The European Association of Medical devices Notified Bodies

Team-NB Position Paper

Editor :	**Team-NB**	Adoption date	5/10/2022	Version 1

Cyber Security

Introduction

The increasing number of connected medical devices and ongoing digitisation in healthcare brings new market opportunities for the manufacturer and, more importantly, improvements in patient care. At the same time, it presents new and different types of risks to the safety, security, and privacy of medical devices. These connected medical devices range from sensor-based technologies such as wearables to software as medical device such as mobile medical apps and also to implantable medical devices such as pacemakers. To ensure the safe and secure use of medical devices, state of the art regulatory frameworks are necessary.

Coherent, consistent, and harmonised regulatory requirements are key to a high level of cybersecurity and competitiveness at the European and international levels. Currently, however, an increasing amount of national cybersecurity requirements and guidances are published, which leads to an increased fragmentation within the European frameworks.

Since cybersecurity evolves on a regulatory and technological level this paper document is intended to reflect the current state of the art at the time of creation only.

There are few cybersecurity experts today and it is likely that it will continue to be a similar situation in the foreseeable future; therefore, it is a goal of this paper to make conformity assessment(s) of cybersecurity as efficient as possible without compromising the quality.

Recommendations

Team-NB recommendations are outlined below:

- Ensure the harmonised adoption of standards, for example, of IEC 81001-5-1 which is a state of the art standard that is expected to be harmonised by the European commission in the near future. It should be adopted by manufacturers as soon as feasible through transition plans and latest following the end of the transition period.

  IEC TR 60601-4-5 may also be used to document security specifications of medical devices in terms of the required security level to support type testing of security properties.

- Harmonise the approach to security risk assessment, for example it is recommended to use a systematic threat modelling technique (one such example is STRIDE) to ensure that all relevant threats are covered. The readability for third parties when using a systematic risk approach can support efficient assessment by notified bodies. Threat modelling techniques such as the example above of STRIDE can easily be integrated to an EN ISO 14971 risk management framework that utilizes failure mode effect analyses (FMEA), which is beneficial, since these are well known and utilised in common use in the medical device

industry. If other threat modelling techniques are utilized, they also must be part of the risk management file.
A list of known threats, for example open web application security project OWASP top ten vulnerabilities, common attack pattern enumeration and classification (CAPEC) list, the use of questionnaires for vulnerability metrics, such as application of common vulnerability scoring systems (CVSS) to medical devices, or brainstorming should only be a supportive element as part of the threat modelling process. It should also be considered that attack trees may reach their limits when modern highly interconnected medical device systems are modelled completely.
Common vulnerability scoring systems (CVSS), self-defined matrices, or other similar methods may be used to score threats for medical devices.

- Harmonise high level penetration test requirement; penetration testing is the primary means of security verification and validation and it is recommended that medical devices shall have appropriate penetration test reports throughout their life cycle at appropriate intervalls. Any penetration test should also have an appropriate depth and coverage, with penetration testers being independent from the development team for the device and appropriately skilled. Common penetration testing methodologies such as open-source security testing methodologies (OSSTMM), OWASP, phased structured approaches such as penetration testing execution standard (PTES) methodologies should be adapted as appropriate for the medical device until appropriate standards are available. Appropriate tools shall also be used for penetration testing. The penetration test should consider any special constraints relating to the medical device(s) such as the safety of the patient and others as well as clinical performance. Penetration testing laboratories should be qualified by the manufacturer according to their quality management system requirements to appropriate standards. ISO 17025 Accredited test laboratories with appropriate capability and competence for medical device penetration testing should be used once available.

- Adapt a secure development life cycle (SDL); the security of a medical device can only be supported by a secure life cycle process throughout the life cycle of the medical device. Cybersecurity should be considered at the early stages of the development as well as through development and in late phases of the life cycle such as multiplication of software, delivery, and disposal or deinstallation. Standards such as IEC 81001-5-1 provide essential details on how to realise this.

- Importance of Cybersecurity Post Market Surveillance (Cybersecurity PMS); Cybersecurity PMS as postulated by MDCG 2019-16 is an essential element to combat, for example, the challenge of rising ransomware attacks on hospitals, since the timely development and distribution of patches is essential to reduce entry gates for ransomware attacks and to stop the spread of ransomware attacks. Due to the criticality of this issue the compliance and effectiveness of the Cybersecurity PMS processes may be part of conformity assessment through regulation audits to MDR and IVDR by notified bodies and it is recommended that manufacturers consider Cybersecurity PMS and document in accordance with the guidance and requirements of the regulations.

Conclusions

To ensure that safety, security, and privacy is protected, a collective effort and efficiency is necessary. This paper therefore outlines areas which may be used as possible solutions to current challenges by focussing on international standards, use of a harmonised approach to security risk assessment, and by seeking a coherent harmonised approach for high level penetration test requirements, to support the medical device software development lifecycle through development to post market surveillance, and through end of device lifetime with use of the quality management system, Medical Device/In-vitro Diagnostic Device regulatory framework and guidances from regulatory bodies.