirements**
  Conduct testing to meet specific regulatory requirements for medical devices, such as FDA in the U.S. or CE marking in Europe.

PAY YOUR ATTENTION!

! Failure to meet certification requirements can prevent access to certain markets or regions where specific standards are mandatory, limiting your product's reach and potential revenue.

! Businesses may face fines, legal action, or both due to non-compliance with regulatory standards, leading to financial losses and damage to reputation.

- **Standards compliance**
  Ensure devices are compliant with healthcare interoperability standards such as HL7, FHIR, and DICOM. This facilitates seamless communication between various healthcare systems and devices.

- **Documentation and traceability**
  Maintain detailed records of testing processes, methodologies, and results for regulatory review and certification

PRIVACY COMPLIANCE TESTING

Verify that the device collects only the data necessary for its intended purpose.

PAY YOUR ATTENTION!

! A medical IoT device collecting excessive data can land a business in hot water.

- Privacy regulations might be violated if the data extends beyond what's necessary for the device's function.
- Excessive data collection by a medical IoT device can trigger hefty fines for privacy violations (e.g., GDPR), lawsuits from patients, and even device recalls if security risks arise.
- Security risks rise as well, with more data to be potentially compromised.
- Patient trust could be eroded if data collection practices are deemed intrusive.

- **Consent management**
  Test the device's mechanisms for obtaining and managing user consent for data collection and processing, in compliance with regulations like GDPR or HIPAA.

DATA ACCURACY AND INTEGRITY TESTING

- **Sensor calibration and accuracy**
  Test sensors for accuracy and precision in various conditions, ensuring they capture data correctly. For example, make sure with temperature variations, humidity levels, vibrational and shock impact, electromagnetic interference, pressure changes, power fluctuations.

- **Data loss and corruption**
  Simulate scenarios where data might be lost or corrupted during transmission or processing to ensure data integrity is maintained.

PERFORMANCE TESTING

- **Load testing**
  Evaluate the device's performance under expected and peak operating conditions to ensure it can handle real-world usage without degradation.

- **Stress testing**
  Push the device beyond normal operational capacity to identify breaking points and ensure that you have a robust plan to address all similar issues and the device will quickly return to stable operation.

USABILITY TESTING

- **User interface (UI) testing**
  For devices with user interfaces, test for intuitiveness, ease of use, and accessibility.

- **Physical interaction testing**
  Evaluate the device's design, buttons, and physical interaction points for durability and ease of use in various healthcare settings, including emergency scenarios and various target audience groups.

PAY YOUR ATTENTION!

! Different audiences will perceive your device differently, and you need to make sure that if your target group is retirees, all buttons for people with disabilities are easily pressed, that the fonts are large, and that blind people will have a Braille duplicate.

POWER CONSUMPTION AND BATTERY LIFE TESTING

- **Battery endurance**
  Test battery life under various usage patterns(like normal usage, standby mode, low power mode, high-intensity usage, cold or hot temperature usage) to ensure it aligns with product claims and user expectations.

- **Power efficiency**
  Evaluate the device's power management features, including sleep modes and energy-saving functionalities. Each sensor should enter sleep mode when it’s not collecting or sending data to conserve battery life.

ENVIRONMENTAL AND DURABILITY TESTING

- **Temperature and humidity**
  Expose devices to extreme temperatures and humidity levels they might encounter in their operational environment.

- **Shock and vibration**
  Test devices against physical shocks, vibrations, and other handling scenarios to ensure durability.

CONNECTIVITY TESTING

- **Network conditions**
  Test device connectivity under various network conditions, including Wi-Fi, Bluetooth, and cellular, to ensure reliable data transmission.

- **Range and stability**
  Verify the range and stability of wireless connections, especially in environments with potential interference, such as hospitals

FAILOVER AND RECOVERY TESTING

- **Redundancy mechanisms**
  Test the device's ability to switch to backup systems or modes in case of failure.

- **Data recovery**
  Evaluate the device's capabilities to recover data after disruptions, ensuring no critical information is lost.

SECURITY TESTING

- **Vulnerability assessment**
  Conduct vulnerability scans to identify potential security flaws in the device firmware and software.

- **Encryption testing**
  Verify the strength and implementation of encryption algorithms for data at rest and in transit with the help of the external security testing team.

- **Access control testing**
  Ensure that robust authentication and authorization mechanisms are in place to control access to device functionalities and data.

SOFTWARE UPDATE AND PATCH MANAGEMENT TESTING

- **Update process**
  Test the device's ability to receive and install software updates and patches without interrupting its normal operation or compromising data integrity.

- **Version compatibility**
  Ensure that after updates, devices remain compatible with the healthcare ecosystem, including other devices and systems they interact with.

REAL-TIME MONITORING AND ALERTING TESTING

- **Latency testing**
  Evaluate the time it takes for the device to collect, process, and transmit data, ensuring it meets the requirements for real-time monitoring and alerting.

- **Alert accuracy and reliability**
  Test the system's ability to generate accurate alerts based on predefined conditions, ensuring alerts are neither missed nor false

Yalantis

www.yalantis.com

hello@yalantis.com

+1 213 401 9311