Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (xxxx) 000–000

Procedia
Computer Science

www.elsevier.com/locate/procedia

Author version - final version to appear

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2023

NEMECYS: Addressing Challenges to Building Security Into Connected Medical Devices

Martin Gilje Jaatun[a,1], Steve Taylor[b], Colin Upstill[c], Ariel Farkash[d], Salvador Garcia[e], Christos Androutsos[f]

[a]SINTEF Digital, Trondheim, Norway
[b]University of Southampton, UK
[c]Information Catalyst for Enterprise, UK
[d] IBM Israel
[e] Marina Salud, Spain
[f] University of Ioannina, Greece

Abstract

The European health care system is moving toward personalised, distributed, and home-based services. This is made possible via new and improved connected medical devices (CMDs), and will benefit health care providers in terms of reduced cost and improved service. Patients will see improved quality of life in terms of reduced travel time and reduced stress via treatment at home or where they want it. However, for these benefits to be fully realised, the cybersecurity of CMDs needs to be ensured. This paper presents a brief survey of challenges to building security into CMDs, and introduces NEMECYS, an EU-funded project which will help practitioners to (a) comply with Medical Device (MD) regulations; (b) be able to apply proportionate MD cybersecurity, and (c) build in cybersecurity by design for both MDs and the connected scenarios they operate in.

Keywords: connected medical devices; security by design; cybersecurity; build security in

* Corresponding author. Tel.: +47-900-26-921.
E-mail address: martin.g.jaatun@sintef.no

1. Introduction

Cybersecurity of connected medical devices (CMDs) is clearly important but faces several critical challenges that introduce risk, incur cost or impair the key medical purpose of delivering care. Firstly, the guidelines and standards for Medical Device (MD) cybersecurity are complex, too generic, and incomplete - due to the changing landscape of cyber threats, and also due to the need to integrate CMDs in ever more advanced, multi-institution and multi-device scenarios to deliver more effective and efficient patient care where and when it is most needed. Secondly, cybersecurity comes at a cost – it is financially costly to implement and maintain, and too much cybersecurity can impair other critical concerns such as the clinical care of the patient or ethics representing citizen rights. Thirdly, the lifecycle of the devices themselves is complex: CMDs need to be independently cybersecure, but additional threats and compromises may arise when they are connected in scenarios, and threats can be propagated from other connected devices that may have vulnerabilities unknown to the device manufacturer. To address these challenges, this paper briefly describes the approach of the Horizon Europe NEMECYS project (2023-2025), which aims to use different tools and techniques to improve the cybersecurity of medical devices in connected situations, balancing cybersecurity protection with patient benefit to determine an appropriate level of cybersecurity controls applied, and ensuring the cybersecurity does not hamper the medical care. The remainder of this paper is structured thus: We outline challenges to securing medical devices in Section 2. In Section 3 we present the NEMECYS concept that aims to address the challenges. In Section 4 we briefly outline the case studies of the project. Finally, Section 5 concludes the paper.

2. Challenges

2.1. Guidelines

All new medical devices to be commercialised in the EU must comply with the Medical Devices Regulation (EU) 2017/745 (MDR) (as of May 26th, 2021) and for in vitro devices the In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR) (as of May 26th, 2022). The Medical Device Coordination Group (MDCG) was established with the introduction of the MDR and has published the MDCG 2019-16 guidelines on cybersecurity of medical devices, covering the cybersecurity requirements of both MDR and IVDR. However, whereas the MDCG guidance is useful and fit for purpose in that it distils process and general advice on MD security from multiple sources (e.g. MDR / IVDR), it does not contain specific advice on threats and risks to devices in the context of their intended usages, nor does it suggest controls to address identified risks

There are several different approaches to the ethical use of data and information from healthcare devices. For instance, mainstream medical practice, with or without the introduction of advanced technologies, observes four principles of medical ethics [5]. These extend the nonmaleficence of the Hippocratic oath to more specific factors comprising benevolence, autonomy and justice, which relate to common, professional practice in research [1, 26]. Though not without critics [25], they provide a valuable starting point to evaluate how cybersecurity in medical devices and protection of healthcare data are managed and exploited, since ultimately any medical institution or clinician relying on or interacting with these devices must still adhere to these principles. At the same time, both non-governmental [2] and government organisations [14, 17, 18] have sought to develop sets of principles and guidelines for the use and validation of advanced technologies, many of which focus on the protection of individual data subject/patient rights and expectations. Instruments such as the European Convention on Human Rights [12] provide explicit equivocation for the assertion of individual rights: for instance, the first paragraph of Art 8 lays out individual rights, whilst the second sets out the circumstances, including for the "protection of health", when individual rights may not apply. Given these perspectives, there is a need to reconcile ethical principles and guidelines with clinical benefit and cybersecurity concerns to ensure that addressing one set of concerns does not compromise another, and to determine a balanced synthesis of different approaches and recommendations in the context of the main stakeholders' expectations and what best serves their needs.

2.2. Cybersecurity by Design

Cybersecurity by design and the need to 'build security in' has been recognized in the software community for decades [23], and although a large number of software security activities have been enumerated [28, 8], many developers are still either not aware of or not prioritising cybersecurity by design, particularly in smaller enterprises [27].

For medical devices' cybersecurity, threat modelling is referenced in MDCG 2019-16 [24] as a technique that can be applied to software, devices, systems, and networks. A recent report on general IoT security [30] noted that 47% of companies perform threat analysis when developing new product but for companies with fewer than 50 employees this drops to 33%. Given that medical devices are subject to regulation that mandates threat / risk analysis, we have to assume that all MD manufacturers do risk analysis on some level, but it is costly and requires expertise that SMEs find difficult or costly to acquire. Cybersecurity risk management, e.g. as specified in ISO/IEC 27001 [19] compliance is a manual process that often requires expert consultancy, making it costly and difficult to update when systems change. Thus there is a need to help SMEs undertake and maintain threat analyses at low cost. The MITRE/MDIC playbook for threat modelling of medical devices [7], developed using funds from FDA, includes techniques such as STRIDE, Attack Trees and Kill Chains. For STRIDE there exist software tools for sketching of systems and generation of threats, but it is less suited for cyber-physical systems consisting of software, hardware, and network components [15], while Attack Trees and Kill Chain rely on less structured methods, increasing the probability of errors.

Existing cybersecurity risk analysis schemes are mainly concerned with controlling cybersecurity risks alone and do not consider benefits and trade-offs between cybersecurity risks and clinical benefits or ethical concerns. Existing benefit-risk methodologies for MDs, e.g., the ISO 14971 standard [20] are focused on clinical risk and clinical benefit. They are only superficially concerned with cybersecurity risks. There is thus a clear need to unify and harmonise these aspects with a view to achieving an acceptable balance and resolving any potential conflicts between them.

Automated tools exist for cybersecurity risk management (e.g. SecuriCad[1] and ThreatModeler[2]) and are focused on the enterprise, reasonably so since this is their target audience. However, connected devices may operate in scenarios that cover multiple enterprises (and even in patients' homes), so therefore there is a need for risk-benefit schemes to operate in multi-stakeholder scenarios. Within the class of patients' homes there will be a large variety of threats due to each home being different and occupied by people with differing awareness and attitudes towards cybersecurity. A key challenge faced by CMD scenarios is that each participant interacts directly or indirectly with others who may be previously unknown, each with their own drivers and priorities. Vulnerabilities may be introduced at any component or process, by corrupted or biased data or by any participant in the scenario, which can provide manifold entry points for security (or other types of) threats to propagate throughout the scenario. Anticipating all possible deployment environments (even within the same class) is challenging, and some threats may be missed. Therefore, consideration of the complete multi-stakeholder nature of a CMD scenario that crosses different legal entities' domains of control is needed in risk assessment.

Current cybersecurity risk assessments are typically static (and costly to update as discussed above), and many situations are highly dynamic involving changing circumstances of patient care priorities or new vulnerabilities detected at runtime. There is a clear need to support automated dynamic, runtime cybersecurity risk management where new events are reflected automatically in risk levels, alarms raised when risk rises unacceptably, and appropriate controls recommended to return the residual risk to an acceptable level.

Threats, risks and controls are changing constantly. Novel technologies (e.g. 5G networks, big data, artificial intelligence, cloud computing, augmented reality, blockchain) and interconnection architectures provide benefits but introduce additional cybersecurity risks. Therefore there is an ongoing need to acquire and consider new knowledge about these aspects in risk benefit schemes.

[1] https://www.foreseeti.com/
[2] https://threatmodeler.com/

3. The way forward: The NEMECYS Concept

NEMECYS will address cybersecurity of CMDs via three integrated approaches, as illustrated below. Firstly we will review relevant MD guidelines and regulations, with the objective of providing recommendations for improvement with respect to how they cover cybersecurity. In consultation with domain experts we will utilise four exemplary case studies to identify gaps, recommendations to address them, and best practice. We will synthesise the results and feed them back to the relevant communities. Secondly, we will investigate proportionate risk-benefit schemes. We will bring existing state of the art background cybersecurity risk assessment work of the partners to bear on connected medical device situations where cybersecurity risks of connected and medical and diagnostic devices are balanced with ethical concerns and clinical benefit to determine proportionate actions based on considerations of vulnerability, patient benefit and rights. The initial approach is to investigate how to bring cybersecurity risk assessment guided by ISO 27005 into the existing MD risk assessments guided by ISO 14971 that are already undertaken. Finally, we will deliver tools and toolboxes that support three key stakeholder roles in the CMD lifecycle. Medical Device Manufacturers (DMs) are the creators of individual CMDs. System Integrators (SIs) are the architects and deployers of usage scenarios where the devices are connected to other devices and systems. Operators (OPs) are responsible for running the usage scenarios designed by System Integrators. Each stakeholder has different (and sometimes overlapping) needs of tooling and risk-benefit schemes. DMs need information about current best practice for cybersecurity, potential vulnerabilities of their devices and how to address them. In order to understand the risks of their device in its intended use, DMs also need information about their devices when they are used in real connected scenarios. SIs need information about the CMDs involved in their planned scenario plus other contextual information such as the stakeholders, actors, network infrastructure, other ICT systems the devices connect to – i.e., the systemic view of the scenario. OPs need the same information as Integrators, plus dynamic runtime warnings of threats, vulnerabilities, emergency situations, resulting risks along with decision support on how to proportionately address these risks.

3.1. MD Cybersecurity Guideline Assessment

There are regulations and guidelines surrounding the field of medical devices covering different aspects of their life cycle, from the design, implementation and integration [24], procurement process from healthcare providers [13], post market normative (FDA Post market requirement guide for medical devices), just to name a few. These regulations vary depending on the geographical market targeted. This lack of uniformity and harmonization proves to be one of the challenges faced by manufacturers when it comes to figuring out what regulations apply to their devices. As such, an important part of NEMECYS aims to identify and map the existing regulations, guidelines and best practices along with the up-coming ones (e.g., revised pre-market guidelines from the FDA in 2023) in order to propose revisions to the MDCG 2019-16 [24] aligned with other regulations and guidelines. To achieve this, a systematic review of the current guidelines and regulations will be performed, followed by an applicability assessment and identification of gaps; stakeholders from the different stakeholder groups will be involved in eliciting to which extent the existing guidelines are effective, and to identify the key points that could increase their effectiveness, considering both current and future needs. The existing guidelines [24] will be employed in each of the NEMECYS case studies (see Section 4) to identify potential blocking points and possible improvements that can enhance the applicability of the guidelines for the stakeholders.

3.2. Risk Benefit Schemes

The addition of specific cybersecurity risk management to MD risk management must be aligned with the overall goal of patient safety. The MDCG asserts: “there is a need to consider the relationship between ’safety and security’ as they relate to risk. [. . .] patients’ safety may be compromised due to ’security issues’ which may have ’safety impacts’.” There is thus a key issue in balancing cybersecurity and patient benefit, so that proportionate decisions may be made to ensure that patient safety is not compromised by “too much” or “too little” cybersecurity. Addressing this challenge is a core component of NEMECYS research by investigating trade-offs between cybersecurity risk, clinical benefit and ethical practice. We will unify approaches to CMD benefit-risk analyses with cybersecurity risk analysis approaches to enable cybersecurity risks to be compared with clinical benefits. We will express losses or reductions in clinical benefit or compromises of ethical practice as risks which will be balanced with cybersecurity risks and compliance to ensure that proportionate cybersecurity is applied in each situation.

We will support systemic risk assessment across a whole multi-stakeholder Connected Medical Device scenario as well as individual perspectives of each participant in a CMD scenario. This risk assessment will be supported at both design time and dynamically at runtime. Static modes concern risks associated with the entities in a scenario; and dynamic modes are where dynamic events generated (e.g. by vulnerability scanners such as Wazuh[3]) lead to updated residual risk levels, and additional controls are recommended when risk levels are raised.

We will extend existing open source machine inference cybersecurity knowledge and tooling [29] to encompass novel technologies, including IoT and widely dispersed, potentially ephemeral connections over e.g. 5G networks, processing in cloud data centres, software as a medical device, where AI / ML can be employed, risks to personal data, and risks of big data. We will identify different types of medical device, technologies and connected situations, and determine indicators of vulnerabilities they may have, the threats that may exploit these vulnerabilities, the risks that can result and controls that may reduce the vulnerabilities.

The above work is implemented as the NEMECYS Risk-Benefit Tool, which builds on extensive partner background from SINTEF and University of Southampton and which will be integrated into the NEMECYS toolboxes.

3.3. NEMECYS Toolboxes & Tools

NEMECYS addresses each of the above stakeholder roles corresponding to the CMD lifecycle (DMs, SIs and OPs) via the creation of three toolboxes, one per stakeholder role, which incorporate tools and methodologies relevant to each role. The toolboxes contain cybersecurity by design tools, secure integration tools, and secure operation tools developed within the project, and other available tools which contribute to increased cybersecurity of connected medical devices, as appropriate for the different stakeholders. Since CMDs generally are more long-lived than commodity devices, we will devise a dynamic update scheme where the tools can be kept current to match the needs of evolving CMDs and the scenarios they operate in.The three toolboxes are specified as follows.

Medical Device Manufacturer (DM) Toolbox: cybersecurity-by-design tools that help CMD manufacturers build security in from inception of their products via updated guidelines, best practice and cybersecurity risk-benefit tooling that identifies vulnerabilities in their devices and enables simulation of their devices in realistic CMD contexts to detect vulnerabilities exposed when their device is used with other devices.

CMD System Integrator (SI) Toolbox: enables MDs to be securely connected into connected scenarios with other devices operated by multiple actors, and to assess system-level cybersecurity with recommendations for controls to lower risks.

CMD (OP) Operator Toolbox: enabling secure operation of the CMD scenario with runtime monitoring and warnings of security vulnerabilities and risk assessment of changing situations.

4. Case Studies

Connected medical devices rely on alternative power sources and offer a broad spectrum of connectivity, complexity, and deployment conditions. The digital capabilities of many medical devices extend beyond their primary purpose of detecting, treating, curing, or preventing disease, allowing them to interact and integrate with other networks and systems.Frequently, these devices are connected to a hospital network, which enables interaction between various devices within the network, including computers, mobile devices, imaging and medication delivery systems. While this network enhances the efficacy and continuity of healthcare, insufficient network security monitoring raises considerable risks [31]. Numerous currently-used medical devices were not designed with security in mind, as clinical reasons were the main focus throughout the development. The lack of high-qualified IT personnel in the healthcare industry leads to increasing cybersecurity concerns for the hospitals [4].

[3] https://wazuh.com/

Motivated by the above, four case studies [10] of connected medical devices are investigated to further illustrate the cybersecurity risks associated with real-world applications. Specifically, the bioimpedance measurement patch [22], the Parkinson's disease monitor [3], smartphone-based app covering the ”software as a medical device” paradigm [16], and the in-vitro diagnostic (IVD) device [32] will be deployed, as described in the following subsections. Each of the NEMECYS case studies will utilize the MDCG 2019-16 [24] advice during the appropriate phases of their lifecycles as part of the attempt to determine relevance and potential gaps among the various stakeholders involved. The results of the investigations will be compiled and incorporated into a gap analysis with recommendations to the guidelines.

4.1. Home Dialysis

The focus of this case study is a bioimpedance monitoring patch for patients with End-Stage Kidney Disease (ESKD) who have minimal or no remaining kidney function; thus, fluid and waste accumulate in the body. During dialysis, the patient will eventually rely on the elimination of waste and extra fluid. This is most beneficial to the body when it is performed frequently. This is tough to implement at a hospital for practical and logistic reasons. Home dialysis [11] can provide greater flexibility, since it can be adapted to times that are more suitable for the patient, as well as additional advantages of being at home rather than in hospital, such as the elimination of travel time. The primary disadvantage of home dialysis is that the equipment is not currently connected to the hospital.

As home dialysis is part of specialist treatment, patients have limited alternatives for remote assistance from health care providers, and community nurses and general practitioners have limited ability to assist. To deal with this limitation, the aforementioned bioimpedance measurement patch supports home dialysis by collecting accurate hydration data in real-time and is capable of wireless communication with, for example, clinical information systems or smart-devices. The developed tools and toolboxes of the project will offer guidelines for the secure wireless transfer of the data from the bio-impedance patch to the gateway, and from the gateway to the health care system for further analysis. Customization of a secure method for providing software updates for the gateway and databases, a secure method for post-market surveillance to confirm usage for the intended purpose, and an option for providing user feedback without compromising patient confidentiality and data security are required.

4.2. Wearable Devices for Continuous Monitoring of Movement Disorders

The subject of this case study is a wearable medical device for continuous monitoring of movement disorders, such as Parkinson's disease [6]. By recording and analyzing several symptoms (such as postural instability, gait problems, ON/OFF situations, etc.), this device enhances treatment of Parkinson's disease patients.This information is supplemented with lifestyle and medication adherence data acquired via a mobile app on the patient's smartphone. This provides the physicians with a complete perspective of the progression of the patient's disease and enables them to alter and personalize the treatment accordingly. The solution consists of a collection of wearable devices and a Smartbox that collects and processes the data before transferring it to a cloud-based platform for physician visualization.

The solution architecture is a prevalent configuration for IoT devices, with accompanying cybersecurity vulnerabilities. Linux or Windows-based embedded Operating Systems might result in undesired exposure to attacks, as they frequently have more interfaces than necessary and may not be appropriately hardened. In addition, they are frequently an ”available target” in security solutions, making them easy to attack with minimal experience. If the system is not updated, this issue will only worsen with time. The physical security of the various ”in the wild”-deployed devices is another persistent issue with these IoT systems. Attackers may want to leverage a compromised component of the device to attack the entire ecosystem, and it is a real challenge for manufacturers to establish the right level of security. Spending too much on security will make the device too expensive, or simply not user friendly, while spending too little on security could have catastrophic consequences, such as a patient data leak. To address the aforementioned, risk assessment schemes and cost-benefit analysis, along with guidelines and recommendations, will be applied to ensure the secure development of IoT cloud-based systems. Considering that the solutions already exist, security tools from the NEMECYS toolboxes will be utilized to discover any existing vulnerabilities in the solution.

4.3. Software as Medical Device

The focus of this case study is a mobile phone application that patients, like those with diabetes, can use to manage their daily therapy [9]. These types of mobile phone applications are considered a Software as Medical Device, since they give recommendations to patients for the evaluation of the quantity of carbohydrate content in their foods, for the dosage of insulin, etc. Despite the disclaimers displayed by some legal manufacturers of these SaMD, the new EU regulation classes these applications as active medical devices from class I up to class IIb. This classification will enforce most of the manufacturers to reconsider their risk assessment of the intended use of the software.

One of the main risks to consider is the potential threats on the SaMD from other applications installed on the mobile phone or downloaded from the internet. Such threats can either alter the correct processing of the SaMD, steal personal / medical data, or induce output errors that could cause severe injuries to the patients. For these reasons it is very important to provide the manufacturers of SaMD devices additional tools that could help them secure their applications, the toolboxes developed in the NEMECYS project will be very valuable in this regard.

4.4. Hospital based Point-of-care testing

This case study focuses on IVD medical devices, which are utilized to determine the health condition of a person based on biological samples [21]. There is a wide variety of such devices, ranging from self-tests for pregnancy, blood glucose tests, and iron deficiency tests to sophisticated laboratory diagnosis. This case examines mostly the first group, namely self-tests. Allowing the patient to self-test at home has numerous advantages. First of all, travelling to the hospital is costly, both financially and in terms of time, and this is especially true for patients undergoing lengthy treatments. Additionally, this mitigates the burden on hospitals by freeing up laboratory resources that can then be allocated to situations that require more attention. Lastly, self-testing permits the patient to do a test whenever they deem it necessary, such as when they believe their condition is deteriorating.

In combination with a personalized nutrition plan, the ability to take these measures frequently can be extremely valuable. In fact, for a diet plan to be effective, it must take the patient's health conditions into consideration. Furthermore, it should be possible to collect these measures regularly and readily so that the nutritionist may adjust the food plan as needed. Diabetes and iron deficiency are two common disorders that might benefit substantially from this technique, as they can cause variations in the patient's health status that must be noticed and treated promptly. The presented case study comprises data interchange between patients' personal IVD medical devices and hospital infrastructure in order to collect patients' information that is monitored outside of hospital premises over time. Thus, every time the infrastructure of a hospital interacts with any of these devices, the risk of sensitive data exposure and infrastructure damage increases. Addressing Personal Data Leakage risk in our models and analytical processes can extend our capabilities and address Data Protection and Privacy Compliance as part of our risk assessment. Therefore, suitable procedures for recognizing and mitigating these risks must be implemented.

5. Conclusion

The increased interconnection of diagnostic and other medical devices offer great benefits to efficiency and effectiveness of healthcare, but these benefits can be negated if cybersecurity of the devices and the interconnected system as a whole is ignored. This paper has presented NEMECYS as one possible answer to this challenge, offering risk-benefit analysis schemes and other tools for important stakeholder groups.

Acknowledgements

This work has been supported in part by the European Commission Horizon Europe programme, grant number 101094323, the UK Research and Innovation (UKRI) Horizon Europe funding guarantee under grant numbers 10065802, 10050933 and 10061304, and the Swiss State Secretariat for Education, Research and Innovation (SERI).

References

[1] American Psychological Association, 2016. Ethical principles of psychologists and code of conduct. URL: https://www.apa.org/ethics/code/.

[2] Amnesty International, Access Now, 2018. The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems. URL: https://www.amnesty.org/en/documents/pol30/8447/2018/en/.

[3] Antonini, A., Reichmann, H., Gentile, G., Garon, M., Tedesco, C., Frank, A., Falkenburger, B., Konitsiotis, S., Tsamis, K., Rigas, G., et al., 2023. Toward objective monitoring of parkinson's disease motor symptoms using a wearable device: wearability and performance evaluation of pdmonitor®. Frontiers in Neurology 14, 1080752.

[4] Ayala, L., 2016. Cybersecurity for hospitals and healthcare facilities. Berkeley, CA .

[5] Beauchamp, T.L., Childress, J.F., 2001. Principles of biomedical ethics. Oxford University Press, USA.

[6] Bloem, B.R., Okun, M.S., Klein, C., 2021. Parkinson's disease. The Lancet 397, 2284–2303.

[7] Bochniewicz, E., Chase, M.P., Coley, S.C., Wallace, K., Weir, M., Zuk, M., 2021. Playbook for threat modeling medical devices. URL: https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf.

[8] Boote, J., Erlikhman, E., Gardner, S., Migues, S., 2022. BSIMM13 foundations report. URL: https://bsimm.com.

[9] Brzan, P.P., Rotman, E., Pajnkihar, M., Klanjsek, P., 2016. Mobile applications for control and self management of diabetes: a systematic review. Journal of medical systems 40, 1–10.

[10] Cai, Y., 2018. Using case studies to teach cybersecurity courses. Journal of Cybersecurity Education, Research and Practice 2018, 3.

[11] Chan, C.T., Wallace, E., Golper, T.A., Rosner, M.H., Seshasai, R.K., Glickman, J.D., Schreiber, M., Gee, P., Rocco, M.V., 2019. Exploring barriers and potential solutions in home dialysis: an nkf-kdoqi conference outcomes report. American Journal of Kidney Diseases 73, 363–371.

[12] ECHR, 1953. European Convention on Human Rights - Official texts, Convention and Protocols. URL: https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=.

[13] ENISA, 2021. Good practices for the security of healthcare services. URL: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health/good-practices-for-the-security-of-healthcare-services.

[14] European Commission, 2019. Ethics guidelines for trustworthy AI | Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[15] Flå, L.H., Jaatun, M.G., 2023. A method for threat modelling of industrial control systems, in: Proceedings of the 2023 Cyber Science Conference. URL: https://jaatun.no/papers/2023/A%20method%20for%20threat%20modelling%20of%20industrial.pdf.

[16] Gerke, S., Babic, B., Evgeniou, T., Cohen, I.G., 2020. The need for a system view to regulate artificial intelligence/machine learning-based software as medical device. NPJ digital medicine 3, 53.

[17] GOV.UK, 2019. A guide to using artificial intelligence in the public sector. URL: https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector.

[18] GOV.UK, 2021. Digital and data-driven health and care technology. URL: https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology.

[19] ISO, 2013. Information technology — Security techniques — Information security management systems — Requirements. Standard ISO/IEC 27001:2013. URL: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html.

[20] ISO, 2019. Medical devices — Application of risk management to medical devices. Standard ISO 14971:2019. URL: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html.

[21] Lan, T., Zhang, J., Lu, Y., 2016. Transforming the blood glucose meter into a general healthcare meter for in vitro diagnostics in mobile health. Biotechnology advances 34, 331–341.

[22] Lindeboom, L., Lee, S., Wieringa, F., Groenendaal, W., Basile, C., van der Sande, F., Kooman, J., 2022. On the potential of wearable bioimpedance for longitudinal fluid monitoring in end-stage kidney disease. Nephrology Dialysis Transplantation 37, 2048–2054.

[23] McGraw, G., 2004. Software security. Security & Privacy, IEEE 2, 80–83. doi:10.1109/MSECP.2004.1281254.

[24] Medical Device Coordination Group, 2020. MDCG 2019-16 - Guidance on Cybersecurity for medical devices. URL: https://ec.europa.eu/docsroom/documents/41863.

[25] Muirhead, W., 2012. When four principles are too many: bloodgate, integrity and an action-guiding model of ethical decision making in clinical practice. Journal of Medical Ethics 38, 195–196. Publisher: Institute of Medical Ethics.

[26] Oates, J., Carpenter, D., Fisher, M., Goodson, S., Hannah, B., Kwiatowski, R., Prutton, K., Reeves, D., Wainwright, T., 2021. BPS Code of Human Research Ethics. British Psychological Society, Leicester. URL: https://www.bps.org.uk/sites/www.bps.org.uk/files/Policy/Policy%20-%20Files/BPS%20Code%20of%20Human%20Research%20Ethics.pdf.

[27] Oueslati, H., Rahman, M.M., ben Othmane, L., Ghani, I., Arbain, A.F.B., 2016. Evaluation of the challenges of developing secure software using the agile approach. International Journal of Secure Software Engineering (IJSSE) 7, 17–37. Publisher: IGI Global.

[28] OWASP, 2020. Software assurance maturity model (SAMM). URL: https://owaspsamm.org/.

[29] Phillips, S., Taylor, S., Boniface, M., Surridge, M., 2023. Automated knowledge-based cybersecurity risk assessment of cyber-physical systems doi:https://doi.org/10.36227/techrxiv.24061590.v1.

[30] PSA Certified, 2022. IoT Security Report 2022. URL: https://report.psacertified.org/.

[31] Pycroft, L., Aziz, T.Z., 2018. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. Expert Review of Medical Devices 15, 403–406.

[32] Sun, X., Wan, J.J., Qian, K., 2017. Designed microdevices for in vitro diagnostics. Small Methods 1, 1700196.