Development of medical applications based on AI models and register data – regulatory considerations

Jaakko Lähteenmäki, Juha Pajula and Emmi Antikainen
VTT Technical Research Centre of Finland Ltd., Finland
jaakko.lahteenmaki@vtt.fi

Abstract
Artificial intelligence based methods, especially machine learning (ML), are increasingly used in healthcare for automatic medical image analysis and clinical decision support systems. Development and validation of ML models involve processing of large volumes of personal data. We analysed regulatory impacts on ML based application development especially from the perspective of privacy protection and usage of ML models as a basis for software under medical device regulation (MDR). We present best practices for ML application development and personal data usage in a use case of predicting elderly individuals' future need for healthcare and social welfare services.

Keywords
Artificial intelligence, machine learning, medical device regulation, MDR, privacy protection

1 INTRODUCTION

There is a growing interest towards the use artificial intelligence (AI) to improve healthcare [1]. Machine learning (ML) is extensively used for automatic medical image analysis for supporting and improving human interpretation. It is increasingly also used to support precision medicine by predicting patient outcomes, identifying patients with elevated risk and suggesting most favourable care pathways and services for the patients. Machine learning models empower decision support applications providing guidance to healthcare professionals and patients [2, 3]. Such applications potentially affect the healthcare of an individual patient, and are considered to be Medical Device Software (MDSW) falling under the Medical Device Regulation (MDR) [4].

Regulatory compliance is based on rigorous risk management and release acceptance processes. This is a challenge for ML based applications, which shall be validated against personal health data, and typically would need to be frequently updated as new data becomes available. Also, the use of agile and continuous development approaches causes the need for frequent software updates challenging the conventional "waterfall-type" development process [5]. The challenges caused by frequent software changes in the context of medical devices have been addressed in several earlier studies and reports [6–8].

Only a few earlier papers address the challenges related to the need to use sensitive healthcare register data in the development of medical device software [8]. In the present paper, we will analyse the regulatory impacts on ML based application development from the perspective of sensitive personal data usage. We will address the relevant development phases starting from research and modelling activities and extending to medical software development and deployment. Detailed analysis of the development phases is beyond the scope of the paper. Our purpose is to provide an overview of the topic highlighting observations that we have made during the planning and data collection phase of the MAITE project, which aims at data-driven prediction of the need for health and social services.

2 RELEVANT REGULATION

2.1 Personal data protection

Access to individual level health data is a precondition for ML model development in the health domain. In most cases the data need to be acquired from one or more health data registers, such as electronic health record systems (EHRs). Real-world data (RWD) accumulated in EHRs can be made available by the respective data controller for so called *secondary use* referring to the usage of data for another purpose than the purpose for which the data was originally collected [9]. Secondary use of data may take place without the consent of the data subject based on *public interest* in the area of public health or scientific research as defined by the General Data Protection Regulation (GDPR), article 9(2) i, j. Some countries, e.g. Finland, have national legislation regulating secondary use of health data, and a related European-level legislative action is on-going [10]. Another data access option is the usage of data specifically collected for research, for example, based on the biobank consent given by the data subject [11].

Data sets available for scientific research - either based on public interest or consent - are typically pseudonymized.

The 18th Scandinavian Conference on Health informatics, Tromsø, Norway, August 22-24, 2022. Organized by UiT The Arctic University of Norway. Conference Proceedings published by Linköping University Electronic Press at https://doi.org/10.3384/ecp187.

Even though this encompasses removal of direct person identifiers of the data released for research use, the data could still be reidentified and, therefore, fall under the GDPR. Privacy of the data is in most cases protected by limiting its use to a secure processing environment (SPE) separated from the environment where the software is developed [12].

2.2 Medical device software

Legal and regulatory requirements for medical devices (including MDSW) in Europe are set out in the Medical Device Regulation 745/2017 (MDR) [4]. MDR classifies medical devices into risk groups (1, 2a, 2b or 3) with respective conformity assessment procedures. In practice, development under MDR requires the manufacturer to have a certified quality system (e.g. complying with the ISO 13485 standard) covering management processes, product requirements management, product realization, customer feedback and support. Food and Drug Administration (FDA) is responsible for the corresponding regulation in the United States, where the term Software as a Medical Device (SaMD) is used instead of MDSW [13].

ML based applications are problematic from the regulatory perspective as they may need to be updated when new data comes available [8, 14, 15]. FDA in the United States has published an action plan with concrete proposals to enable software changes to be implemented in a controlled way without a new regulatory approval. The FDA approach is based on a predetermined *change control plan* and *algorithm change protocol* which the manufacturer needs to specify upon product approval [16]. EU has chosen to provide related guidance through Artificial Intelligence Act (AIA) draft proposal, but is less explicit in defining the procedures to be adopted.

2.3 AI regulation

Specific EU-level regulation, the Artificial Intelligence Act (AIA) is currently under development [17] and will affect the development and use of AI based applications. AIA defines all AI systems under the Union harmonization legislation (including MDR) to be included in the high-risk category.

The AIA regulation complements the MDR in addressing aspects related to the quality of training, validation and testing data sets. The regulation specifically requires the manufacturer to record detailed documentation on the AI system development, including data cleaning and model training methodologies as well as usage of third-party tools. AIA also addresses several ethics-related issues, such as interpretability of results produced by an AI system and the need for human oversight in the service provision context.

2.4 Healthcare information systems

Medical device regulation, referred above, is focused to ensure the safety and performance of the product. ML based medical software typically needs to be integrated in the information system environment of a healthcare service [18, 19]. Such integration may be subject to additional regulation besides the MDR [20]. Healthcare infrastructures are to a large extend country-specific and regulated by national laws and requirements [21]. Additionally, GDPR and AIA set considerable limits to the use of AI in automatic decision making and profiling.

3 APPLICATION DEVELOPMENT PHASES

ML application development phases and their main linkage to regulation are indicated in Table 1. The application development lifecycle is divided into three major phases: research, software development, and application deployment.

3.1 Research

The research phase starts by defining the study approach and objectives in co-operation with the relevant healthcare professionals and other domain experts. The research plan describes the target population (inclusion criteria), research methodology, and data contents to be used. The development of an ML model typically falls to the category of exploratory research, where study endpoints are not known at the time of data permit application and are not explicitly defined in the study protocol. The research plan is an important part of the data permit application and shall comply with standard scientific research practices to be aligned with the GDPR requirements concerning access to data for secondary purposes.

After positive data permit decision, the data resources are made available for the data user. Data usage is subject to several restrictions due to the sensitivity of the data. Most typically, the data is made available for research in a secure processing environment (SPE), which provides the tools, storage capacity and computing resources needed for data processing, but does not allow exporting the data out of the environment. The installation of additional data analytics tools may also be subject to approval by the permit authority, and the availability of high performance computing (HPC) resources may be limited.

These limitations may complicate ML model development. On the other hand, the SPE approach can also be seen as an enabler for using data resources, which would not be accessible otherwise. Furthermore, an external SPE may be an attractive alternative for a research organization, which can avoid to invest in its own computing resources. SPE's are still emerging and expected to be improved in terms of services and computing performance.

3.2 Software development

Depending on the results of the research phase, the software development activity in line with MDR requirements may be started after completion or during the research phase. The ML model developed in the research phase should include only anonymous information (e.g. tuned model coefficients), which enables the model to be exported from the SPE and used in the medical device software development process.

Regulation	Research	Software development	Application deployment
GDPR	Privacy and ethics of data usage for research and development	Privacy and ethics of the product	Privacy and ethics of the operational service
AIA	Privacy and ethics of data usage for research and development	Privacy, ethics, resilience and performance of the product	Privacy, ethics, resilience and performance of the operational service
MDR	ML-model documentation to enable traceability	Product safety and clinical performance	Enabling post-market surveillance
National regulation	Regulation on secondary use of data	Privacy, security, interoperability, functionality (digital health applications)	Privacy, security, interoperability, functionality

Table 1. Regulatory objectives in the development phases of ML based health applications.

The basic requirement for medical device software is that the released product is safe and provides the declared clinical benefits. When significant changes are introduced for class 2a devices or higher, they need to be approved by a Notified Body [4]. Applicable standards (in particular IEC 62304:2006 medical device software – software life cycle processes) expect the development cycle to be divided into phases such as product planning, product design, design transfer, product realization and release.

Each phase ends in a design review, where final versions of the created documents and other artefacts are reviewed and approved. As indicated above in Section 2.2., new approaches for enabling agile updating of AI based applications are being introduced both in the USA and in Europe.

3.3 Application deployment

ML based applications are typically not stand-alone applications, but need to be integrated in health and social services information system environment. For example, a decision support application needs to be integrated with an EHR system to get access to patient records. Such deployment may be subject to additional national regulation besides the MDR [21]. The purpose of such national requirements is to ensure correct exchange of information between software components, appropriate personal data protection and resilience towards cyber-attacks. Certification demonstrating compliance with national requirements may be required. Also, joint testing with other software providers may be necessary to demonstrate interoperability [20].

Efficient clinical use of ML based applications requires, besides technical interoperability, also seamless integration with the clinical process. Although process-level integration would not be directly covered by regulation, it is a prerequisite for positive impact and clinical benefits of ML based applications. Therefore, it is important that ML based applications are reliable, compatible with current care guidelines and practices, show direct benefit for healthcare professionals and customers [22]. Also, final responsibility of treatment choices should always rest with the healthcare professional, and ML based applications should only be use as assistive tools [23] .

4 BEST PRACTICES - CASE “MAITE”

In the following, we will analyse typical challenges in developing and deploying ML based applications and deploying them in health and social services. As an example, we will use the MAITE project (Data-driven identification of elderly individuals with future need for multi-sectoral services), where VTT Technical Research Centre of Finland Ltd. (VTT) is responsible for ML model development. We will identify the best practices to be adopted in the MAITE project to overcome the challenges of ML application development.

4.1 Case overview

The MAITE project emerges from the observation that health and social services expenditure is concentrated to a small fraction of the population [24]. It is expected that future heavy users of services could be identified based on their current health and social status and service usage history. The objective of the project is to develop an ML based model and proof-of-concept (PoC) application for predicting future service usage of elderly individuals. The model would support personalized and group-level preventive interventions to avoid excessive service need in the future.

VTT is responsible for the ML model development based on register data of Päijät-Häme Joint Authority for Health and Wellbeing (PHHYKY), a public health and social services provider with catchment area of 200 000 inhabitants in Southern Finland. The Finnish institute of health and welfare (THL) is responsible for coordinating the co-operation of stakeholders and ensuring continuous interaction between developers and end-users. The project is currently in the research phase with the data permit application recently accepted. The data permit covers the data resources listed in Table 2.

Data resource	Data description
Health and social services encounter data (Effica and Lifecare systems)	Basic demographic information: age, sex, municipality of residence. Information about health and social services visits: primary and specialized healthcare outpatient and inpatient visits, mental health services, substance abuse services, social services for elderly, dental care services. For each visit: (1) visited service, (2) date, (3) main diagnose and operation related to the visit, (4) medication data (ATC groups: M01, N05, N06), (5) laboratory results (HbA1c, glucose, hemoglobin, ferritin, vitamin D, PEth)
Social services decisions (Effica and Lifecare systems)	Information about social services decisions: rehabilitation, elderly housing service, caregiver support, homecare, transportation services For each decision: (1) service decision category, (2) decision outcome (positive/negative), (3) date
Service need and physical function assessment (Raisoft)	Information about service need and physical function assessments.

Table 2. Data resources covered by the data permit of the MAITE project.

4.2 Protecting privacy

ML based models typically require large data sets in terms of data subjects and variables. Extracting such large cohorts to be processed in external computing environments may involve high privacy risks. Consequently, register controllers have been reluctant to grant data permits to external research users, especially if data would need to be transferred across country borders.

Privacy risks can be reduced by limiting the data processing to a closed SPE with a remote desktop user interface for the researcher. Such approach is currently mandatory for register based research studies in Finland.

In the case of the MAITE project, we submitted the data permit application to the data controller (PHHYKY). The positive decision was received within two weeks. The data will be next transferred from the data controller to the SPE ("Kapseli") hosted by the Finnish Social and Health Data Permit Authority (Findata) [25]. Although the closed SPE limits the researcher's freedom in data processing, we consider the related benefits to be higher. Privacy protection in the MAITE project is of high priority as the targeted number of study participants is high (N=33 000) and a wide set of data for each individual will be used in the research and ML model development. We expect that our commitment of using the certified SPE had a positive impact on the data permit application process by convincing the register controller about sufficient privacy protection.

After the development phase, machine learning models may still be vulnerable to security threats compromising the privacy of the training data. Adversarial attacks may for instance attempt to identify and de-pseudonymize individuals included in training or reconstruct the training data [26]. Privacy concerns can be partly reduced by controlling access to the model parameters and output at deployment, but further defence mechanisms can also be employed when developing the model. Differential privacy mechanisms constitute the state-of-the-art and improves privacy by adding noise to the data or the algorithm itself, e.g., in the objective function or in the gradients at each training iteration [26, 27]. Such mechanisms will also be considered in the MAITE project. We will identify and compare suitable privacy-preserving methods to ensure secure future integration of the ML model in commercial software.

4.3 From research to medical software

Medical device software development based on ML models originating from research projects can be a challenge for traceability. Even if the ML model development is carried out in the closed SPE, the traceability requirements of MDR and AIA should be fulfilled. This means that data pipelines, processing algorithms, data sets (tuning and testing) and respective version information shall be carefully documented. This may be a challenge for an SPE, which has primarily been designed for research purposes. Additional challenges arise from the fact that data permit is normally granted for a fixed duration after which the data is no more available unless an extension is granted.

In the MAITE project we will develop a software demonstration (PoC) without any requirement to comply with MDR. However, preparing for potential MDSW development after the MAITE project, we shall follow a systematic process to carefully document the ML model development steps. This will be achieved by the setting up software and data version management tools in the SPE to ensure full traceability between the ML model and the MDSW.

4.4 Deployment in the clinical environment

Deployment of ML based applications in the operational clinical environment involves many challenges. Technical integration challenges may be caused by the diversity of healthcare information systems between different service providers. Such challenges, require investment of resources to multiple integrations, but can usually be overcome. The most critical issue seems to be low acceptance by the professional users: development of solutions for healthcare is in many cases technology-driven without sufficient contribution of end-users [28, 29].

The MAITE project addresses this problem by involving health and social services professionals during the full application development lifecycle. The project organizes several workshops during the research and model-development phase to understand user needs and the relevant personal health and social services usage data to be included as ML model variables.

Other potential challenges for ML application deployment are related to the GDPR and AIA regulation. The GDPR may limit the possibility of updating the application's ML model by directly using data from an EHR system. Even more critical an issue is the overall lawfulness of the application. For example, using applications for automatic profiling of individuals is not allowed by GDPR and AIA. Therefore, it is considered important to stress that ML based applications should only be used as decision support tools, leaving the final decision always to the end-user. The MAITE project addresses such problems by carrying out an in-depth investigation of the regulatory impacts and needed precautions to ensure that the application complies with applicable regulation.

5 DISCUSSION AND CONLUSIONS

ML models are increasingly used in healthcare applications. The life cycle of ML based applications differs from conventional MDSW products, such as EHR systems. Existing studies concerning the development process of ML based medical applications have been mainly focused to the challenges of software change management of continuously updated applications. Less attention has been given to the challenges related to the exploitation of large amounts of personal data in the application development. However, the related data protection requirements have a remarkable impact on the application life cycle.

In this paper, we have outlined three main phases of application development. Each phase is characterized by its specific relation with regulation. In the research phase, regulation (GDPR) especially concerns privacy protection, while in the software development phase the main objective of regulation (MDR) is to ensure safety and performance. In the application deployment phase, regulation is typically national and focused to ensure secure integration of the application to the operational service environment.

Using our ongoing MAITE project as an example, we have analysed challenges in ML application development and we have presented best practices to overcome them. In the research phase, we propose a certified SPE to be used for data processing. This approach minimizes privacy risks and helps to reassure the data controller of appropriate data usage. We also propose privacy-preserving methods, such as differential privacy, to be applied for protecting the ML model. In order to meet the traceability requirements of MDSW, we recommend systematic version control and data set management processes to be applied already in the early phase of ML model development taking place in a closed SPE environment. This approach will help the transfer of the ML model developed in the research phase into the software development phase. To overcome the deployment challenges, we propose early involvement of end-users already in the research phase as well as involvement of legal experts to ensure that the application being developed complies with regulation.

6 SUMMARY

This paper analyses the impact of regulation on the development of ML applications for healthcare. We especially focus on the challenges related to the use of sensitive personal data in the ML model development. We outline best practices for ensuring safe personal data processing and usage of the ML models as a basis for medical software development. We also highlight the importance for end-user involvement and legal evaluation at early development stage as a precondition for successful application deployment.

7 REFERENCES

[1] Muehlematter UJ, Daniore P, Vokinger KN. Approval of artificial intelligence and machine learning-based medical devices in the USA and Europe (2015–20): a comparative analysis. *Lancet Digit Health* 2021; 3: e195–e203.

[2] Subrahmanya VG, Shetty DK, Patil V., et al. The role of data science in healthcare advancements: applications, benefits, and future prospects. *Irish J Med Sci (1971 -);* 2021.

[3] WHO. Ethics and Governance of Artificial Intelligence for Health: WHO guidance. *World Health Organ* 2021: 1–148.

[4] Keutzer L, Simonsson USH. Medical Device Apps: An Introduction to Regulatory Affairs for Developers. *JMIR mHealth uHealth* 2020; 8.

[5] Kane DW, Hohman MM, Cerami EG, et al. Agile methods in biomedical software development: a multi-site experience report. *BMC Bioinformatics* 2006; 7.

[6] Granlund T, Stirbu · Vlad, Mikkonen · Tommi. Towards Regulatory-Compliant MLOps: Oravizio's Journey from a Machine Learning Experiment to a Deployed Certified Medical Product. *SN Comput Sci* 2021; 2: 1–14.

[7] Hsieh M-T, Huang K-C, Hsieh C-Y, et al. Validation of ICD-10-CM Diagnosis Codes for Identification of Patients with Acute Hemorrhagic Stroke in a National Health Insurance Claims Database. *Clin Epidemiol* 2021; 13: 43–51.

[8] Artificial Intelligence in Medical Device Legislation | Futurium, https://futurium.ec.europa.eu/en/european-ai-alliance/document/artificial-intelligence-medical-device-legislation (accessed 27 June 2022).

[9] Lähteenmäki J, Vuorinen A-L, Pajula J, et al. Integrating data from multiple Finnish biobanks and national health-care registers for retrospective studies: Practical experiences. *Scand J Public Health* 2021; 140349482110044.

[10] European Health Data Space | Public Health, https://ec.europa.eu/health/ehealth/dataspace_en (accessed 27 June 2022).

[11] Beskow LM, Dombeck CB, Thompson CP, et al. Informed consent for biobanking: consensus-based guidelines for adequate comprehension. *Genet Med* 2015; 17: 226–233.

[12] Oxley PR, Ruffing J, Campion TR, et al. Design and Implementation of a Secure Computing Environment for Analysis of Sensitive Data at an Academic Medical Center. *AMIA Annu Symp Proc* 2018: 857.

[13] Feng J, Emerson S, Simon N. Approval policies for modifications to machine learning-based software as a medical device: A study of bio-creep. *Biometrics* 2021; 77.

[14] Babic B, Gerke S, Evgeniou T, et al. Algorithms on regulatory lockdown in medicine. *Science* 2019; 366: 1202–1204.

[15] Minssen T, Gerke S, Aboy M, et al. Regulatory responses to medical machine learning. *J Law Biosci* 2020; 7: 1–18.

[16] Gilbert S, Fenech M, Hirsch M, et al. Algorithm Change Protocols in the Regulation of Adaptive Machine Learning–Based Medical Devices. *J Med Internet Res* 2021; 23.

[17] Artificial Intelligence Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (accessed 27 June 2022).

[18] Harp S, Carpenter T, Hatcliff J. A Reference Architecture for Secure Medical Devices. *Biomed Instrum Technol* 2018; 52: 357–365.

[19] Frenz C. OWASP Secure Medical Device Deployment Standard, https://owasp.org/www-pdf-archive/SecureMedicalDeviceDeployment.pdf (accessed 27 June 2022).

[20] Jormanainen V, Reponen J. CAF and CAMM analyses on the first 10 years of national Kanta services in Finland. *Finnish J eHealth eWelfare* 2020; 12: 302–315.

[21] Overview of the national laws on electronic health records in the EU Member States (2016), https://ec.europa.eu/health/other-pages/basic-page/overview-national-laws-electronic-health-records-eu-member-states-2016_en (accessed 27 June 2022).

[22] Leppla L, Hobelsberger S, Rockstein D, et al. Implementation Science Meets Software Development to Create eHealth Components for an Integrated Care Model for Allogeneic Stem Cell Transplantation Facilitated by eHealth: The SMILe Study as an Example. *J Nurs Scholarsh* 2021; 53: 35–45.

[23] Lysaght T, Lim HY, Xafis V, et al. AI-Assisted Decision-making in Healthcare. *Asian Bioeth Rev* 2019; 11: 299–314.

[24] Pritchard D, Petrilla A, Hallinan S, et al. What contributes most to high health care costs? Health care spending in high resource patients. *J Manag Care Spec Pharm* 2016; 22: 102–109.

[25] Kapseli remote access - Findata, https://findata.fi/en/kapseli/ (accessed 27 June 2022).

[26] Al-Rubaie M, Chang JM. Privacy-Preserving Machine Learning: Threats and Solutions. *IEEE Secur Priv* 2019; 17: 49–58.

[27] Bae H, Jang J, Jung D, et al. Security and Privacy Issues in Deep Learning. *SN Comput Sci* 2020; 1: 253.

[28] McIntosh C, Conroy L, Tjong MC, et al. Clinical integration of machine learning for curative-intent radiation treatment of patients with prostate cancer. *Nat Med* 2021; 27: 999–1005.

[29] El Naqa I. Prospective clinical deployment of machine learning in radiation oncology. *Nat Rev Clin Oncol* 2021; 18: 605–606.

8 ACKNOWLEDGEMENT

The paper originates from research work carried out in AHMED project (Agile and holistic medical software development) and MAITE project (Data-driven identification of elderly individuals with future need for multi-sectoral services). The authors want to thank Business Finland, Ministry of social affairs and health and VTT Technical Research Centre of Finland for their financial contributions in the projects and the support of Päijät-Häme Joint Authority for Health and Wellbeing in defining the research plan and data contents in the MAITE use case.