# AMBIENT ASSISTED LIVING TECHNOLOGIES – REGULATORY FRAMEWORK AND SAFETY AND SECURITY CONCERNS

Michal Koscik

Michal Koscik, Researcher, Masaryk University, Faculty of Medicine, Faculty of Law, SYRI institute, Kamenice 5, 625 00, Brno, Czechia, E-Mail; koscik@med.muni.cz ; https://www.muni.cz/en/people/76882-michal-koscik

***Keywords:*** ***Information security, Ambient assisted living, AI, Natural language user interface***

***Abstract:*** *The paper provides an overview of the prevailing regulatory framework and highlights challenges concerning the safety, security, and protection of rights related to Ambient Assisted Living platforms. These platforms are intricate ecosystems comprising information technology, consumer products, medical devices, and quasi-medical devices. The paper argues that the current regulatory framework is insufficient to regulate larger environments composed of mixed hardware and software elements. It tends to focus on the functioning of individual pieces of technology, leaving AAL platforms vulnerable from an information safety and security perspective. The expansion of language models and the growth of AI technologies bring new capabilities, but also risks of potential exploitation or misleading of the end user.*

## 1. Introduction

The decade from 2010 to 2020 saw significant advancements in electronic health and mobile health applications. The emerging concept of the Internet of Things expanded the scope of internet usage in healthcare. Governments, companies, and research institutions recognised that the internet could be utilised for more than just the exchange of electronic records between healthcare providers or online consultations between patients and physicians. It became clear that digitalisation in healthcare entails more than just adopting electronic health records and enhancing digital healthcare communication. The push for digitalisation is now directed towards advanced electronic decision support systems for physicians, tools for patient self-management, and electronic systems for telemonitoring care processes.[1] The concept of Ambient Assisted Living presented a „captivating technology that seamlessly integrates into ‚smart home environments' and aids individuals in their everyday lives."[2]. Within this concept, the monitoring of individual well-being, lifestyle counselling, diagnostics, and even treatment become constantly present and automated aspects of life. This integration is made possible by the interoperation of various household devices and wearable sensors. Some of these are classified as medical devices, while others are considered regular consumer products. AAL technologies merge single-purpose medical devices designed for specialised tasks, such as insulin pumps, glucometers, heart rate sensors, or oximeters, with general multi-purpose devices like personal computers, smartwatches, Wi-Fi routers, and internet networks. Prime examples of these practical applications include diabetes management systems[3] or systems designed to monitor the well-being of the elderly. They also assist caregivers in

[1] Melchiorre, Maria Gabriella et al. eHealth in integrated care programs for people with multimorbidity in Europe: Insights from the ICARE4EU project. In: Health Policy Vol. 122, No. 1, 53-63 (2018).

[2] Fagerberg/Gunnar et al. „Platforms for AAL applications." In European Conference on Smart Sensing and Context, Springer, Berlin, Heidelberg, 177-201 (2010).

[3] See e.g. Jara/Zamora/MiguelSkarmeta/Antonio. An internet of things–based personal device for diabetes therapy management in ambient assisted living (AAL). In: Personal and Ubiquitous Computing, Vol. 15, No. 4, 431-440 (2011).

addressing the repetitive behaviours of patients with dementia.[4] With the rapid evolution of AI and machine learning, the potential for AAL is vast. Future systems might predict potential health challenges before they manifest, offer virtual companionship to the lonely, or even integrate with advanced robotics to offer physical support.

Much like other areas of medical technology, take-home medical devices and wearable sensors bring about concerns of potential malfunctions. Beyond just the mechanical failures of hardware, there's the risk of malware attacks or unforeseen software errors and errors caused by malfunctioning interoperability to consider. Another significant concern is the potential threat that the adoption of AAL technology poses to an individual's privacy. In this context, AAL technology and wearable devices mirror challenges faced by other e-health technologies. After all, security and privacy issues are prevalent across all digital technologies employed in patient care.[5]

## 2. Is AAL technology a medical device or consumer product?

The AAL technology has been widely encouraged by governments as they perceived AAL technology as a part of their public health policy. AAL has potential to lead individuals to healthier lifestyle, to reduce negative impacts of diseases on one's lifestyle[6] and makes delivery of healthcare more efficient. The AAL technologies have also significant social policy context as it has potential to reduce inequalities in access to healthcare for vulnerable patients, elderly, or individuals living in remote areas and can potentially reduce a social isolation of the aged population[7].

On the other hand, private sector and technological companies see AAL technologies as an opportunity to extend the functionality of the already existing multi-purpose technological solutions. The e-health and m-health is perceived as a vehicle for adding more users and increase the network effect of the existing eco-systems[8] (an example, the smart functions of wearable electronics or smart-home devices).

The two different approaches lead to two different designs. The healthcare-centric design focuses on improving the functionality of individual medical device, or efficient treatment of a specific disease. AAL is seen as an extension to the system of healthcare, with the objective of make healthcare system more efficient. The individual devices necessary for functioning of AAL are designed and distributed as medical devices. The end user learns about the functionalities of the technology from his healthcare provider and often cannot purchase the technology without direct prescription/referral of the provider.

The IT-centric design focuses AAL as an extension of technological environment, usually provided by big technology firm. The objective is to offer the broadest possible range of features to the already established "ecosystem" of hardware and software products[9]. The individual devices are designed and marketed mostly as gadgets/consumer goods, which sometimes have certifications of medical devices. For example, „Apple Healthcare"[10] product range includes software, hardware and cloud solutions to deliver personalized medical care without having a single product whose primary function is a function of a medical device. The end user

4 Cedillo et al. A systematic literature review on devices and systems for ambient assisted living: solutions and trends from different user perspectives. In: 2018 International Conference on eDemocracy & eGovernment (ICEDEG), IEEE, 59-66 (2018).

5 Hoffman/Podgurski. E-Health hazards: provider liability and electronic health record systems. In: Berkeley Tech. LJ Vol. 24, 1523 (2009).

6 For example diabetes management systems. See Jara/Zamora/MiguelSkarmeta/Antonio. An internet of things–based personal device for diabetes therapy management in ambient assisted living (AAL).

7 Manoj/Thyagaraju. Active and assisted living: a comprehensive review of enabling technologies and scenarios." International Journal of Advanced Research in Computer Science Vol. 9, No. 1 (2018).

8 A good example is oximeter function of a smart watch or voice scanner in Amazon Halo wristband.

9 „Healthcare - Products and Platform". b.r. Apple. Viděno 14. březen 2021. https://www.apple.com/healthcare/products-platform/.

10 See - https://www.apple.com/healthcare/products-platform/ (cited 22.12.2023). It is important to note, that the presentation of product range is targeted to US audience. In Europe, the displayed hardware and software solutions are also available, but not presented as a healthcare product range.

receives the information about the functionalities of the devices from manufacturer and purchases the product on his own via commercial vendors.

The differences of the two designs have significant legal implications, because both frameworks have origins in different regulatory backgrounds. The safety and security standards on medical devices are arguably higher than safety and security standards of consumer products[11]. The AAL environment blurs the border between regular consumer products and medical devices. It is important to ask, whether we the standards applied on medical devices shall be also applied on all elements of IT ecosystem that offers AAL features. Consumer driven healthcare empowers patient autonomy and provides patients with a choice[12], however the emergence of this trend needs to meet with the response of a regulator. Some states, like US[13] and India[14] have reflected this trend in their rules governing consumer goods with dual-use[15] and marketing of consumer products for healthcare[16]. The European framework remains fragmented and as will be described in the next section, develops in two separate regulatory channels for consumer products and medical devices.

## 3. European regulatory framework

### 3.1. Medical devices regulation

#### 3.1.1. The definition of a medical device

The second Article of the Medical devices regulation[17] (MDR) defines the "medical device". According to the definition, the main criterion to asses, whether an individual product shall be considered as a medical device is the *intention of the manufacturer* to design and sell product that can be used for medical purposes.[18] The device, which has multiple possible uses in medical and non-medical areas shall fulfil cumulatively the requirements applicable to devices with an intended medical purpose and those applicable to devices without an intended medical purpose.[19] The *intended purpose* is assessed by the manufacturer's statements and promotions of the device on the label, in the instructions for use or in promotional or sales materials.[20] The MDR also defines accessory for a medical device, an article which, "whilst not being itself a medical device, is intended by its manufacturer to be used together with one or several particular medical device(s) to specifically

11 Even though the current European regulatory framework puts relatively high standards on product safety as well as on information security of IT ecosystem.

12 Hoffman/Podgurski. E-Health hazards: provider liability and electronic health record systems. In: Berkeley Tech. LJ Vol. 24, 1523 (2009).

13 Hodge/James/Gostin/Jacobson. Legal issues concerning electronic health information: privacy, quality, and liability. In: JAMA 282.15, 1466-1471 (1999)

14 Nomani/Rahman/Alhalboosi. Consumer Protection Act, 2019 and its implications for the medical profession and health care services in India." Journal of Indian Academy of Forensic Medicine 41.4, 282-285 (2019).

15 Yang/Ross. Mobile health applications: the patchwork of legal and liability issues suggests strategies to improve oversight. In: Health affairs Vol. 33, No. 2, 222-227 (2014).

16 Hollon. Direct-to-Consumer Advertising: A Haphazard Approach to Health Promotion. In: JAMA. 2005., 293(16): 2030–2033. doi:10.1001/jama.293.16.2030 (2005).

17 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

18 The list what is considered to be a medical purpose contains: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,; investigation, replacement or modification of the anatomy or of a physiological or pathological process or state; providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations.

19 Art. 1 par (3) MDR.

20 Art. 2 par (12) MDR.

enable the medical device(s) to be used in accordance with its/their intended purpose(s) or to specifically and directly assist the medical functionality of the medical device(s) in terms of its/their intended purpose(s)".[21]

### 3.1.2. The information security standards of MDR

The general rules for medical devices that require interaction with their environment are described in the Art. 14 of the MDR. If the device is intended for use in combination with other devices or equipment the whole combination, including the connection system shall be safe and shall not impair the specified performance of the devices. Medical Devices that require interaction must be manufactured in such a way as to remove or reduce risks connected with reasonably foreseeable external influences or environmental conditions.[22]

The Regulation on medical devices (EU) 2017/745 recognises devices that incorporate programmable systems and non-implantable active devices. Manufacturers shall set out requirements concerning and IT security measures, including protection against unauthorised access. Not all devices that are used for home-diagnostics, Active Assisted Living or as "fitness wearables" are marketed as medical devices. The manufacturer or distributor can choose whether he subjects himself to the regulation of the directive or not by marketing strategy. Devices that are not marketed as „medical devices" are not subject to the Regulation 2017/745.

Software alone can be considered as a medical device.[23] The standards for "Electronic programmable systems" (i.e. devices that are based on software or contain programmable element) are set forth in the Art. 17 of the MDR. The manufacturers have duty to ensure repeatability, reliability and performance in line with their intended use.[24] The software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation. Software that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).[25] Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

## 3.2. General Data Protection Regulation

General Data Protection Regulation (GDPR)[26] is built around the legal principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability.[27] Apart from the main principles, the data controller has to make sure, that the rights of the data subject stated in the third chapter of GDPR are respected. These rights revolve around transparency of the data processing, right to access to the personal data and transfer them to another controller, information on the sources of personal data, rights for objections, rectification and erasure. Biometric data and data concerning health data are considered as special categories of data,[28] which means that they need to be processed only under explicit consent that relates to defined purposes.

---

21 Art. 2. par (2) MDR.
22 Art. 14 par (3) MDR.
23 See Art. 2 par. (1) MDR.
24 Art. 17 par. 1.
25 Art. 17 (3).
26 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://data.europa.eu/eli/reg/2016/679/oj.
27 Art 5 GDPR.
28 Art 9 GDPR.

AAL technologies process special categories of data and often include systematic and extensive evaluation of patients based on automated processing, which means the necessity of data protection impact assessments.[29] The responsibility to ensure that all of the rights above are respected lies mainly on the controller of the personal data. The controller is any entity which alone or jointly with others, determines the purposes and means of the processing of personal data.[30] The processor[31] is a provider of service that carries out processing of data on behalf of the controller without using data for other purposes. The efficient operation of a take-home device or a medical device integrated into an AAL (Ambient Assisted Living) system necessitates data processing by various controllers and data processors. In this scenario involving multiple participants, it is crucial to identify which party assumes the role of controller and which assumes the role of processor. This distinction is important to understand their respective liabilities for the security of the personal data involved.

In a healthcare-centric design, the healthcare provider who recommended, prescribed, or distributed the technology to the end-user (patient) is the ultimate controller of personal data. The manufacturers of hardware components, developers of software solutions, and providers of data services act as data processors. They have very limited legal bases for using the data for their own purposes. The end-user (patient) assumes the role of data subject, who has several rights with respect to the data controller, especially those granted by the third chapter of the GDPR. In this context, the healthcare provider bears the primary responsibility for ensuring the security of processing,[32] for providing appropriate risk assessments[33] and for allocation of responsibilities. It can be assumed that a healthcare provider licensed in an EU country possesses the technical capability to select reliable processors. These processors should provide sufficient guarantees to implement appropriate technical and organisational measures. This ensures that the processing complies with the requirements of this Regulation and safeguards the rights of the data subject. In this scenario, the primary responsibility for the safety of patient data rests chiefly with the healthcare provider. The liability of other participants is confined to breaches of contractual obligations. For the patient, the liability for his own harm, it is limited to instances of patient's non-compliance with instructions on how to use the technology properly.

In an IT-centric design, where the healthcare provider is absent or plays a peripheral role, the end user becomes the ultimate controller of the data. However, in this context, it becomes significantly easier for the provider of the technological solution to obtain consent to use the data for their own purposes. Here, the provider of the hardware/software solution assumes primary responsibility for the security of data processing and conducting appropriate risk assessments, whether acting as a data controller or a processor. It's noteworthy that the entire ecosystem of exchanging patient data is governed by GDPR in both scenarios. Yet, in the absence of a licensed healthcare provider, key regulatory mechanisms common in the healthcare industry in European countries—such as physician-patient privilege, standardization of medical information, protection of vulnerable subjects, surrogate consent, and decision-making support—are missing. On one hand, this reduces transaction costs, expedites the process of receiving the device for the end-user and makes patient less dependent on the healthcare provider. On the other hand, a scenario where the patient acts as the ultimate data controller assumes that the patient is fully capable of making informed decisions, both legally and in terms of actual understanding of what they are consenting to. The healthcare-centric setting can potentially identify gaps in a patient's capacity to understand, decide, and consent—gaps that an IT-centric design simply cannot address.

[29] Art. 35 GDPR.
[30] Art. 4 (7) GDPR.
[31] Art. 28 GDPR.
[32] Art. 32 GDPR.
[33] Art. 35 GDPR.

### 3.3. The Network and Information Security Directive

The first Network and Information Security Directive[34] (hereinafter called also "NIS 1") mandates member States to identify and regulate security measures of *operators of essential services* and *providers of digital services.* Operator of essential service is an entity that provides a service which is essential for the maintenance of critical societal activities via networked information systems and could be disrupted by a security incident.[35] A good example of operator of operator of essential service would be a large regional hospital that would equip its patients with medical devices to monitor their health status during their lives outside the hospital. The security requirements for this system are defined mostly in the chapter IV of the NIS Directive.

However, if the equipment used in AAL setting is provided by the tech-company as an extension of ecosystem of cloud-based solutions, it could be qualified as a *digital service* and regulated under the standards of the chapter V. Under this framework, itis was also possible that standards of both chapters must be achieved if a medical device provided/prescribed by a healthcare provider but integrated in a network that uses solutions of a commercial consumer platform. The "NIS 2" Directive[36] broadens the scope of its predecessor, "NIS 1", to cover a wider range of sectors and entities and includes also certain pharmaceutical companies and producers of certain medical devices. The factual impact of the "NIS 2" Directive on AAL platforms is yet to be seen, but it can be expected, that most AAL solutions that did not fall under the scope NIS 1 directive will remain outside of the scope of "NIS 2" Directive as well. The improvement might be seen in emphasis on more complex approaches to security of networked solutions that are integrated into formal healthcare provision.

#### 3.3.1. AI Act – projected impact

It is plausible to presume that a significant portion of Ambient Assisted Living (AAL) platforms will fall under the purview of the proposed EU AI Act.[37] This legislative proposal endeavours to establish a uniformed framework governing the conception, implementation, and utilisation of artificial intelligence (AI) technologies. In the context of AAL solutions, which will very likely tend to incorporate AI in order to improve their functionality related to health, well-being, and routine activities, certain specifications of this proposal become exceedingly pertinent. Depending on their inherent functionalities, AAL systems may be categorised as ‚high risk', particularly if they have a direct bearing on health, safety, or foundational human rights. For example, an AAL system that employs AI for the monitoring of vital signs or the dispensation of medication could potentially be classified as ‚high risk' due to the consequential ramifications of any operational aberrations. On the other hand, the strict regulatory framework of high risk AI solutions may lead developers to design their platforms without certain high risk functionalities and offering "limited risk" functionalities instead. For example, as chatbots with general advice who fall within the scope of proposed Art. 52 of the AI act, rather than chatbots that can warn about immediate threats to life and health under Art. 6 and following. The economic incentive to incorporate "high risk" functions might be too small in comparison with risks and liability. We can only speculate, that the division between "high risk" solutions that will be incorporated into formal healthcare and "limited risk" consumer solutions will remain even after AI Act comes into force.

[34] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ELI: http://data.europa.eu/eli/dir/2016/1148/oj.

[35] See Art. 5 (2) "NIS 1".

[36] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

[37] COM/2021/206 final: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52021PC0206.

### 3.4. National rules

The regulation matrix of take home devices incorporated into AAL platforms becomes more complex when we take into the consideration the national rules regarding physician-patient privilege and rules regarding keeping and accessing health records.[38] The application of national rules, however, is beyond the scope of this paper.

## 4. Liability issues

### 4.1. Liability for product malfunction

The form of liability for a product malfunction is different if a device is supplied via commercial channels based on consumers preferences and decisions or if it is supplied via healthcare system or on recommendation of a healthcare provider.

A consumer product that does not function properly or develops a mechanical flaw can be returned during warranty period. The producer is liable for any damage that is caused by the product[39] and relates to both material damage on property as well as immaterial damage to life and health. The directive does not however cover other forms of immaterial damage, such as damage to privacy, personal life or family life. The right of redress would be applied to the final seller in a contractual chain.[40]

If a medical device was purchased directly by an individual, his claims towards the final seller for product malfunction and even injury might be similar to any regular consumer products, even if healthcare products and medical devices are explicitly excluded from certain rules regarding the consumer rights.[41] However, significant proportion of medical devices handed out to individuals is procured by public entities, distributed by a healthcare system, handed out on basis of prescription. They often remain in the ownership of healthcare provider and are returned by the patient once they are not needed. In this setting any failure of a product is a potential medical malpractice. The medical malpractice claims may arise also form wrongly indicated use of a product that shows no flaw during the period of its indication. As opposed to liability for malfunction of a consumer product, the liability for medical malpractice includes also liability for all kinds of immaterial damage.

### 4.2. Liability for breach information safety or security

The privacy by design request incorporated in the GDPR means that the manufacturer or provider of any consumer product, including software product, has a broad responsibilities to protect the privacy and integrity of the consumers data. The secondary law of EU does not directly address the liability of an injury that could result from an information security breach. Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services does not apply on services regarding healthcare and does not cover medical devices. This means clear distinction between consumer and regulatory framework, as Considering the fact, that cloud-based services or software can be classified as a medical device.

Malfunction of medical device as a result of information security breach (regardless of intentional direct attack or unintentional interaction with other software solution) may lead to material and immaterial damage to the patient and will be considered as a medical malpractice in many scenarios. The healthcare provider usually

[38] Lytvynenko. Common law right to access to medical records: the commonwealth and European Court of Human Rights practice. In: 7th International Conference of PhD Students And Young Researchers, Vol. 2, (2019).

[39] Art. 1 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[40] Art. 4 Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees.

[41] Art. 3 (2) CHR.

bears objective responsibility[42] for any equipment he directly or indirectly uses in the process of treatment. It is well documented, that threats to security of information systems used in healthcare consist more of internal factors than external[43] but the healthcare provider would be most likely liable for both of them.

## 5. Conclusion

It is clear, that take home devices and wearables that can serve dual purpose have two regulatory frameworks which lead to different outcomes in manufacturer's or service provider's accountability. It is unsurprising to see that the regulatory framework puts higher standards and more severe liability outcomes on the devices and solutions that are marketed as a medical devices. Unlike regulatory frameworks in the USA and India which reflect the consumer driven demand for IT solutions in healthcare by applying healthcare standards on consumer products, the EU secondary law tries to draw clear distinctions between the two regulatory frameworks. This however allows for a regulatory "forum shopping". Unless manufacturers market their dual-use products as ‚medical devices', they can avoid the strict regulations applicable to medical devices in the European market, even if these products can interact with other medical devices or function de facto as medical devices Most consumers are not likely to distinguish between a medical device that is certified as such and a regular consumer product. This regulatory environment is favourable for large tech companies which are able to market "health" applications connected to wearable sensors which are marketed as commercial products with relatively low responsibility for its actual functionality. On the other hand, the healthcare providers, who recommend and supply certified products to their patients for home treatment carry objective liability for every security incident, even if such incident was caused by interaction of regular consumer product.

## 6. Funding

This work of the author during the work on this paper is supported by Ministry of Education, Youth and Sports of the CR / Operational Programme Research, Development and Education, CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence (CZ.02.1.01/0.0/0.0/16_019/0000822) and "Systemic Risk Institute" number LX22NPO5101, funded by the European Union—Next Generation EU (Ministry of Education, Youth and Sports, NPO: EXCELES).

[42] Gong. Objective Responsibility vs. Subjective Responsibility: A Critical Reading of the CCP's Internal Supervision Regulation. In: China Review, Vol. 8, No. 2, 77–102 (2008).

[43] Kierkegaard. Electronic health record: Wiring Europe's healthcare. In: Computer Law & Security Review Vol. 27, no. 5, 503-515 (2011).