# Challenges for AI in Healthcare Systems*

Markus Bertl[1], Yngve Lamo[2] Martin Leucker[3], Tiziana Margaria[4], Esfandiar Mohammadi[5], Suresh Kumar Mukhiya[6], Ludwig Pechmann[3], Gunnar Piho[1], and Fazle Rabbi[7]

[1] School of Information Technology, Tallinn University of Technology, 12616, Estonia
{markus.bertl, gunnar.piho}@taltech.ee
[2] Department of Computer science, Electrical engineering and Mathematical sciences, Western Norway University of Applied Sciences, Norway
{yngve.lamo}@hvl.no
[3] Institute for Software Engineering and Programming Languages, University of Lübeck, Lübeck, Germany
{leucker,lpechmann}@isp.uni-luebeck.de
[4] Department of Computer Science and Information Systems, University of Limerick, Ireland
tiziana.margaria@ul.ie
[5] Institute for IT Security, University of Lübeck, Lübeck, Germany
esfandiar.mohammadi@uni-luebeck.de
[6] Tryg, Norway
{suresh.mukhiya}@tryg.no
[7] Information Science and Media Studies, University of Bergen, Norway
{fazle.rabbi}@uib.no

**Abstract.** This paper overviews the challenges of using artificial intelligence (AI) methods when building healthcare systems, as discussed at the AIsola Conference in 2023. It focuses on the topics (i) medical data, (ii) decision support, (iii) software engineering for AI-based health systems, (iv) regulatory affairs as well as (v) privacy-preserving machine learning and highlights the importance and challenges involved when utilizing AI in healthcare systems.

**Keywords:** healthcare · artificial intelligence · medical systems

## 1 Introduction

Artificial intelligence has gained a lot of attention in previous years in various domains like finance [52], education [31], human resources [112], healthcare [93], etc. To a large part, this is due to the advances in machine learning, especially in deep learning. Moreover, the success of large language models also empowers new applications in various areas. In addition, the advances in huge dedicated high-performance computers with enormous GPU power drive this

* This work was partially supported by the BMBF project AnoMed 16KISA050K and 16KISA056.

field of computer science. While decades ago it was more the symbolic approaches in artificial intelligence that were the driving force, it is now the sub-symbolic approaches [38]. However, it may be expected that the combination of both approaches yields solutions having the benefits of both techniques [14].

Healthcare is of great importance to society. It is also economically significant and may become even more influential in the future due to an aging society [58]. Therefore, as expected, artificial intelligence techniques are finding their way into the health domain. Healthcare affects humans' lives and is a prime example of a safety-critical domain [8,129,117]. Therefore, there are several challenges when applying artificial intelligence to medical applications, ranging from medical care and medicines to medical devices [116].

This paper gives a short overview of the discussions and contributions presented and partially reflected in the subsequent chapters of the healthcare track volume of the AIsola Conference 2023. The track consisted of six invited presentations analyzing several challenges when applying artificial intelligence techniques to healthcare applications. We summarize these presentations in the subsequent sections and refer the reader to dedicated papers in this volume or published elsewhere. In the track, we discussed the following challenges:

- medical data,
- decision support,
- software engineering in the healthcare domain,
- regulations when building medical devices and
- privacy in machine learning.

It should be stressed that the papers contained in this volume are interim discussions of ongoing studies and not final results.

This paper is structured as follows: in the next section, we discuss the role of health data in the medical domain, focusing on machine learning applications. Section 3 gives a quick summary of challenges when building medical decision support systems. Software engineering challenges for building medical devices are sketched in Section 4. Regulatory requirements for building machine learning applications for the health domain are explained in Section 5. Section 6 recalls the privacy challenges in machine learning. Conclusions are drawn in Section 7.

## 2 Data Handling

A vast amount of data is generated in the healthcare domain regularly, and it consists of diverse information such as admission records, medical histories, diagnosis reports, laboratory test results, and treatment procedures from various departments and clinics. AI has the potential to analyze this extensive dataset and extract insightful information, such as comorbidity patterns, trends, and correlations, which may play an important role in improving the service quality of healthcare systems. Identifying recurring patterns within healthcare processes is crucial for streamlining healthcare procedures and ultimately improving patient outcomes. AI provides an opportunity to reduce the cost of healthcare by optimizing processes and maximizing resource utilization, as well as providing better service quality by offering personalized treatments. Effective implementation of AI in healthcare relies on various factors, including data quality and availability; data interpretability and explainability; ethical considerations and bias; AI model complexity and selection; scalability and performance; data privacy and security; integration with existing systems; user acceptance and adoption; and regulatory compliance. In the following subsections, we present various types of healthcare data, their characteristics, and various challenges in healthcare data collection, management, analysis, and reporting.

### 2.1 Types of Healthcare Data

Healthcare data comes in various types and possess distinct characteristics. The following are different types of healthcare data that possess distinct significance for AI.

- Electronic Healthcare Records (EHRs)
- Clinical data
- Administrative data
- Genomics Data, e.g. DNA
- Patient-reported data, e.g., biological markers
- Health Behavior Data, e.g., diet, exercise, substance use
- Public Health Surveillance Data
- Research Data encompasses data
- Imaging and Diagnostic Data, e.g., X-rays, MRIs, CT scans
- Social Determinants of Health (SDOH), data encompasses factors outside the healthcare system that influence health outcomes, such as socioeconomic status, education, and environmental conditions

### 2.2 Characteristics of Healthcare Data

Healthcare data has several characteristics that distinguish it from data in other domains.

- *Complexity:* Healthcare data involves a wide range of information related to patient health, medical treatments, and administrative processes.
- *Variability:* Healthcare data exhibits variability in formats, structures, and types. It includes structured data (e.g., databases), various kinds of images, and unstructured data (e.g., free-text clinical notes).
- *Volume:* Healthcare data are often voluminous, with large datasets generated from various sources, such as diagnostic tests, medical imaging, and continuous monitoring.
- *Velocity:* Healthcare data is generated and updated in real-time. Continuous monitoring, streaming data, and rapid updates contribute to high-velocity data.

– *Variety:* Healthcare data comes in diverse formats, including text, numerical values, images, and signals. Integrating and analyzing these varied data types is a challenge.
– *Veracity:* The accuracy and trustworthiness of healthcare data can vary.
– *Privacy and Security:* Healthcare data is sensitive and subject to strict privacy regulations. Protecting patient confidentiality and ensuring data security are paramount.
– *Longitudinal:* Healthcare data often span long periods, providing a longitudinal view of a patient's health history. This historical context is crucial for comprehensive patient care.
– *Inter-connectedness:* Different healthcare data elements are interconnected. Patient records, diagnoses, medications, and treatments are linked to provide a holistic view of care.
– *Context Dependency:* Healthcare data requires contextual understanding. Clinical data interpretation often depends on the medical context and the patient's history.
– *Regulatory Compliance:* Healthcare data should comply with regulatory frameworks to protect patient rights and privacy, such as compliance with HIPAA, GDPR, and other data protection laws.
– *Multidimensional:* Healthcare data are often multidimensional, involving data from various sources and aspects of patient care, including clinical, financial, and operational dimensions.

### 2.3 Challenges of Healthcare Data

Addressing the challenges of healthcare data is pivotal for advancing the quality and effectiveness of healthcare services. Several vital challenges emerge as we delve into the intricacies of managing healthcare data. Figure 1 outlines different healthcare data collection, management, analysis, and reporting challenges.

*Interoperability:* There is a need for standardized interoperability to ensure the seamless exchange of healthcare data between different systems and providers. Common data standards and interoperability frameworks are necessary to facilitate better care coordination and enhance data sharing for research purposes. Even though there exist several healthcare ontologies, e.g., ICD-10 [84] and SNOMED-CT [30], the healthcare dataset often consists of unstructured data. Image processing and Natural Language Processing (NLP) may play an important role in extracting structured information from unstructured information. However, there are still many challenges as the state-of-the-art technique for image processing, and NLP could provide inaccurate results.

*Data Quality and Accuracy:* Maintaining data quality and accuracy is challenging due to errors in data entry, variations in documentation practices, and evolving standards. Implementing data validation processes and quality assurance measures are essential to ensure the reliability of healthcare data. Adopting cutting-edge techniques such as machine learning algorithms for anomaly detection [120,57], natural language processing for semantic validation

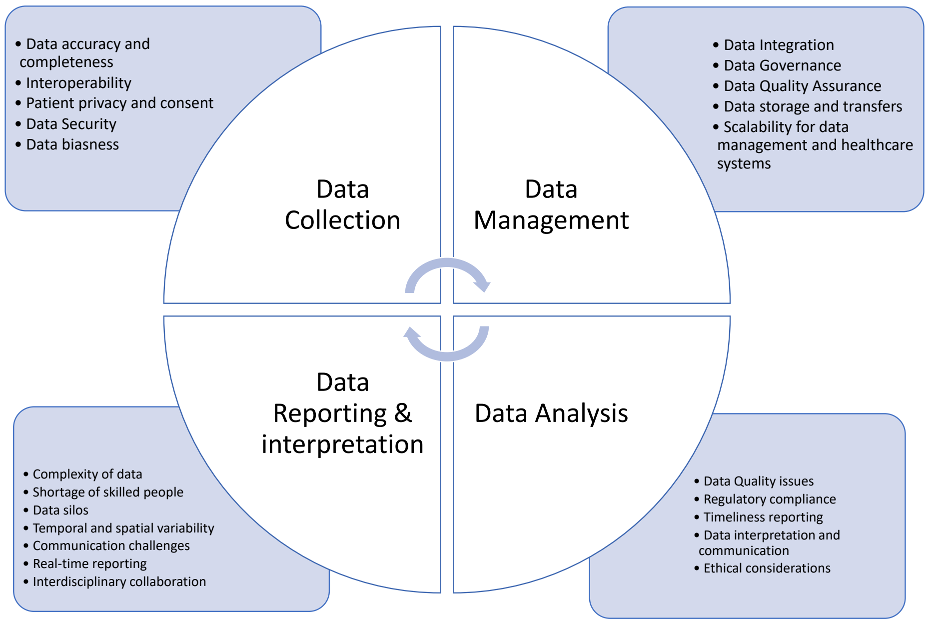


**Fig. 1.** Challenges in healthcare data collection, management, analysis and reporting

[64,100], and blockchain technology for immutable data records [106,104] can strengthen data validation processes and quality assurance measures, thereby enhancing the reliability and integrity of healthcare data.

*Bias and Fairness:* Ethical and responsible AI practices are paramount when implementing AI methods in the healthcare domain. Quality of data is essential for the application of AI. Bias in data poses a significant risk to the development of responsible AI. Systems trained on biased data may produce inaccurate and harmful predictions. This bias is particularly concerning when it affects individuals from specific demographic groups. Advanced methodologies such as adversarial de-biasing [127,128], fairness-aware learning [68,126], and counterfactual fairness [124,131] are pivotal for promoting fairness and mitigating bias in AI healthcare applications.

In this volume, the contribution *Towards a Multi-dimensional Health Data Analysis Framework* by Rabbi et al. [92] studies a framework for analyzing health data.

## 3 Tests vs. learning from massive data sets

The dichotomy between traditional testing methods and learning from massive data sets through Artificial Intelligence (AI) presents a compelling discourse in healthcare. Traditional testing methods in healthcare often suffer from limitations such as time inefficiency, capacity, human resources, and practicality.

In healthcare, traditional testing refers to the conventional medical testing methods that have been used for years. These methods typically involve a multi-step process that includes collecting samples from the patient at the bedside or the clinic, transporting the samples to a centralized laboratory (often located far away), and then subjecting them to several processing steps. Examples of traditional tests include blood tests, urine tests, and tissue biopsies, among others. These tests are usually performed in a laboratory by trained professionals, and the results are returned to the healthcare provider. This process can take some time, which can delay treatment [51,66].

In contrast, point-of-care testing is a more modern approach where tests are conducted close to the site of patient care, providing a rapid turnaround of test results. This can lead to improved clinical or economic outcomes compared to traditional laboratory testing [51,66]. Examples of point-of-care tests include blood glucose monitoring and home pregnancy tests [82]. Traditional testing and point-of-care testing play crucial roles in healthcare, each with its own strengths and limitations [51]. However, advances in ICT can also add to and enhance current medical testing processes.

With its capacity to learn from massive data, AI offers unprecedented opportunities for predictive analytics, pattern recognition, and decision-making support. Rule-based AI algorithms [28], machine learning [25], and deep learning algorithms [20] have been applied to healthcare with good results in terms of algorithmic accuracy, often even outperforming humans in diagnosing illnesses or predicting outcomes of treatment trajectories. However, the rise of AI in medicine also brings challenges regarding data privacy, algorithmic transparency, and validation of AI models. With increasing use, AI systems in healthcare are also increasingly targeted by cyber attacks [18]. Therefore, an optimal approach may lie in integrating both methodologies, leveraging the robustness of traditional tests and the innovative potential of AI to drive a new era of precision medicine and personalized healthcare. This approach necessitates rigorous regulatory frameworks to ensure the ethical and responsible use of data and continuous evaluation to maintain the accuracy and reliability of AI systems. Thus, the interplay between tests and learning from massive data through AI is not a competition but rather a symbiotic relationship that could redefine the future of healthcare.

Besides its potential, AI in healthcare still suffers from low adoption rates [27]. Even large tech companies like IBM with Watson for Healthcare failed to deliver on the promise of revolutionizing healthcare with AI [110]. The reasons for that were a missing interdisciplinary approach between IT researchers and healthcare professionals [22] and the complexity, quality, and large quantity of data needed for training algorithms [21]. Those factors could have also led to a bias in the good research results of machine and deep learning algorithms, especially because most published deep learning research in healthcare is only based on small datasets [23,26,21].

In conclusion, the healthcare industry stands at a crossroad between traditional testing methods and the innovative potential of AI. The integration of AI into healthcare represents a transformative shift from traditional methodologies. While traditional testing has been the backbone of medical diagnostics for decades, it is encumbered by efficiency, capacity, and resource allocation constraints. Point-of-care testing has emerged as a viable alternative, offering rapid results and the potential for better clinical outcomes. However, the true paradigm shift lies in the application of AI, which provides a level of predictive analytics, pattern recognition, and decision-making support previously unattainable through its ability to analyze vast data sets. This fusion of AI with traditional and point-of-care testing methods does not diminish the value of either; instead, it augments the healthcare ecosystem, creating a more robust, responsive, and efficient framework for patient care. We see the future of healthcare testing as one that harmonizes the reliability of traditional methods with the agility of point-of-care solutions and the innovative prowess of AI, paving the way for a more proactive and patient-centric approach to medical diagnostics. Despite this potential, the reliance on small data sets in AI research poses a risk of bias, and the lack of robust Randomized Controlled Trials (RCTs) to validate AI's efficacy is a significant gap in the literature. Moving forward, the healthcare sector must embrace a balanced approach that leverages the strengths of traditional and AI-driven testing methods while also addressing the challenges of data representativeness and empirical validation challenges. Only through such a comprehensive strategy can we ensure the delivery of efficient, accurate, and equitable healthcare services.

Note that this section presents a summary of research on Systematic AI Support described in detail in [19]. In this volume, the contribution *Future Opportunities for Systematic AI Support in Healthcare* by Bertl et al. [24] studies further opportunities for using AI in healthcare.

## 4 Software Engineering for Developing AI-intensive Healthcare Systems: Opportunities and Challenges

Integrating Artificial Intelligence (AI) in healthcare systems is related to the expectation to transform medicine [72], including economic and viability considerations of Disruption, Discontinuity and Differentiation (3-D-Model) [96]. It offers unprecedented opportunities to enhance patient care outcomes [50,121] by fostering personalized care that leads to continuity of care [39] and active and healthy longevity. These opportunities can be summarized as follows:

- *Personalized Medicine:* AI's capability to analyze vast datasets enables the development of personalized treatment plans [50]. By considering an individual's genetic predisposition, lifestyle, and environmental factors [111], AI may help physicians predict the most effective evidence-based treatments, hopefully reducing medication errors and therapy selections [4].
- *Predictive Analytics:* AI algorithms can identify patterns and predict outbreaks of diseases [113], helping public health officers plan proactive

healthcare measures [122]. For example, machine learning models can forecast the spread of infectious diseases by analyzing data from various sources, including social media, citizens' mobility patterns, and climate changes, probably enabling more timely interventions [56].
- *Enhanced Diagnostic Accuracy:* AI has demonstrated superior performance in diagnosing diseases using medical image processing [69]. Deep learning models, trained on thousands of images, may help medical specialists detect anomalies such as tumors [36] and fractures [123], often with higher accuracy and speed than human experts alone can do, leading to earlier treatment and better outcomes [63,5].
- *Operational Efficiency:* AI may help physicians streamline healthcare operations, reducing the burden on healthcare professionals and improving patient care [130]. From scheduling appointments to managing patient flow and automating administrative tasks, AI can significantly enhance efficiency in healthcare settings [80].
- *Bridging the Accessibility Gap:* AI-powered telemedicine and mobile health applications can deliver healthcare services to remote and underserved populations [29]. By reducing geographical barriers, AI has the potential to democratize access to healthcare services, making it possible for more individuals to receive timely and appropriate care [85].

### 4.1 Challenges

However, robust, efficient, and ethical AI-intensive healthcare systems bring with them and amplify complex challenges for software engineers who engineer such systems [44]. We summarize these challenges as follows:

- *Data Privacy and Security:* The backbone of AI in healthcare is data, which often includes sensitive personal information [125]. Ensuring the privacy and security of this data is paramount, requiring robust encryption methods, secure data-sharing protocols, and compliance with regulations [37] such as HIPAA (Health Insurance Portability and Accountability Act) in the United States and GDPR in the EU.
- *Bias and Ethical Concerns:* AI systems are only as unbiased as the data they are trained on [83]. If the training data is skewed, the AI's decisions may be as well, potentially leading to unequal treatment outcomes among different demographic groups [102]. Addressing these biases and ensuring ethical considerations are integrated into AI systems is a complex challenge [71].
- *Interoperability:* Healthcare data is fragmented across various systems and formats, making it difficult to aggregate and analyze comprehensively [67]. Software engineers must tackle the interoperability challenge to enable seamless data exchange and semantic integration [46,10,43], ensuring AI systems can leverage diverse data sources for comprehensive analysis [105]. A further complexity dimension is that data is often processed while the representation format remains the same (e.g. TIFF files). So semantics has also the role of a refinement of the concept of type, captured for example

through semantic data types in [65] and [35]. Also this needs to be included in the scope of AI tools.
- *Regulatory Compliance:* Navigating the regulatory landscape in the medical domain is challenging [103]. AI-based healthcare systems must comply with many regulations governing medical devices and patient data [88,47,15]. Ensuring these systems are effective and legally compliant requires a deep understanding of both technological and regulatory domains.
- *Trust and Adoption:* Building trust among healthcare professionals and patients is crucial for adopting AI-based systems [42,12]. This involves demonstrating AI interventions' reliability, safety, and efficacy [98,70]. Software engineers must work closely with healthcare professionals to design systems that complement clinical workflows, enhancing rather than replacing human judgment [55].

Therefore, integrating AI into healthcare systems offers a promising avenue for enhancing healthcare delivery, making personalized medicine a reality, and improving access to care. However, the journey is fraught with challenges ranging from data privacy and bias to regulatory hurdles and the need for interoperability.

### 4.2 Opportunities

As software engineering continues to evolve in response to these challenges, the collaboration between software engineers, healthcare professionals, and policymakers will be critical [9]. By navigating these complexities, we can harness the full potential of AI in healthcare, ensuring that it serves as a tool for equitable, efficient, and effective patient care. Therefore, we summarize the following possible opportunities in software engineering for developing AI-intensive healthcare systems:

- *Advanced Tool Development:* There's a growing demand for sophisticated tools to manage and analyze health data at scale [17,115] as well as recommender systems to manage imbalance [107]. Software engineers have the opportunity to develop and refine platforms that facilitate the training of AI models on vast datasets, including electronic health records, imaging data [32], diagnostics [101], health information [34] and genomics [41]. These tools must be powerful in terms of computational capabilities and user-friendly for healthcare professionals.
- *Interoperability Solutions:* One of the significant opportunities lies in creating solutions that ensure seamless semantic interoperability among diverse healthcare systems [90,108,94], including considerations of simplicity [95] in times of disruption. By engineering advanced APIs and data exchange protocols, software engineers can enable different systems to communicate effectively, enhancing data sharing and collaboration across the healthcare sector. This impacts also the availability and interoperability of data for long-lived interdisciplinary research [74].

– *Data Privacy and Security Innovations:* With the sensitivity of healthcare data, there's an urgent need for innovative solutions that protect patient information as data breaches [7,81] harm the trust and privacy. Architectural solutions that enforce privacy [6] and blockchain-based privacy enhancing technologies have been proposed [54]. Software engineers are at the forefront of designing encryption methods, secure data storage solutions [60,61,62], and privacy-preserving algorithms, ensuring that AI-based systems adhere to strict data protection standards.
– *Scalable Infrastructure:* Developing AI models requires significant computational resources. There is a tremendous opportunity for software engineers to build scalable infrastructures [53,13] that can support the development and deployment of AI models, making advanced healthcare analytics accessible to institutions of all sizes.

### 4.3 AI-Intensive Healthcare Systems

However, those opportunities for software engineers are in harmony with the complex challenges that software engineers face in developing software and systems for AI-intensive healthcare systems. We summarize some of these challenges as follows:

– *Managing Complex Data:* Healthcare data is notoriously complex, heterogeneous, and voluminous [2,3,114,67]. Software engineers face the challenge of creating systems capable of handling this complexity, including different data formats, incomplete datasets, and the integration of real-time data streams, all while maintaining high performance. An example is in [33], where the sheer size of TIFF files for highly-plexed tissue image analysis required an extension to the underlying platform.
– *Ensuring Model Explainability:* AI models, especially deep learning, are often seen as "black boxes" due to their complex nature [11]. Developing methodologies and tools that enhance the transparency and explainability of these models is a significant challenge but essential for gaining trust among healthcare providers and patients [97]. Alternatively, one can use different ML techniques, where explainability can be supported by formal methods [48,49].
– *Addressing Bias and Fairness:* Data bias is a critical issue that can lead to skewed AI predictions [118]. Software engineers must devise strategies for identifying and mitigating bias in training datasets and algorithms, ensuring that AI-intensive healthcare solutions are fair and equitable [12,42,97].
– *Navigating Regulatory Landscapes:* The healthcare industry is heavily regulated, and AI-intensive systems must comply with many regulations and standards [47,103]. Software engineers must stay abreast of these evolving requirements, integrating compliance into the software engineering life-cycle, which can be complex and time-consuming.
– *Integration with Existing Healthcare IT Ecosystems:* Integrating AI solutions into existing IT infrastructures without disrupting clinical workflows

represents a significant challenge [40]. Software engineers must design AI systems that are not only interoperable [99,91] but also align with the needs and processes of healthcare professionals, ensuring smooth deployment, adoption, and effective use.

Integrating AI into healthcare systems offers software engineers an opportunity-rich ground for innovation, with substantial opportunities to impact patient care positively. The combination with model driven development of software systems, including the current push towards Low-Code/No-Code can be a help. Here, approaches based on eXtreme Model Driven Development (XMDD) [78,79], based on a Digital Thread approach [76,73] and enriched by formal methods [75,77] have proven useful in many areas including cyberphysical systems, which has direct application to medical devices and Health IoT. However, the path is full of complex technical, ethical, and regulatory challenges that require thoughtful navigation. By addressing these challenges head-on and leveraging the opportunities, software engineers can play a pivotal role in shaping the future of healthcare, making it more accurate, efficient, and accessible for all by supporting transformation in medicine for enhanced patient care outcomes and personalized and continuity of care towards the active and healthy longevity of citizens.

In this volume, the contribution *Model Driven Development for AI-based Healthcare Systems: A Review* by Colm Brandon, Amandeep Singh and Tiziana Margaria [35] reviews four case studies that illustrate different quadrants in the bidimensional space of AI/ML and advanced model driven development, specifically in a low-code/no code fashion.

## 5 Regulatory Affairs

Manufacturers of Medical Devices (MD) and Software as a Medical Device (SaMD) encounter a variety of challenges when aligning with regulatory standards, both in the US under FDA regulations and in the EU under the Medical Device Regulation (MDR) [59]. These challenges are compounded by technology's dynamic and evolving nature, particularly in AI and machine learning. The US Food and Drug Administration (FDA) has a comprehensive set of regulations and guidelines for medical devices, which include detailed requirements for the safety, efficacy, and quality of these products. These regulations ensure that medical devices are safe for patients and effective in their intended use. The FDA's approach to regulation is comprehensive, covering every stage of a medical device's life cycle, from design and development to post-market surveillance. The Medical Device Regulation (MDR) plays a similar role in the European Union. The MDR sets stringent standards for medical devices, focusing on safety and performance. It emphasizes the importance of clinical evaluation and post-market surveillance, ensuring that medical devices meet high standards throughout their life cycle. Both sets of regulations demand rigorous risk management like ISO 14971, testing and validation processes, extensive documentation, and adherence to quality management systems, especially one compliant with standards like ISO 13485 [86]. The complexities in these regulatory landscapes arise from the need to balance technological innovation with patient safety and product efficacy.

The task is further complicated by the evolving nature of Artificial Intelligence (AI) and Machine Learning (ML) in medical devices, which challenges traditional models of software change management and regulatory compliance [89]. We highlight how the adaptive capabilities of ML tasks challenge traditional software change management. Unlike conventional software, ML systems, especially those engaged in continual learning, where an ML can autonomously evolve their algorithms based on new data, blurring the lines of standard change control practices. This autonomous evolution poses unique regulatory challenges, as it may not fit within established frameworks that expect static, well-tested software versions before market release. Understanding and navigating these nuances is crucial for regulatory compliance in the ML-driven landscape of medical technology.

One approach to support evolving software for medical devices is to anticipate or predetermine the system's evolution and to foresee to which extent these changes do not affect the safety of the medical device. The FDA introduced a so-called Predetermined Change Control Plan (PCCP) [119], in which anticipated changes are described and evaluated according to their impact on the medical device. If the impact is moderate, the FDA may approve such evolving systems. However, the systematic identification of potential changes in the software and their criticality assessment is difficult. To support this complex task of identifying and documenting the development and potential changes, we introduce the CRISP-PCCP as a methodology for developing AI/ML-enabled medical devices in the context of FDA approval. CRISP-PCCP facilitates the identification of potential changes in AI/ML processes and ensures that these changes are compliant and safe. It aims to streamline the development process, focusing on quality assurance and effective project management in the complex area of medical device regulations. This makes it an important tool for manufacturers seeking FDA approval for AI/ML-enabled medical devices.

In this volume, the contribution *CRISP-PCCP – A Development Methodology Supporting FDA Approval for Machine Learning Enabled Medical Devices* by Pechmann et al. [87] explains the CRISP-PCCP approach in detail.

## 6 Privacy-challenges in Machine Learning

Learning predictive machine learning (ML) models from patient data and similar medical applications requires a particularly careful treatment of the patient data. Recent work in ML security has illustrated that using classical learning methods can lead to models that leak information about the training data, i.e., the patient data [45]. A classical countermeasure against data leakage has been to sanitize the patient data before using it, e.g., via methods that achieve k-anonymity.

Yet, data sanitization has been shown to be ineffective against deanonymization attacks [109].

Consequently, modern methods for protecting yet learning from patient data rely on data aggregation, which is what many machine learning methods are based on [1]. By solely using the patient data in aggregated statistics (e.g., the mean of gradients), the impact of single data points is limited. Furthermore, adding random noise to these statistics can prevent partial deidentification attacks. The state-of-the-art definition used to prove that no deanonymization attack is possible against a given data processing algorithm is differential privacy.

Differentially private ML algorithms aim to protect single data points yet try to preserve an acceptable degree of usefulness, e.g., classification accuracy. For many differentially private ML algorithms, the degree of usefulness increases with increasing data points, which in medical applications translates to patients in a study. The same studies can be conducted at several medical institutions to maximize the number of patients in a study. To ensure that no party has to collect all patient data centrally, so-called secure distributed learning algorithms have been developed.

Secure distributed learning algorithms [16] ensure that no party leaks their locally collected data while each party can contribute their data to a joint learning protocol. Secure distributed learning algorithms aim to achieve performance similar to classical learning algorithms, where the data is centrally collected. Secure differentially private distributed learning algorithms additionally ensure that the result of the learning, the resulting ML model, does not leak information about the training data, i.e., the patient data.

## 7 Conclusion

In AI's integration into healthcare, a domain that directly impacts human well-being and is a complex, data-rich environment, we face many opportunities and challenges that probably impact the medical informatics future. This paper summarizes contributions and discussions at the AIsola Conference 2023. It explains opportunities where software engineering not only profits from the advancement of healthcare through AI but also faces complex challenges inherent in such a critical domain.

The promise of AI in healthcare is enormous, offering to revolutionize patient care through personalized medicine, predictive analytics, and enhanced diagnostic accuracy. The potential to streamline operational efficiencies, bridge accessibility gaps, and ultimately improve patient care outcomes and quality of life underscores a future where healthcare is accessible, effective, and more evidence-based. Software engineers find themselves at the heart of translating this potential into reality, developing the tools, systems, and algorithms that empower AI-intensive healthcare.

Yet, the path to realizing this potential has diverse and significant challenges. Data privacy and security are paramount concerns, reflecting the sensitive nature of healthcare information and the imperative to protect patient confidentiality in an increasingly digital world. AI systems' possible bias and ethical considerations further complicate the landscape, raising questions about equity and fairness in healthcare outcomes. Interoperability, regulatory compliance, and integrating AI systems into existing healthcare infrastructures present complex technical and bureaucratic issues that require understanding and innovative solutions.

In addressing these challenges, software engineering is not just a technical endeavor but a multidisciplinary one, demanding a synthesis of healthcare, ethics, law, and beyond expertise. It requires a balance between innovation and caution, pushing the boundaries of what is possible with AI while ensuring the developed systems' safety, reliability, and fairness. The collaborative effort between software engineers, healthcare professionals, policymakers, and patients is crucial in facing the medical informatics domain's ethical, legal, and technical complexities.

The opportunities for software engineering in developing AI-intensive healthcare systems are vast, ranging from advanced tool development and interoperability solutions to innovations in data privacy and scalable infrastructure. Each opportunity enhances healthcare systems' capabilities and opens new avenues for research, development, and application in an ever-evolving field. The challenges prompt reevaluating traditional approaches and encourage a critically creative forward-thinking mindset.

As we look to the future, the convergence of AI and healthcare mediated through software engineering will probably lead to a transformative change in medicine. Yet, this convergence also requires a thoughtful approach considering healthcare's ethical, social, and technical facets. By embracing the opportunities and addressing the challenges, software engineering stands to play a pivotal role in shaping a future where AI not only enhances healthcare but does so in a manner that is equitable, secure, and deeply attuned to the democratic values of society. In this endeavor, the lessons learned and the strategies developed will benefit healthcare and offer valuable insights for applying AI across other domains, reflecting the broader implications of this work for society at large.

## References

1. Abadi, M., Chu, A., Goodfellow, I., McMahan, H.B., Mironov, I., Talwar, K., Zhang, L.: Deep Learning with Differential Privacy. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 308–318. Association for Computing Machinery (2016)
2. Abdalla, H., Artoli, A.M.: Towards an efficient data fragmentation, allocation, and clustering approach in a distributed environment. Information **10**(3), 112 (2019)
3. Agrawal, R., Prabakaran, S.: Big data in digital healthcare: lessons learnt and recommendations for general practice. Heredity **124**(4), 525–534 (2020)
4. Ahmed, Z., Mohamed, K., Zeeshan, S., Dong, X.: Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. Database **2020**, baaa010 (2020)

5. Ahmed, Z., Mohamed, K., Zeeshan, S., Dong, X.: Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. Database **2020**, baaa010 (2020)
6. Alamri, B., Javed, I.T., Margaria, T.: A gdpr-compliant framework for iot-based personal health records using blockchain. In: 2021 11th IFIP international conference on new technologies, mobility and security (NTMS). pp. 1–5. IEEE (2021)
7. Alder, S.: Largest healthcare data breaches of 2021. The HIPAA Journal (2021), accessed: 2022-10-09
8. Ali, N., Punnekkat, S., Rauf, A.: Modeling and safety analysis for collaborative safety-critical systems using hierarchical colored petri nets. Journal of Systems and Software **210**, 111958 (2024)
9. Amann, J., Blasimme, A., Vayena, E., Frey, D., Madai, V.I., Consortium, P.: Explainability for artificial intelligence in healthcare: a multidisciplinary perspective. BMC Medical Informatics and Decision Making **20**, 1–9 (2020)
10. Amar, F., April, A., Abran, A.: Electronic health record and semantic issues using fast healthcare interoperability resources: Systematic mapping review. Journal of medical Internet research **26**, e45209 (2024)
11. Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., et al.: Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai. Information Fusion **58**, 82–115 (2020)
12. Asan, O., Bayrak, A.E., Choudhury, A.: Artificial intelligence and human trust in healthcare: focus on clinicians. Journal of Medical Internet Research **22**(6), 7 (2020)
13. Asch, M., Moore, T., Badia, R., Beck, M., Beckman, P., Bidot, T., Bodin, F., et al.: Big data and extreme-scale computing: Pathways to convergence-toward a shaping strategy for a future software and data ecosystem for scientific inquiry. The International Journal of High Performance Computing Applications **32**(4), 435–479 (2018)
14. Azevedo, B.F., Rocha, A.M.A., Pereira, A.I.: Hybrid approaches to optimization and machine learning methods: a systematic literature review. Machine Learning pp. 1–43 (2024)
15. Beckers, R., Kwade, Z., Zanca, F.: The eu medical device regulation: Implications for artificial intelligence-based medical device software in medical physics. Physica Medica **83**, 1–8 (2021)
16. Bell, J.H., Bonawitz, K.A., Gascón, A., Lepoint, T., Raykova, M.: Secure single-server aggregation with (poly) logarithmic overhead. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. pp. 1253–1269 (2020)
17. Belle, A., Thiagarajan, R., Soroushmehr, S.M., Navidi, F., Beard, D.A., Najarian, K.: Big data analytics in healthcare. BioMed Research International (2015)
18. Bertl, M.: News Analysis for the Detection of Cyber Security Issues in Digital Healthcare: A Text Mining Approach to Uncover Actors, Attack Methods and Technologies for Cyber Defense. Young Information Scientist **4**, 1–15 (2019)
19. Bertl, M.: Systematic AI Support for Psychiatry: A Framework on How to Implement Decision Support Systems. Phd thesis, Tallinn University of Technology, Tallinn, Estonia (November 2023), available at https://digikogu.taltech.ee/en/Item/a77022c7-b2af-46f9-ae83-62fe04f9bc72

20. Bertl, M., Bignoumba, N., Ross, P., Yahia, S.B., Draheim, D.: Evaluation of Deep Learning-based Depression Detection using Medical Claims Data. Artificial Intelligence in Medicine (2023)
21. Bertl, M., Kankainen, K.J.I., Piho, G., Draheim, D., Ross, P.: Evaluation of Data Quality in the Estonia National Health Information System for Digital Decision Support. In: Proceedings of the 3rd International Health Data Workshop. CEUR-WS (2023)
22. Bertl, M., Klementi, T., Piho, G., Ross, P., Draheim, D.: How domain engineering can help to raise adoption rates of artificial intelligence in healthcare. In: International Conference on Information Integration and Web Intelligence. pp. 3–12. Springer (2023)
23. Bertl, M., Metsallik, J., Ross, P.: A Systematic Literature Review of AI-based Digital Decision Support Systems for post-traumatic Stress Disorder. Frontiers in Psychiatry **13** (2022). https://doi.org/10.3389/fpsyt.2022.923613, https://www.frontiersin.org/articles/10.3389/fpsyt.2022.923613
24. Bertl, M., Piho, G., Draheim, D., Ross, P., Pechmann, L., Bucciarelli, N., Sharma, R.: Future opportunities for systematic ai support in healthcare. In: Steffen, B. (ed.) Bridging the Gap Between AI and Reality - First International Conference, AISoLA 2023, Crete, Greece, October 23-28, 2023, Post-Proceedings (2024), this volume
25. Bertl, M., Ross, P., Draheim, D.: Predicting Psychiatric Diseases Using AutoAI: A Performance Analysis Based on Health Insurance Billing Data. In: Database and Expert Systems Applications. pp. 104–111. Springer International Publishing (2021)
26. Bertl, M., Ross, P., Draheim, D.: A Survey on AI and Decision Support Systems in Psychiatry – Uncovering a Dilemma. Expert Systems with Applications **202**, 117464 (2022). https://doi.org/https://doi.org/10.1016/j.eswa.2022.117464, https://www.sciencedirect.com/science/article/pii/S0957417422007965
27. Bertl, M., Ross, P., Draheim, D.: Systematic AI Support for Decision Making in the Healthcare Sector: Obstacles and Success Factors. Health Policy and Technology (2023)
28. Bertl, M., Shahin, M., Ross, P., Draheim, D.: Finding Indicator Diseases of Psychiatric Disorders in BigData Using Clustered Association Rule Mining. In: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. pp. 826–833. SAC '23, Association for Computing Machinery (2023). https://doi.org/10.1145/3555776.3577594
29. Bhatt, P., Liu, J., Gong, Y., Wang, J., Guo, Y.: Emerging artificial intelligence–empowered mhealth: scoping review. JMIR mHealth and uHealth **10**(6), e35053 (2022)
30. Bodenreider, O., Cornet, R., Vreeman, D.J.: Recent developments in clinical terminologies - snomed ct, loinc, and rxnorm. Yearbook of medical informatics **27**, 129–139 (Aug 2018)
31. Boscardin, C.K., Gin, B., Golde, P.B., Hauer, K.E.: Chatgpt and generative artificial intelligence for medical education: potential impact and opportunity. Academic Medicine **99**(1), 22–27 (2024)
32. Brandon, C., Boßelmann, S., Singh, A., Ryan, S., Schieweck, A., Fennell, E., Steffen, B., Margaria, T.: Cinco de bio: A low-code platform for domain-specific workflows for biomedical research. BioMedInformatics **(to appear)** (2024)
33. Brandon, C., Boßelmann, S., Singh, A., Ryan, S., Schieweck, A., Fennell, E., Steffen, B., Margaria, T.: Cinco de bio: A low-code platform for domain-specific workflows for biomedical research. BioMedInformatics **(to appear)** (2024)

34. Brandon, C., Doherty, A.J., Kelly, D., Leddin, D., Margaria, T.: Hippp: Health information portal for patients and public. Applied Sciences **13**(16), 9453 (2023)
35. Brandon, C., Singh, A., Margaria, T.: Model driven development for AI-based healthcare systems: A review. In: Steffen, B. (ed.) Bridging the Gap Between AI and Reality - First International Conference, AISoLA 2023, Crete, Greece, October 23-28, 2023, Post-Proceedings (2024), this volume
36. Chartrand, G., Cheng, P.M., Vorontsov, E., Drozdzal, M., Turcotte, S., Pal, C.J., Kadoury, S., Tang, A.: Deep learning: a primer for radiologists. Radiographics **37**(7), 2113–2131 (2017)
37. Chenthara, S., Ahmed, K., Wang, H., Whittaker, F.: Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access **7**, 74361–74382 (2019)
38. Ciatto, G., Sabbatini, F., Agiollo, A., Magnini, M., Omicini, A.: Symbolic knowledge extraction and injection with sub-symbolic predictors: A systematic literature review. ACM Computing Surveys (2024)
39. Cohen, E., Lindman, I.: Importance of continuity of care from a patient perspective–a cross-sectional study in swedish health care. Scandinavian Journal of Primary Health Care **42**(1), 195–200 (2024)
40. Directorate-General for Health and Food Safety: A european health data space: harnessing the power of health data for people, patients and innovation. European Commission (2022), uRL: https://health.ec.europa.eu/document/download/17c7065c-c432-445f-9b27-8ccf283581bc_en?filename=com_2022-196_en.pdf (Accessed on 2024-01-28)
41. Dlamini, Z., Francies, F.Z., Hull, R., Marima, R.: Artificial intelligence (ai) and big data in cancer and precision oncology. Computational and Structural Biotechnology Journal **18**, 2300–2311 (2020)
42. Esmaeilzadeh, P.: Use of ai-based tools for healthcare purposes: a survey study from consumers' perspectives. BMC Medical Informatics and Decision Making **20**, 1–19 (2020)
43. Fennelly, O., Moroney, D., Doyle, M., Eustace-Cook, J., Hughes, M.: Key interoperability factors for patient portals and electronic health records: A scoping review. International Journal of Medical Informatics p. 105335 (2024)
44. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., et al.: Ai4people—an ethical framework for a good ai society: opportunities, risks, principles, and recommendations. Minds and machines **28**, 689–707 (2018)
45. Fredrikson, M., Jha, S., Ristenpart, T.: Model inversion attacks that exploit confidence information and basic countermeasures. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. pp. 1322–1333 (2015)
46. Gansel, X., Mary, M., van Belkum, A.: Semantic data interoperability, digital medicine, and e-health in infectious disease management: a review. Eur J Clin Microbiol Infect Dis **38**(6), 1023—1034 (2019), doi.org/10.1007/s10096-019-03501-6
47. Gerke, S., Babic, B., Evgeniou, T., Cohen, I.G.: The need for a system view to regulate artificial intelligence/machine learning-based software as medical device. NPJ digital medicine **3**(1), 53 (2020)
48. Gossen, F., Margaria, T., Steffen, B.: Towards explainability in machine learning: the formal methods way. it prof. 22 (4), 8–12 (2020) (2020)
49. Gossen, F., Margaria, T., Steffen, B.: Formal methods boost experimental performance for explainable ai. it prof. 23 (6), 8–12 (2021) (2021)

50. Gouripur, K., et al.: The impact of artificial intelligence on healthcare: A revolution in progress. The North and West London Journal of General Practice **10**(1) (2024)
51. Gubala, V., Harris, L.F., Ricco, A.J., Tan, M.X., Williams, D.E.: Point of care diagnostics: status and future. Analytical chemistry **84**(2), 487–515 (2012)
52. Hidayat, M., Defitri, S.Y., Hilman, H.: The impact of artificial intelligence (ai) on financial management. Management Studies and Business Journal (PRODUCTIVITY) **1**(1), 123–129 (2024)
53. Hu, H., Wen, Y., Chua, T.S., Li, X.: Toward scalable systems for big data analytics: A technology tutorial. IEEE Access **2**, 652–687 (2014)
54. Javed, I.T., Alharbi, F., Margaria, T., Crespi, N., Qureshi, K.N.: Petchain: A blockchain-based privacy enhancing technology. IEEE Access **9**, 41129–41143 (2021)
55. Jeyaraman, M., Ramasubramanian, S., Balaji, S., Jeyaraman, N., Nallakumarasamy, A., Sharma, S.: Chatgpt in action: Harnessing artificial intelligence potential and addressing ethical challenges in medicine, education, and scientific research. World Journal of Methodology **13**(4), 170–178 (2023)
56. Jing, F., Li, Z., Qiao, S., Zhang, J., Olatosi, B., Li, X.: Using geospatial social media data for infectious disease studies: a systematic review. International Journal of Digital Earth **16**(1), 130–157 (2023)
57. Kavitha, M., Srinivas, P.V.V.S., Kalyampudi, P., F, C.S., Srinivasulu, S.: Machine learning techniques for anomaly detection in smart healthcare. In: 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA). pp. 1350–1356 (2021). https://doi.org/10.1109/ICIRCA51532.2021.9544795
58. Khanna, N.N., Maindarkar, M.A., Viswanathan, V., Fernandes, J.F.E., Paul, S., Bhagawati, M., Ahluwalia, P., Ruzsa, Z., Sharma, A., Kolluri, R., Singh, I.M., Laird, J.R., Fatemi, M., Alizad, A., Saba, L., Agarwal, V., Sharma, A., Teji, J.S., Al-Maini, M., Rathore, V., Naidu, S., Liblik, K., Johri, A.M., Turk, M., Mohanty, L., Sobel, D.W., Miner, M., Viskovic, K., Tsoulfas, G., Protogerou, A.D., Kitas, G.D., Fouda, M.M., Chaturvedi, S., Kalra, M.K., Suri, J.S.: Economics of artificial intelligence in healthcare: Diagnosis vs. treatment. Healthcare **10**(12) (2022). https://doi.org/10.3390/healthcare10122493, `https://www.mdpi.com/2227-9032/10/12/2493`
59. Klar, E.: Medical Device Regulation als aktuelle Herausforderung für die rechtssichere Einführung neuer Technologien. Der Chirurg **89**(10), 755–759 (Oct 2018). https://doi.org/10.1007/s00104-018-0705-3, `https://doi.org/10.1007/s00104-018-0705-3`
60. Klementi, T., Kankainen, K.J.I., Piho, G., Ross, P.: Prospective research topics towards preserving electronic health records in decentralised content-addressable storage networks. In: HEDA@ Petri Nets. p. 14 (2022)
61. Klementi, T., Piho, G.: Method and system for managing data using decentralized content-addressable storage networks. European patent Office, priority number EP24166173.5 (March 2024), submitted pattent
62. Klementi, T., Piho, G., Ross, P.: A reference architecture for resolving health data accessibility, comprehensiveness, and ownership dilemmas through preserving semantically interoperable personal health records in decentralized content-addressable storage networks. (2024), will be published soon
63. Komorowski, M., Celi, L.A., Badawi, O., Gordon, A.C., Faisal, A.A.: The artificial intelligence clinician learns optimal treatment strategies for sepsis in intensive care. Nature medicine **24**(11), 1716–1720 (2018)

64. Kraljevic, Z., Searle, T., Shek, A., Roguski, L., Noor, K., Bean, D., Mascio, A., Zhu, L., Folarin, A.A., Roberts, A., Bendayan, R., Richardson, M.P., Stewart, R., Shah, A.D., Wong, W.K., Ibrahim, Z., Teo, J.T., Dobson, R.J.: Multi-domain clinical natural language processing with medcat: The medical concept annotation toolkit. Artificial Intelligence in Medicine **117**, 102083 (2021). https://doi.org/https://doi.org/10.1016/j.artmed.2021.102083, https://www.sciencedirect.com/science/article/pii/S0933365721000762
65. Lamprecht, A., Naujokat, S., Margaria, T., Steffen, B.: Semantics-based composition of EMBOSS services. J. Biomed. Semant. **2**(S-1), S5 (2011), http://www.jbiomedsem.com/content/2/S1/S5
66. Larkins, M.C., Thombare, A.: Point-of-care testing. In: StatPearls [Internet]. StatPearls Publishing (2023)
67. Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., Hua, D.: Review on security of federated learning and its application in healthcare. Future Generation Computer Systems **144**, 271–290 (2023)
68. Liu, M., Ning, Y., Ke, Y., Shang, Y., Chakraborty, B., Ong, M.E.H., Vaughan, R., Liu, N.: Fairness-aware interpretable modeling (faim) for trustworthy machine learning in healthcare (2024)
69. Liu, X., Faes, L., Kale, A.U., Wagner, S.K., Fu, D.J., Bruynseels, A., Mahendiran, T., Moraes, G., Shamdas, M., Kern, C., et al.: A comparison of deep learning performance against health-care professionals in detecting diseases from medical imaging: a systematic review and meta-analysis. The lancet digital health **1**(6), e271–e297 (2019)
70. Liu, X., Rivera, S.C., Moher, D., Calvert, M.J., Denniston, A.K., Ashrafian, H., Beam, A.L., et al.: Reporting guidelines for clinical trial reports for interventions involving artificial intelligence: the consort-ai extension. The Lancet Digital Health **2**(10), e537–e548 (2020)
71. Magrabi, F., Ammenwerth, E., McNair, J.B., De Keizer, N.F., Hyppönen, H., Nykänen, P., Rigby, M., Scott, P.J., Vehko, T., Wong, Z.S.Y., et al.: Artificial intelligence in clinical decision support: challenges for evaluating ai and practical implications. Yearbook of medical informatics **28**(01), 128–134 (2019)
72. Maleki Varnosfaderani, S., Forouzanfar, M.: The role of ai in hospitals and clinics: Transforming healthcare in the 21st century. Bioengineering **11**(4), 337 (2024)
73. Margaria, T., Chaudhary, H.A.A., Guevara, I., Ryan, S., Schieweck, A.: The interoperability challenge: building a model-driven digital thread platform for cps. In: International Symposium on Leveraging Applications of Formal Methods. pp. 393–413. Springer (2021)
74. Margaria, T., Floyd, B.D., Gonzalez Camargo, R., Lamprecht, A.L., Neubauer, J., Seelaender, M.: Simple management of high assurance data in long-lived interdisciplinary healthcare research: a proposal. In: Leveraging Applications of Formal Methods, Verification and Validation. Specialized Techniques and Applications: 6th International Symposium, ISoLA 2014, Imperial, Corfu, Greece, October 8-11, 2014, Proceedings, Part II 6. pp. 526–544. Springer (2014)
75. Margaria, T., Kubczak, C., Steffen, B.: Bio-jeti: a service integration, design, and provisioning platform for orchestrated bioinformatics processes. BMC Bioinformatics **9**(4), S12 (2008). https://doi.org/10.1186/1471-2105-9-S4-S12, https://doi.org/10.1186/1471-2105-9-S4-S12
76. Margaria, T., Schieweck, A.: The digital thread in industry 4.0. In: Integrated Formal Methods: 15th International Conference, IFM 2019, Bergen, Norway, December 2–6, 2019, Proceedings 15. pp. 3–24. Springer (2019)

77. Margaria, T., Steffen, B.: Backtracking-free design planning by automatic synthesis in metaframe. In: International Conference on Fundamental Approaches to Software Engineering. pp. 188–204. Springer (1998)
78. Margaria, T., Steffen, B.: Business process modeling in the jabc: the one-thing approach. In: Handbook of research on business process modeling, pp. 1–26. IGI Global (2009)
79. Margaria, T., Steffen, B.: Extreme model-driven development (xmdd) technologies as a hands-on approach to software development without coding. Encyclopedia of Education and Information Technologies pp. 732–750 (2020)
80. Munavalli, J.R., Boersma, H.J., Rao, S.V., Van Merode, G.: Real-time capacity management and patient flow optimization in hospitals using ai methods. Artificial intelligence and Data mining in healthcare pp. 55–69 (2021)
81. Murray-Watson, R.: Healthcare data breach statistics. The HIPAA Journal (2021), accessed: 2022-10-09
82. Nichols, J.H.: Utilizing point-of-care testing to optimize patient care. EJIFCC **32**(2), 140 (2021)
83. Ntoutsi, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M.E., Ruggieri, S., Turini, F., Papadopoulos, S., Krasanakis, E., et al.: Bias in data-driven artificial intelligence systems—an introductory survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery **10**(3), e1356 (2020)
84. Organization., W.H.: ICD-10 : international statistical classification of diseases and related health problems / World Health Organization. World Health Organization Geneva, 10th revision, 2nd ed. edn. (2004)
85. Patibandla, R.L., Rao, B.T., Murty, M.R.: Revolutionizing diabetic retinopathy diagnostics and therapy through artificial intelligence: A smart vision initiative. In: Transformative Approaches to Patient Literacy and Healthcare Innovation, pp. 136–155. IGI Global (2024)
86. Pechmann, L., Mildner, M., Suthau, T., Leucker, M.: Regulatorische anforderungen an lösungen der künstlichen intelligenz im gesundheitswesen. In: Pfannstiel, M.A. (ed.) Künstliche Intelligenz im Gesundheitswesen: Entwicklungen, Beispiele und Perspektiven, pp. 175–198. Springer Fachmedien Wiesbaden (2022). https://doi.org/10.1007/978-3-658-33597-7_8, https://doi.org/10.1007/978-3-658-33597-7_8
87. Pechmann, L., Potdevin, Y., Brehmer, K., Nowotka, D., Leucker, M.: Crisp-pccp – a development methodology supporting fda approval for machine learning enabled medical devices. In: Steffen, B. (ed.) Bridging the Gap Between AI and Reality - First International Conference, AISoLA 2023, Crete, Greece, October 23-28, 2023, Post-Proceedings (2024), this volume
88. Pesapane, F., Volonté, C., Codari, M., Sardanelli, F.: Artificial intelligence as a medical device in radiology: ethical and regulatory issues in europe and the united states. Insights into imaging **9**, 745–753 (2018)
89. Petersen, E., Potdevin, Y., Mohammadi, E., Zidowitz, S., Breyer, S., Nowotka, D., Henn, S., Pechmann, L., Leucker, M., Rostalski, P., Herzog, C.: Responsible and regulatory conform machine learning for medicine: A survey of challenges and solutions. IEEE Access **10**, 58375–58418 (2022). https://doi.org/10.1109/ACCESS.2022.3178382, https://doi.org/10.1109/ACCESS.2022.3178382
90. Piho, G., Tepandi, J., Thompson, D., Woerner, A., Parman, M.: Business archetypes and archetype patterns from the hl7 rim and openehr rm perspectives:

towards interoperability and evolution of healthcare models and software systems. Procedia Computer Science **63**, 553–560 (2015)
91. Raab, R., Küderle, A., Zakreuskaya, A., Stern, A.D., Klucken, J., Kaissis, G., Rueckert, D., Boll, S., Eils, R., Wagener, H., et al.: Federated electronic health records for the european health data space. The Lancet Digital Health **5**(11), e840–e847 (2023)
92. RABBI, F., Mukhiya, S.K., Norge, T., Lamo, Y.: Towards a multi-dimensional health data analysis framework. In: Steffen, B. (ed.) Bridging the Gap Between AI and Reality - First International Conference, AISoLA 2023, Crete, Greece, October 23-28, 2023, Post-Proceedings (2024), this volume
93. Rahman, M.A., Victoros, E., Ernest, J., Davis, R., Shanjana, Y., Islam, M.R.: Impact of artificial intelligence (ai) technology in healthcare sector: A critical evaluation of both sides of the coin. Clinical Pathology **17**, 2632010X241226887 (2024)
94. Randmaa, R., Bossenko, I., Klementi, T., Piho, G., Ross, P.: Evaluating business meta-models for semantic interoperability with fhir resources. In: HEDA@Petri Nets (2022)
95. Rasche, C., Margaria, T., Floyd, B.D.: Service model innovation in hospitals: Beyond expert organizations. Service Business Model Innovation in Healthcare and Hospital Management: Models, Strategies, Tools pp. 1–20 (2017)
96. Rasche, C., Reinecke, A.A., Margaria, T.: Künstliche Intelligenz im Gesundheitswesen als Kernkompetenz? Status quo, Entwicklungslinien und disruptives Potenzial, pp. 49–79. Springer Fachmedien Wiesbaden, Wiesbaden (2022), https://doi.org/10.1007/978-3-658-33597-7_2
97. Rawal, A., McCoy, J., Rawat, D.B., Sadler, B.M., St Amant, R.: Recent advances in trustworthy explainable artificial intelligence: Status, challenges, and perspectives. IEEE Transactions on Artificial Intelligence **3**(6), 852–866 (2021)
98. Rivera, S.C., Liu, X., Chan, A.W., Denniston, A.K., Calvert, M.J., Ashrafian, H., Beam, A.L., et al.: Guidelines for clinical trial protocols for interventions involving artificial intelligence: the spirit-ai extension. The Lancet Digital Health **2**(10), e549–e560 (2020)
99. Saelaert, M., Mathieu, L., Van Hoof, W., Devleesschauwer, B.: Expanding citizen engagement in the secondary use of health data: an opportunity for national health data access bodies to realise the intentions of the european health data space. Archives of Public Health **81**(1), 168 (2023)
100. Sager, N., Lyman, M., Bucknall, C., Nhan, N., Tick, L.J.: Natural Language Processing and the Representation of Clinical Data. Journal of the American Medical Informatics Association **1**(2), 142–160 (03 1994). https://doi.org/10.1136/jamia.1994.95236145, https://doi.org/10.1136/jamia.1994.95236145
101. Seelaender, M., Laviano, A., Busquets, S., Püschel, G.P., Margaria, T., Batista, M., et al.: Inflammation in cachexia (2015)
102. Seyyed-Kalantari, L., Zhang, H., McDermott, M.B., Chen, I.Y., Ghassemi, M.: Underdiagnosis bias of artificial intelligence algorithms applied to chest radiographs in under-served patient populations. Nature medicine **27**(12), 2176–2182 (2021)
103. Shah, V., Konda, S.R.: Cloud computing in healthcare: Opportunities, risks, and compliance. Revista Espanola de Documentacion Cientifica **16**(3), 50–71 (2022)
104. Shen, B., Guo, J., Yang, Y.: Medchain: Efficient healthcare data sharing via blockchain. Applied Sciences **9**(6) (2019). https://doi.org/10.3390/app9061207, https://www.mdpi.com/2076-3417/9/6/1207

105. Shickel, B., Tighe, P.J., Bihorac, A., Rashidi, P.: Deep ehr: A survey of recent advances in deep learning techniques for electronic health record (ehr) analysis. IEEE Journal of Biomedical and Health Informatics **22**(5), 1589–1604 (2018), doi.org/10.1109/JBHI.2017.2767063
106. Simpson, G., Nana, L., Kester, Q.A.: A centralized data validation system model for healthcare systems based on blockchain. In: 2021 International Conference on Cyber Security and Internet of Things (ICSIoT). pp. 55–58 (2021). https://doi.org/10.1109/ICSIoT55070.2021.00019
107. Singh, A., Minguett, O., Margaria, T.: Binary decision diagrams and composite classifiers for analysis of imbalanced medical datasets. Electronic Communications of the EASST **82** (2023)
108. Sõerd, T., Kankainen, K., Piho, G., Klementi, T., Ross, P.: Towards specification of medical processes according to international standards and semantic interoperability needs. In: MODELSWARD. pp. 160–167 (2023)
109. Stadler, T., Oprisanu, B., Troncoso, C.: Synthetic data - anonymisation groundhog day. In: 31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022. pp. 1451–1468. USENIX Association (2022)
110. Strickland, E.: Ibm watson, heal thyself: How ibm overpromised and underdelivered on ai health care. IEEE Spectrum **56**(4), 24–31 (2019)
111. Subramanian, M., Wojtusciszyn, A., Favre, L., Boughorbel, S., Shan, J., Letaief, K.B., Pitteloud, N., Chouchane, L.: Precision medicine in the era of artificial intelligence: implications in chronic disease management. Journal of translational medicine **18**, 1–12 (2020)
112. Sucipto, H.: The impact of artificial intelligence (ai) on human resource management practices. Management Studies and Business Journal (PRODUCTIVITY) **1**(1), 138–145 (2024)
113. Surya, L.: How government can use ai and ml to identify spreading infectious diseases. International Journal of Creative Research Thoughts (IJCRT), ISSN pp. 2320–2882 (2018)
114. Syed, R., Eden, R., Makasi, T., Chukwudi, I., Mamudu, A., Kamalpour, M., Kapugama Geeganage, D., Sadeghianasl, S., Leemans, S.J., Goel, K., et al.: Digital health data quality issues: Systematic review. Journal of Medical Internet Research **25**, e42615 (2023)
115. Tariq, M.U.: Advanced wearable medical devices and their role in transformative remote health monitoring. In: Transformative Approaches to Patient Literacy and Healthcare Innovation, pp. 308–326. IGI Global (2024)
116. Tettey, F., Parupelli, S.K., Desai, S.: A review of biomedical devices: classification, regulatory guidelines, human factors, software as a medical device, and cybersecurity. Biomedical Materials & Devices **2**(1), 316–341 (2024)
117. Turner, N., Baxter, D.: How to enable ambidexterity in safety-critical software development: This article reports on a safety-critical development project that achieved ambidexterity and highlights four leadership behaviors that can enhance project outcomes. Research-Technology Management **67**(2), 35–43 (2024)
118. Ueda, D., Kakinuma, T., Fujita, S., Kamagata, K., Fushimi, Y., Ito, R., Matsui, Y., Nozaki, T., Nakaura, T., Fujima, N., et al.: Fairness of artificial intelligence in healthcare: review and recommendations. Japanese Journal of Radiology **42**(1), 3–15 (2024)
119. U.S. Food and Drug Administration: Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine

Learning (AI/ML)-Enabled Device Software Functions (Apr 2023), https://www.fda.gov/media/166704/download
120. Šabić, E., Keeley, D., Henderson, B., Nannemann, S.: Healthcare and anomaly detection: using machine learning to predict anomalies in heart rate data. AI Soc. **36**(1), 149–158 (mar 2021). https://doi.org/10.1007/s00146-020-00985-1, https://doi.org/10.1007/s00146-020-00985-1
121. Wachter, R.M., Brynjolfsson, E.: Will generative artificial intelligence deliver on its promise in health care? JAMA **331**(1), 65–69 (2024)
122. Wang, Q., Su, M., Zhang, M., Li, R.: Integrating digital technologies and public health to fight covid-19 pandemic: key technologies, applications, challenges and outlook of digital healthcare. International Journal of Environmental Research and Public Health **18**(11), 6053 (2021)
123. Wang, S., Summers, R.M.: Machine learning and radiology. Medical image analysis **16**(5), 933–951 (2012)
124. Wastvedt, S., Huling, J.D., Wolfson, J.: An intersectional framework for counterfactual fairness in risk prediction. Biostatistics p. kxad021 (08 2023). https://doi.org/10.1093/biostatistics/kxad021, https://doi.org/10.1093/biostatistics/kxad021
125. Wu, Q., Chen, X., Zhou, Z., Zhang, J.: Fedhome: Cloud-edge based personalized federated learning for in-home health monitoring. IEEE Transactions on Mobile Computing **21**(8), 2818–2832 (2020)
126. Wu, Z., He, J.: Fairness-aware model-agnostic positive and unlabeled learning. In: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency. pp. 1698–1708. FAccT '22, Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3531146.3533225, https://doi.org/10.1145/3531146.3533225
127. Yang, J., Soltan, A., Eyre, D., Yang, Y., Clifton, D.: An adversarial training framework for mitigating algorithmic biases in clinical machine learning. NPJ Digital Medicine **6**(1) (2023)
128. Yang, J., Soltan, A.A.S., Yang, Y., Clifton, D.A.: Algorithmic fairness and bias mitigation for clinical machine learning: Insights from rapid covid-19 diagnosis by adversarial learning. medRxiv (2022). https://doi.org/10.1101/2022.01.13.22268948, https://www.medrxiv.org/content/early/2022/01/14/2022.01.13.22268948
129. Yao, Y., Han, T., Yu, J., Xie, M.: Uncertainty-aware deep learning for reliable health monitoring in safety-critical energy systems. Energy **291**, 130419 (2024)
130. Zheng, Y., Wang, L., Feng, B., Zhao, A., Wu, Y.: Innovating healthcare: the role of chatgpt in streamlining hospital workflow in the future. Annals of Biomedical Engineering **52**(4), 750–753 (2024)
131. Zuo, A., Wei, S., Liu, T., Han, B., Zhang, K., Gong, M.: Counterfactual fairness with partially known causal graph. In: Koyejo, S., Mohamed, S., Agarwal, A., Belgrave, D., Cho, K., Oh, A. (eds.) Advances in Neural Information Processing Systems. vol. 35, pp. 1238–1252. Curran Associates, Inc. (2022), https://proceedings.neurips.cc/paper_files/paper/2022/file/08887999616116910fccec17a63584b5-Paper-Conference.pdf