AI solutions in healthcare: GDPR compliance and the new AIA.

Yasmine Yachou

Supervisor: Sieuwert van Otterloo

Vrije Universiteit Amsterdam

y.yachou@student.vu.nl

Abstract: This paper investigates in what manner innovative tech companies in the Netherlands can research or provide AI technology that is based on healthcare data, while complying to the rules and regulations of the GDPR and the AIA. The use of AI technologies in the healthcare sector is considered high risk, according to the newly proposed AIA, introduced in April 2021. This is because of the risks these technologies could pose when it comes to the health or life of the data subjects. According to the GDPR, the use of health data is furthermore considered a special category of personal data, meaning it can only be used under specific conditions.
The aim of the research is therefore to investigate how these innovative companies can implement sufficient privacy measures in order to be allowed to conduct research on AI technologies that use health data. Also, as the GDPR and the AIA are both separate regulations, the aim is to investigate the main differences between the GDPR and the AIA in the way these regulations regulate the use of AI, as well as the use of health data in specific. The findings have shown that AIA can be considered an addition to the GDPR, and that the selected companies comply sufficiently to the GDPR, as well as most aspects of the AIA.

Keywords: GDPR, AIA, compliance, AI, data protection, health data, healthcare

1 Introduction

The perceived potential of Artificial Intelligence (AI) has resulted in an increased development of AI technologies in many different industries [1]. This increased development is especially prevalent in the healthcare industry, as it is believed that the use of AI technologies provides further advancements when it comes to the care that is provided to patients [1, 5]. An example of such advancements can be recognized when it comes to diagnostic processes or other forms of clinical decision making [1]. Many researchers suggest that the use of AI in this process, can greatly improve the accuracy in which diseases are diagnosed and even suggest that these technologies can eventually outperform humans [5, 15].

1.1 Motivation

In order to truly capture the benefit of the use of AI technologies in the healthcare industry, it is required for these technologies to have access to large amounts of personal data [7]. Since this data is sensitive, consisting of the medical data of patients, it is important that this information is appropriately safeguarded. It is therefore necessary that appropriate privacy measures are in place to ensure the privacy of the data subjects, which in this case are the patients [7]. The General Data Protection Regulation[1] (GDPR), in effect since May 2018, is considered the legal framework when it comes to the regulation of both the processing and collecting of personal data for all individuals residing in the European Union (EU) [6].

1.2 Problem definition

As aforementioned, the GDPR has been set in place in order to regulate how personal data is dealt with. However, there still exists some doubts about its possibility to properly regulate how sensitive data is processed when making use of AI technologies in the healthcare sector [5]. This is because processing health data, which is considered a special category of personal data, is not allowed according to Article 9 of the GDPR, unless done under specific conditions. It is specifically Article 9(1)[2] that forbids the processing of such sensitive information, unless it is based on legal grounds that are specified in Article 9(2)[3]. These conditions mentioned in Article 9(2) allow for health data to be processed in case explicit consent is given by the data subjects. However, the GDPR also makes it possible to process, and therefore make use of health data, without the explicit consent of the data subjects. The use of health data without having to obtain explicit consent from the data subjects, is allowed in case of a larger public interest in regards to the general health of the public, protecting a data subject in a situations where explicit consent legally or physically cannot be given, health data that is already made public by the data subject themselves, the provision of healthcare services, such as having a specialist inform a medical practitioner about a patient's health status, dealing with legal claims, social protection and security laws, as well as research, archiving and statistic purposes [18].

Not being able to process health data could prove to be an issue, especially for small innovative tech companies that are researching or providing AI technologies in the healthcare industry. Article 9(2) does mention the use of special categories, such as health data, for the provision of healthcare services and therefore treating patients. However, it does not mention the use of health data for the research or development of AI technologies in the healthcare sector [21]. Also, as these so-called small innovative

---

[1] *The General Data Protection Regulation* (May 25, 2018) https://eur-lex.europa.eu/eli/reg/2016/679/oj. Visited on January 17, 2022.

[2] Article 9(1) (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[3] Article 9(2) (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

companies often have limited resources, such as limited expertise or knowledge, it is a challenge for these companies to implement sufficient privacy measures in order to be able to conduct research and make use of health data. Compared to larger firms, these companies usually do not have easy access to large quantities of data, such as customer data [11]. These small innovative companies usually also do not possess over a large budget and can therefore not easily create additional positions within the company that aim to deal with the compliance to the rules of the GDPR. This often leads to these companies being put in a position where they need to reallocate their resources in order to fit their budget, which often stunts innovation [3].

In April 2021, the European Commission has proposed a draft of a possible new regulation, namely the Artificial Intelligence Act (AIA). This proposal of a new regulation aims to reduce the possible risks of AI technologies, by further categorizing these technologies into minimal risk, limited risk, high-risk and completely prohibited, and aims to regulate compliance with these new guidelines [22]. This approach however, could further impact tech companies when it comes to innovating AI technologies within healthcare, as many of these technologies can be considered high-risk due to the risks these AI technologies could pose on a person's health or life. This means that the proposed AIA could impose even more restricting legal requirements for the development of such technologies.

1.3 Research question

The aim of this research is to investigate in what manner innovative tech companies in the Netherlands can research or provide AI technologies that are based on healthcare data, while complying to the rules and regulations of the GDPR and the AIA. This will be done by investigating specific AI technologies, through conducting interviews with the small innovative companies of the respective technologies. Furthermore, this research aims to provide a clear overview of the main differences between the GDPR and the AIA in the way these regulations aim to regulate the use of AI, as well as the use of health data in specific. Overall, this research aims to recognize possible solutions or insights into how AI technologies can be implemented specifically in the healthcare industry, without breaching the laws and regulations of the GDPR and the AIA that are currently in place.

In the aforementioned objectives of this research in mind, the following research question can be constructed:

"In what manner can innovative tech companies in the Netherlands research or provide AI technology that is based on healthcare data, while complying to the rules and regulations of the GDPR and the AIA."

In order to eventually be able to provide an answer to this main research question, the following sub-questions can be constructed:

"Are there any differences between the AIA and the GDPR when it comes to the regulation of AI and the use of health data?"

"In what manner do small innovative tech companies in the Netherlands, currently comply with the existing laws and regulations of the AIA and the GDPR?"

1.4 Scientific and practical contribution

The use of AI technologies in the healthcare industry has been proven to bring forth many advancements when it comes to providing care to patients. However, the use of health data, that is often required for these technologies, is what makes the implementation of these technologies rather difficult, as there are currently still many implications in terms of data privacy and protection, transparency and even accountability [5, 7]. Related literature has shown some effort in recognizing ways to further improve on these implications and therefore provide more clarity in how such technologies can be implemented while being compliant to the guidelines of the GDPR [13]. However, related literature has also shown a lack of research when it comes to specific AI technologies that exist in the healthcare industry.

This research aims to contribute to already existing research by investigating specific AI technologies, through conducting interviews with various small innovative tech companies in the Netherlands that research or provide such technologies. By using this approach, the aim is to obtain additional insights, especially in regards to how these providers exactly go about complying to the GDPR, which could possibly lead to beneficial information that might not be found through solely reviewing existing literature. Besides compliance to the GDPR, this research also aims to include the new AIA draft that was published last year, in an attempt to compare possible differences between the AIA and the GDPR.

2 Related Literature

Related literature has shown that many studies recognize that there are still some existing difficulties when it comes to the use of health data for the provision of AI technologies geared towards the healthcare sector. As the proposed AIA has only been introduced quite recently, namely April 2021, related literature currently still shows a lack of researches done on the topic of the AIA, especially when it comes to the use of health data for the provision of AI technologies geared towards the healthcare sector. The related literature can be categorized into the following topics:

2.1 AI in healthcare and the GDPR

When it comes to the implementation of AI in the healthcare industry, the availability of sufficient data is crucial in order for these AI technologies to assist in decision making and provide accurate results. As this data mostly consists of health data, it is especially important to properly maintain sufficient data privacy and protection

measures, which needs to be done on the basis of the rules and regulations of the GDPR [7]. Expecting compliance to the GDPR can help create a sense of responsibility and accountability for the companies that make use of these AI technologies, and can therefore help minimize the possible risks these technologies could pose once implemented in the healthcare industry [7].

The research conducted by Jokic [9] recognizes the difficulties when it comes to the use of automated decision making through the implementation of AI technologies in the healthcare industry and the rules and guidelines provided by the GDPR, especially when it comes to the topic of consent [9]. The research analyzes how the use of health data for medical devices, challenges the concept of consent that has been set up in the GDPR. Jokic [9] however, does not consider other concepts of the GDPR in terms of data protection, nor does this research investigate how specific tech companies go about ensuring data protection.

The research conducted by Mourby et al. [13] takes a different approach, as it aims to investigate on what basis of the GDPR the implementation of AI in healthcare industry can be justified and in what manner transparency can be increased when it comes to the use of health data for the provision of AI technologies in the healthcare sector. Mourby et al. [13] however, also do not consider other aspects of the GDPR, besides transparency, nor do they include the newly proposed AIA or the subjective perspective of specific tech companies.

2.2 Tech startups and ensuring data protection

Small innovative tech companies are known to have limited resources. This often makes it challenging for these companies to implement sufficient privacy measures in order to ensure data protection and privacy, which results in these companies having to reallocate their resources in order to fit their budget [3].

The research of Norval [14] does share some similarities with this research, as it focuses specifically on how tech startups in the United Kingdom (UK) go about ensuring data protection and privacy, however also only considers the laws and regulations of the GDPR, as the study has been conducted before the existence of the proposed AIA. Also, important to note, is that the research does not focus on the use of AI in the healthcare sector or the use of health data.

2.3 The difference between the AIA and the GDPR

As part of this research aims to investigate in what manner the AIA and the GDPR differ when it comes to the use of health data, as well as the manner in which AI is regulated, it is also important to take a look at existing literature that analyzes both the AIA and the GDPR.

The research of Gellert [8] investigates the main differences when it comes to how the GDPR and the AIA go about ensuring data protection. However, besides generally

discussing the differences when it comes to regulating the use of data, the research does not investigate the differences between both the AIA and the GDPR when it comes to the use of health data in specific.

To conclude, related literature has shown that many studies recognize that there are still some existing difficulties when it comes to the use of AI technologies in the healthcare industry. There has also been some research done when it comes to the experience or struggles that smaller tech companies often face in regards to compliance to the GDPR. However, it becomes apparent there has not been any literature found that considers the newly proposed draft of the AIA regulation and how this regulation compares to the GDPR, specifically when it comes to the use of health data. There also seems to be a lack of investigation when it comes to how innovative tech companies, specifically in the Netherlands, go about using health data in order to provide AI technologies that can be used in the healthcare sector, while complying to both the AIA and the GDPR.

3 Methodology

In order to provide an answer to the previously mentioned research questions, a qualitative, interpretivist, inductive approach has been be taken, as the research questions can be used to "build" and test possible new theories or additional insights [4]. Furthermore, from this qualitative approach, three different research strategies can be identified, namely a literature review, web search, as well as conducting structured interviews, further described in the section about data collection.

3.1 Data collection

Literature review:

In order to answer the main research question, the sub-question *"Are there any differences between the AIA and the GDPR when it comes to automated decision making and the use of health data?"* can be investigated by conducting a literature review. Through reviewing already existing literature, more clarity can be provided when it comes to exactly how AI technologies and the use of health data are being regulated by both the GDPR and the AIA [17]. Using this information, a clear overview can be given of the differences between both the AIA and the GDPR when it comes to regulating the use of AI and health data in the healthcare industry.

Once this overview has been made, it is possible to investigate in what manner the small innovative tech companies that research or provide these different technologies comply with the laws and regulations of both the GDPR and the AIA regulation.

Web search:

In order to be able to investigate in what manner small innovative tech companies in the Netherlands currently comply to the rules and regulations of the GDPR and the AIA, it is important to first identify which companies fit within the scope of this research and can therefore be approached to be interviewed. This is done through a web search, in which the information, readily made available on the web, is used to create a shortlist of companies that fit within the scope of this research. Various different web pages have been visited, in order to find the relevant innovative tech companies in the Netherlands that research or provide AI technologies for the healthcare sector, such as platforms as Crunchbase[4], RocketReach[5] and Dealroom[6]. Besides these online platforms, other web pages have been visited as well, such as the Dutch AI coalition[7], that gives an overview of all different types of small tech companies throughout the Netherlands. In order to assess exactly which companies are considered suitable within the scope of this research, the following criteria has been established:

- The respective company is based in the Netherlands.
- The respective company researches or provides AI technologies for the healthcare sector.

If the respective company passes the aforementioned criteria, it is added to the shortlist. All companies added to the shortlist have been approached, in order to obtain their consent for the conduction of the interviews. All companies in the shortlist have then been contacted through emails, phone calls or the social network LinkedIn[8].

Structured interviews:

After the relevant innovative tech companies have been identified, interviews with the respective small innovative tech companies that research or provide AI technologies, geared towards the healthcare sector, can be conducted. Through these interviews, it is possible to obtain insights into how exactly such experts go about compliance to the GDPR, as well as the newly proposed AIA, which can often not be acquired through literature review alone [4, 10]. This research strategy can therefore be used in order to answer the second sub-question, namely *"In what manner do small innovative tech companies that research or provide AI technologies in the healthcare sector, currently comply with the existing laws and regulations of the GDPR and the AIA?".* Overall, conducting interviews with the providers allows for obtaining additional insights, especially in regards to the subjective perspective of the experts when it comes to the identified research questions.

[4] https://www.crunchbase.com/
[5] https://rocketreach.co/
[6] https://dealroom.co/
[7] https://nlaic.com/
[8] https://www.linkedin.com/

The interviews that have been conducted were an hour long and structured, meaning prior to the interviews there were already open-ended, predefined questions that have been considered relevant for the research [4]. The same interview protocol is used for all conducted interviews. The content of the questions is based on the relevant articles of both the GDPR and the AIA regulation.

The questions that have been asked during the interviews, are based on survey questions that have been created beforehand. These questions can be divided into two different categories, namely questions that refer to the requirements of the AIA when it comes to high-risk AI technologies, and questions that refer to the GDPR, in specific when it comes to how these companies experience complying to the rules and guidelines of the GDPR.

3.2 Focus

As aforementioned, the focus of this research and the conducted interviews are the small innovative tech companies that research or provide AI technologies, geared towards the healthcare sector. However, as the questions consist of two parts, namely a part that revolves around the GDPR and a part that revolves around the AIA, it is also important that for each company, the relevant experts are interviewed. As the AIA part mainly concerns technical aspects of the AI technologies the companies research or provide, the technical responsible staff of each company is approached to answer the respective questions. For the GDPR part however, the GDPR responsible staff is approached, as these questions revolve around compliance questions.

However, important to note is that since the focus is on small innovative tech companies, it might be possible that one person has responsibilities when it comes to both the technical and compliance activities within a company. It is therefore not considered a necessity to interview two different persons within a company, as long as the respective person possesses over the necessary knowledge in order to answer both the technical and compliance questions.

In total twelve interviews have been conducted, which either took place over the phone, in-person or through Google Meet meetings. Out of these interviews, eight where conducted with the respective GDPR responsible staff of a company, and four with the respective technical responsible staff of a company, which can be seen in *Table 1*. Each company personally appointed the representatives that were suitable to be interviewed within the scope of the research. In order to make use of the insights provided by the companies, the different companies have been pseudonymized.

Company	*Company focus*	*Conducted interview*
1	Wearable smart technology	GDPR
2	Medical imaging analysis	GDPR, AIA
3	Medical imaging analysis	GDPR, AIA
4	Precision medicine (personalized care)	GDPR, AIA
5	Medical diagnostics	GDPR
6	Precision medicine (personalized care)	GDPR, AIA
7	Movement analysis	GDPR
8	Movement analysis	GDPR

Table 1. Information interviewed small innovative tech companies.

3.3 Data analysis

After transcribing and compiling all of the answers from the interviews, the different answers that have been provided by the different experts have been analyzed, in order to possibly recognize patterns or inconsistencies in how these experts go about reaching compliance. This analysis has been done by using the thematic content analysis method, meaning the interviews have been analyzed in a comparative manner in order to recognize possible patterns [10]. In order to facilitate this method, the answers given during the interview have been entered into the created survey, in order to get a clear overview of the different answers given. Having this collection of answers, therefore helps identify possible patterns or inconsistencies more easily.

4 The GDPR and the AIA

4.1 AIA analysis:

As aforementioned, the AIA, proposed in 2021 by the European Commission, aims to regulate the growing use of AI technologies by any party that either distributes or provides such technologies within the EU [2]. The AIA takes on a risk-based approach, in which possible risks, associated to the use of an AI technology, are recognized. The AIA categorizes these risks into four different categories, namely minimal risk, limited risk, high-risk and prohibited AI technologies [8]. As aforementioned, the scope of the research is on the high-risk category of AI technologies. Article 6(1) of the AIA provides the following definition for high-risk AI technologies:

"*An AI system shall be considered high risk in case the AI system is intended to be used as a safety component of a product, or is itself a product covered by the Union harmonization legislation listed in Annex II, or is required to undergo a third-party*

conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonization legislation listed in Annex II."[9]

Article 6(2) of the AIA expands on this definition by providing several categories of AI technologies that are also deemed high-risk, namely:

"

1. *Biometric identification and categorization of natural persons.*
2. *Critical infrastructure where AI could pose risks for the life and health of people*
3. *Educational and vocational training*
4. *Employment, worker management, and self-employment*
5. *Access to essential private and public services*
6. *Law enforcement*
7. *Migration, asylum, and border control*
8. *The administration of justice and democratic processes* "[10]

AI technologies developed for the use in the healthcare industry are often classified high-risk technologies, as a lot of these technologies, such as the use of medical devices for example, are subjected to conformity assessments by third-parties, and could pose risks when it comes to the health or life of a patient that is subjected to the use of these AI technology. For AI technologies that are classified as high-risk, the AIA elaborates on multiple requirements that providers or distributors of such technologies need to abide by in order to be able to properly mitigate the possible risks. These requirements can be divided into the following categories and serve as the base for the interview questions:

1. Risk management system:

According to Article 9[11] of the AIA, all AI technologies that are considered high-risk have to implement a risk management system. This system is aimed to help companies identify the possible risks of their AI technology and can therefore help companies identify measures to counter such risks. In order to properly identify possible risks, and therefore be able to have appropriate safeguards in place in order to protect its data subjects from these possible risks, it is important that these risk management systems are kept up to date and run continuously throughout the entire time the AI technology is in use. In order to be able to generate these insights, the following questions have been created:

---

[9] Article 6(1) (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[10] ANNEX III (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[11] Article 9 (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

- "*Is there a risk management system in place that is able to identify and analyze the possible risks that might occur from the use of the AI technology?*"
- "*How often is the system used?*"
- "*Do you use a set of standard risks? If so, what are these standard risks?*"

2. Post-market monitoring:

AI technologies make use of training data sets in order to extract general information or patterns, which eventually allows the technology to be able to make accurate predictions. As these so-called algorithms are meant to respond to changes in data, specifically the growing volumes of the data [7], the AIA considers it important for the developers of these technologies to implement a post-market monitoring system. This post-market monitoring system is aimed to provide a better overview of the performance of AI systems in the long run, as it collects and analyzes real-world data of the users of the technology. Important to note is that this step is done after the technology is approved and is therefore already introduced to the market [12].

According to Article 61[12] of the AIA, all AI technologies that are considered high-risk have to implement a post-market monitoring system and have to ensure that this system is kept up to date and runs continuously throughout the entire time the AI technology is in use. Article 61(3) of the AIA furthermore clarifies that the post-market monitoring system is based on a so-called monitoring plan, which explains what methods are used for the monitoring of the AI technology. In order to be able to generate these insights, the following questions have been created:

- *"Is there a post-market monitoring system?"*
- "*How is this system monitored?*"
- "*Is there also a monitoring plan in place that explains the methods for monitoring, which the monitoring system is based on?*"

3. Technical documentation:

According to Article 11[13] of the AIA, all AI technologies that are considered high-risk need a technical documentation. This documentation provides additional information when it comes to the manner in which the technology is designed, as well as any other relevant information in regards to the use of the AI technology. In order to be able to generate these insights, the following questions have been created:

- "*Is a technical documentation made available?"*
- "*Do you publish details about the algorithm used?*"

---

[12] Article 61 (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[13] Article 11 (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

- "*Do you publish details on what data has been used to train the algorithms?*"
- "*Do you publish source code of the AI solution?*"
- "*If these details are published, where are they published?*"

4. Data:

The development of high-risk AI technologies requires training, testing and validating on various data sets. It is important to know how these data sets are governed and managed, meaning what type of data is collected, how it is prepared, how is dealt with possible biases etc.[16] This is all relevant information, as it can give an overview of how the safety and accuracy of AI technologies is ensured, which is related to how well the technologies have been trained and tested beforehand.

According to Article 10[14] of the AIA, all AI technologies that are considered high-risk, need to be properly trained, tested and validated. Article 10(2) specifically clarifies the different requirements in terms of data governance that need to be considered when going through the process of training, testing and validating data sets. These requirements have to do with the type of data that is collected, how the data is prepared, how the data sets are assessed, how is dealt with possible biases and other possible shortcomings or data gaps. In order to be able to generate these insights, the following questions have been created:

- "*Are the respective AI technologies tested before they are implemented? If so, how is this testing process performed?"*
- *"How do you assess the suitability and quantity of data sets for your specific AI technology?*
- *"How are possible biases, data gaps and other shortcomings addressed and dealt with?"*

5. Accuracy, robustness and security:

According to Article 15[15] of the AIA, AI technologies need to implemented in such a way that accuracy, robustness and security aspects are all appropriately ensured, for as long as the respective AI technologies are in use. It is therefore important to know what measures are taken in order to ensure these aspects, such as whether they have appropriate backup plans, data security measures, as well as appropriate measures for dealing with errors etc. In order to be able to generate these insights, the following questions have been created:

- "*How do you ensure that the AI technology is resilient to possible errors or inconsistencies?*"

---

[14] Article 10 (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[15] Article 15 (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

- "*How is the security of the data ensured (e.g. cyberattacks such as manipulating the data or unauthorized access)?*"

6. Record keeping:

Article 12[16] of the AIA clarifies that it is important for the operations of the AI technologies to be traceable throughout its whole lifecycle, in order to be able to monitor the technology and to be able to possible recognize possible situations that could result in risks for the data subjects. It is therefore important to know whether the AI technology has some sort of logging or recording capabilities in order to recognize such situations and therefore to be able to mitigate possible risks more easily. In order to be able to generate these insights, the following questions have been created:

- "*Is there a log system in place that is able to record the operations of the respective AI technology?*"
- "*How long are these records stored for?*"
- "*Are there any natural persons involved when it comes to verifying the results of the automatic recordings?*"

7. Human oversight:

Whether the AI technologies are overseen by natural persons during its use, is relevant information as it allows for the recognition of risks to the health, safety or fundamental rights of the respective data subjects, when the technology is in use [20]. It is therefore not only important to know whether these technologies are overseen by natural persons, but also how these natural persons operate in order to be able to identify or address any anomalies, dysfunctions and unexpected performances as soon as possible.

Article 14[17] of the AIA clarifies that all AI technologies that are considered high-risk, are required to have additional human-machine interface tools in order to ensure that the AI technology can properly be overseen by natural persons and therefore allows for the recognition of risks to health, safety or fundamental rights when the technology is in use. Article 11(4) further clarifies the responsibilities of the natural persons that are assigned to perform the human oversight task. These responsibilities described mainly have to do with need for the individuals to have a full understanding of the AI technology and are therefore able to interpret its results and detect possible issues. It is important for these individuals to intervene if necessary and to recognize when such decisions need to be made. In order to be able to generate these insights, the following questions have been created:

---

[16] Article 12 (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[17] Article 14 (April 21, 2021) *The Artificial Intelligence Act* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

- "*Under the new AIA, individuals responsible for overseeing the AI technology need to be able to intervene if necessary. Are there such natural persons involved?"*
- "*Individuals responsible for overseeing the AI technology need to be able to intervene if necessary and therefore need to be able to stop the operation whenever deemed necessary. Does your AI technology provide such a "stop-button" that is able to override any operation? If so, what does this process look like?*"

4.2 GDPR analysis

As aforementioned, besides researching how small innovative companies researching AI currently comply to the AIA before its implementation, another part of the research is to investigate in what manner these companies currently comply to the rules and guidelines of the GDPR. Like the AIA, the GDPR takes on a risk-based approach, in which possible risks, associated to how data from data subjects is being processed, are recognized. Unlike the AIA, the GDPR does not make any categorizations based on the perceived risk or any other aspect in regards to data processing.

When it comes to the processing of personal data through the use of AI technologies, there are several requirements that can be recognized that the innovative tech companies that research or provide of such technologies need to abide by in order to be able to properly mitigate the possible risks. These requirements can be divided into the following categories and serve as the base for the interview questions:

1. Understanding of the GDPR:

   In order for companies to be able to properly deal with processing personal data from data subjects, it is crucial for these companies to have a good understanding of the laws and regulations of the GDPR. It is important that this understanding is not just kept on a high level, such as to the CEO's of a company, but also made available to the various employees that are working for the company.

   According to Article 47(2)[18] of the GDPR, companies should provide employees with trainings in order to increase the awareness of data privacy protection of individuals amongst employees. This way, it will be clear throughout all levels of a company how personal data should be protected, handled and properly processed, and can therefore help diminish the risk of data being handled unfairly or unrightfully.

[18] Article 47(2) (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Also, without a clear understanding of the GDPR, it would be hard to recognize exactly what measures need to be taken within a company in order to ensure data protection [14]. When it comes to innovative companies researching or providing AI in the healthcare sector, it can therefore be considered important to investigate, as these companies often make use of health data, which is considered a special category of personal data. Investigating how these companies go about ensuring that the GDPR is properly understood and implemented is therefore of great importance. In order to be able to generate these insights, the following questions have been created:

- "*Do you believe the GDPR did a good job in informing your company what exactly needs to be done in order to be compliant?*"
- "*What was the company's experience implementing or adjusting to the rules and regulations of the GDPR?*"
- "*Has your company put any effort towards providing employees with data protection training in order to increase awareness of data privacy protection of individuals? If so, what does this training look like?*"

2. Processing special categories of personal data:

AI technologies are known to require large amounts of data in order to be able to properly train the respective algorithms and therefore in order to eventually be able to provide accurate results. When it comes to the use of AI in the healthcare sector however, the data required often consist of health data, which is data that provides information about a person's medical history.

However, according to Article 9(1) of the GDPR, the processing of special categories of personal data is prohibited, unless under some specific conditions (e.g. consent is given, it is necessary to carry out specific obligations) [7]. It is therefore very important to investigate how this measure affects innovative companies researching AI for the healthcare sector, when it comes to accessing this data, as these AI technologies require health data from its data subjects.

As aforementioned, the necessary data can be accessed under certain circumstances, such as in case explicit consent is given by the data subjects or in case the data is needed for the sake of fulfilling a specific legal ground [7]. It is therefore also important to investigate under what legal ground these companies aim to access and process the respective data. In order to get a better understanding of how these companies go about accessing these special categories of personal data, the following questions have been generated:

- "*Under Article 9 of the GDPR, the processing of special categories of data is prohibited, unless explicit consent is given or it is necessary to carry out specific obligations. Do these requirements hinder the company's ability to access the needed health data for the AI technology of your company and how easy would you say it is to access this data? If so, how?*"

- "*What has your experience been accessing the necessary health data for the AI technology your company provides?*"
- "*What has your experience been setting the legal ground on which you process your health data?*"
- "*Under what legal ground do you process the health data?*"

3. Data subjects' rights:

As aforementioned, being subjected to the use of AI technologies, often means having to disclose sensitive forms of personal data, which in the case of the use of AI in healthcare, often consists of medical, or more generally, health data.

Under the GDPR, specifically the Articles 15-18[19] and Articles 20-22[20], the data subjects are given the right to obtain information about the data that is being collected and processed from them (e.g. the right to access, delete, rectify, object, restrict, data portability and object automated decision making and profiling). It is necessary for innovative companies that are researching or providing AI in the healthcare industry to allow the data subjects that are subjected to the use of these technologies, to exercise their rights. Investigating how these companies allow data subjects to exercise their given rights is therefore of importance, as this data is considered necessary in order to provide an AI technology that generates accurate results. The following questions have been created in order to provide more insights when it comes to how these companies allow data subjects to exercise their rights:

- "*How well do you believe your company is able to deal with such requests?*"
- "*Do you believe the GDPR provides sufficient information when it comes to how to properly respond to such requests?*"
- "*Was there any right that was considered the easiest or the hardest to implement? If so, why?*"

4. Privacy by design and default principle:

According to Article 25[21] of the GDPR, the privacy by design and default is considered important, which means that every new project revolving AI technologies for example, should be provided with the necessary organizational and technical tools and measures in order to ensure data protection (e.g. data minimization, pseudonymization etc.) [18]. This is in order to ensure that the personal data of patients is not accessible to any unauthorized users, cannot be further linked to other information of the patients and that only the necessary data is being processed for

[19] Articles 15-18 (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[20] Articles 20-22 (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[21] Article 25 (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

the sake of fulfilling its originally intended purpose [8]. It is therefore important to investigate how innovative companies researching or providing AI in the healthcare sector go about ensuring the data protection of data subjects, and therefore what measures are implemented within the company. In order to be able to generate these insights, the following questions have been created:

- "*How have you implemented the privacy by design and default principle?*"
- "*What was your experience implementing these measures into your company?*"
- "*Has a lack of resources such as money, expertise or time ever affected the ability to adhere to the data protection requirements of the GDPR?*"

5. DPIA:

The need for a Data Protection Impact Assessment (DPIA) is clarified in Article 35[22] of the GDPR. The GDPR clarifies that this assessment is necessary for any form of processing that could be considered high-risk, of which the use of health data. This DPIA serves as a measure that allows for identifying the possible risks that could occur when processing personal data of data subjects, while also ensuring the identification of ways in which these identified risks can be mitigated. It is therefore of importance that companies have a good understanding of how to conduct such a DPIA and what exactly the content needs to be. In order to be able to generate these insights, the following questions have been created:

- "*Would you say that it is clear exactly when and under what circumstances it is necessary to conduct a DPIA?*"
- "*Would you say that it is clear exactly in how much detail the content of the DPIA needs to be described?*"
- "*Have data privacy concerns ever resulted in a change of project plans?*"

6. Record keeping:

Article 30[23] of the GDPR clarifies the need for record keeping when it comes to processing activities, in order for companies to have a clear overview of the data flow throughout the company. Record keeping is a great way to ensure data protection, as well as accountability, as it allows for a clear overview of what exactly is done with the processed data and by who. It is therefore important to investigate how innovative companies researching or providing AI in the healthcare sector go about the record keeping of the various processing activities they perform. In order to be able to generate these insights, the following questions have been created:

---

[22] Article 35 (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[23] Article 30 (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

- "*Would you say the GDPR makes it is clear how exactly these records need to be formatted?*"
- "*Would you say that it is clear how exactly these records need to be maintained and kept up to date?*"
- "*How exactly do you maintain and update these records?*"

7. Supervisory authority:

According to Article 33(1)[24] of the GDPR, it is necessary for companies to notify the supervisory authority in case of a breach of personal data within 72 hours. In case a data breach of any kind occurs within a company that provides AI technologies for the healthcare sector, this would mean that the health data of the data subjects is at risk of being misused by unauthorized parties. It is therefore of importance that companies have a procedure in place that clearly explains in what manner needs to be handled, as well as who needs to be contacted in case such a situation occurs. The following questions have been created in order to provide more insights when it comes to how innovative companies researching or providing AI in the healthcare sector go about dealing with such possible scenarios:

- "*Would you say the GDPR provides sufficient information when it comes to exactly how this communication process should take place?*"
- "*What was your experience setting up such a communication plan*?"

4.3 The differences between the AIA and the GDPR

Now that a clear overview has been given when it comes to the relevant aspects of both the GDPR and the AIA in regards to how innovative companies can research or provide AI in the healthcare sector, while complying to both the respective regulations, it is important to investigate what exactly the differences are between these regulations when it comes to how the use of AI is regulated.

The regulation of AI

As aforementioned, both regulations take on a risk-based approach, with the AIA recognizing possible risks, associated to the use of an AI technology. The AIA additionally categorizes these risks into four different categories, namely minimal risk, limited risk, high-risk and prohibited AI technologies, whereas the GDPR takes a more general approach, and instead of specifying exactly which technologies need to be

[24] Article 33(1) (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

regulated, it addresses possible issues or risks that might occur when it comes to the processing of personal data from data subjects [8].

The AIA:

When closely investigating the AIA, it becomes clear that a large emphasis is placed on the proper monitoring and regulating of AI technologies that are considered high-risk, as the vast majority of additional requirements that are added to the AIA are geared towards the high-risk AI technologies. The only other requirement added is geared towards the use of AI technologies that are considered to be of limited risk, and this requirement solely mentions to clearly communicate the interaction with a machine towards the users [2]. The AIA can therefore be considered an additional component next to the GDPR, as it clarifies in more detail exactly which AI technologies need to be regulated, and how these technologies need to be regulated.

When it comes to the scope of this research, which is set to the use of AI technologies in the healthcare sector, this means that the risk-based approach of the AIA is aimed to determine exactly under what circumstances the use of AI technologies can result in possible high-risk situations for the data subjects that are subjected to the use of these technologies. The AIA clearly describes what is considered a high-risk system and what is not, and also clearly describes the additional requirements that should be abided to when it comes to high-risk technologies, in an attempt to properly regulate the risks the use of such technologies might pose on the health or fundamental rights of the data subjects [22].

The GDPR:

As aforementioned, the GDPR takes a way more general approach, and instead of specifying exactly which technologies need to be regulated and which specific requirements are necessary to regulate the processing of personal data, such as the implementation of a risk management system or a post-market monitoring system like in the AIA, it addresses possible issues or risks that might occur when it comes to the processing of personal data from data subjects [23]. The GDPR is therefore aimed for the purpose of achieving compliance through increasing a sense of responsibility for the data controllers, by providing them with the necessary risk management measures to ensure this [8].

Another significant difference between the GDPR and the AIA that can be recognized is when it comes to the flexibility of the respective rules and regulations. The GDPR is known for its flexibility and interpretability, giving data controllers some “freedom” when it comes to how to implement the necessary data protection measures [8]. The AIA on the other hand can be considered more rigid in the way its requirements are set up, such Article 10 that provides clear requirements when it comes to how the AI technologies of high-risk systems need to be trained [8].

The use of health data:

Important to note, is also how the differences between these regulations when it comes to how the use of AI is regulated, affects the manner in which health data can be used according to both the GDPR and the AIA.

The AIA:

As aforementioned, the AIA proposes additional requirements that need be abided to, especially when it comes to high-risk technologies, which is what AI technologies in healthcare are often classified as, due to the possible risks it possibly poses when it comes to the safety and health of the data subjects [22]. Article 6 of the AIA clarifies under what conditions AI technologies are considered high-risk. Article 6(2) in particular, clarifies the use of health data to be considered high-risk, as the use of health data for AI technologies that are geared towards the healthcare sector, could pose possible high-risk situations when it comes to the health and even the life of the data subjects that are subjected to the use of these technologies. This affects the manner in which health data can be used within the AIA, as additional requirements are proposed, specifically for the use of high-risk AI technologies.

The AIA however, does not mention any requirements that are geared specifically towards the use of health data. Also, unlike the GDPR, the AIA does not specifically mention any general measures such as purpose limitation, data minimization or anonymization, and instead focuses more on technical aspects, such as the implementation of specific systems that are aimed to minimize the possible high-risk situations of the use of AI technologies that make use of health data.

When it comes to the use of health data for AI technologies geared towards the healthcare sector, which, as aforementioned, is categorized as high-risk in the AIA, several requirements are clarified, which have been earlier described in more detail in the AIA analysis section. In order to introduce an AI technology that is categorized as high-risk, and therefore in order to make use of health data, it is considered important that proper measures are set in place in order to ensure the quality of the health data (e.g. to ensure the representability and correctness of the data, as well as minimize possible biases), meaning that the relevant health data needs to be properly trained, tested, as well as validated, before it officially be used for the respective AI technology the acquisition of the data is intended for [22]. Before health data can be used, the AIA also clarifies the need for a risk management system that is able to identify the possible risks a specific AI technology, and therefore the processing of health data, can have. The AIA also clarifies the importance of disclosing such risks to the respective data subjects, before their personal health data is allowed to be processed for the use of AI in the healthcare sector. In order to use health data, it is also necessary that the AI technology is overseen by natural persons during its use, as it allows for the recognition of risks to health, safety or fundamental rights when the technology is in use [22].

The GDPR:

As has been mentioned, the GDPR does not categorize the possible risks AI technologies could pose. Instead, according to Article 4(15)[25] of the GDPR, health data is considered a special category of personal data, as it provides information about a person's health status, which could relate to either their physical or mental state. For the GDPR, it is especially Article 9(1) that forbids the processing of such sensitive information, unless it is based on legal grounds that are specified in Article 9(2) [23]. As health data belongs to this special category of personal data, it is crucial for this data to be handled with care, which is why processing health data is only allowed under specific conditions. These conditions mentioned in Article 9(2) allow for health data to be processed in case explicit consent is given by the data subjects. However, the GDPR also makes it possible to process and therefore make use of health data without the explicit consent of the data subjects. The use of health data without having to obtain explicit consent from the data subjects is allowed in case of a larger public interest in regards to the general health of the public, such as dealing with a global pandemic (e.g. COVID-19), protecting a data subject in a situations where explicit consent legally or physically cannot be given, health data that is already made public by the data subject themselves, the provision of healthcare services, such as having a specialist inform a medical practitioner about a patient's health status, dealing with legal claims , social protection and security laws, as well as research, archiving and statistic purposes [18].

In case any of these conditions apply, the processing of health data is allowed, and the general measures that are clarified within the GDPR will also apply for the use of health data. These measures have been identified and explained in the previous section, namely the GDPR analysis. The GDPR firstly clarifies that only the necessary health data in order to fulfill the determined purpose (e.g. the legal basis) can be processed. This means that purpose limitation is also considered a very important aspect within the GDPR when it comes to the use of health data. Furthermore, the GDPR also clarifies the implementation of sufficient security measures in order to ensure data protection, before any kind of data can be used and processed, such as the minimization of data, data anonymization, the notification of a supervisory authority in case of any data breaches, as well as ensuring that medical records of data subjects cannot be accessed by any unauthorized parties and are therefore recorded in a secure environment (e.g. the use of two-factor authentication). Lastly, before any health data can be used, the GDPR clarifies properly informing data subjects about the data that is used, as well as the rights these data subjects are allowed to exercise, such as accessing, deleting and restricting the use of their health data [23].

As aforementioned, the GDPR is considered to be more general and flexible in its approach of regulating data protection [8]. Unlike the AIA, the implementation of specific systems or documentations (e.g. risk management system, post-market monitoring, log system) that are needed before health data is allowed to be used and processed, is not clarified in the GDPR. Of course, the GDPR still clarifies the implementation of sufficient measures in order to ensure data protection, however,

[25] Article 4(15) (May 25, 2018) *The General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

exact measures are not specified. General measures, such as purpose limitation and data anonymization are specified, however, when it comes to how these measures need to be implemented, no specifications are clarified within the GDPR, unlike the AIA [23].

Now that some of the most significant differences between the GDPR and the AIA have been identified, it is safe to say the introduction of the AIA might bring forth beneficial insight when it comes to how AI, specifically high-risk, as well as the use of health data, can be implemented and used, while safeguarding the health and freedom of the data subjects that are subjected to these technologies. It might therefore help create more trust in the use of AI, and could help bring forth more acceptance when it comes to the adoption of AI in many industries. This increase of trust could therefore especially have an impact on the use of AI in the healthcare industry, where the safety of patients is especially important, as the newly proposed regulation has set up a more rigid form of compliance, compared to the more open for interpretation and flexible GDPR, especially on the topic of AI [19].

5 Interview results

Based on the results from the interviews, various insights in regards to both the experience of small innovative companies in the Netherlands when complying to the GDPR, as well as how such companies currently comply to the AIA before its implementation, have been generated. These results will be further discussed, starting from the experience of companies when complying to the GDPR.

5.1 Experience complying to the GDPR

As aforementioned, the scope of this research concerns several aspects of the GDPR, namely the general understanding of the GDPR, the processing of special categories of personal data, the rights data subjects have, the implementation of the privacy by design and default principle, conducting a DPIA, record keeping of all actions relating to processing and the notifying of a supervisory authority in case of a data breach of any sort. The interviews have provided the following insights in terms of how innovative companies researching AI for the healthcare sector in the Netherlands experience complying to these various aspects of the GDPR.

Understanding of the GDPR:

When it comes to the general understanding of the GDPR within companies, opinions seem to vary when it comes to how well the GDPR is able to inform companies when it comes to what exactly needs to be done in order to be considered compliant, as can be seen in *Figure 1*. The majority of the companies however, do all mention the ambiguousness of the GDPR and how many aspects of the GDPR could be left open

for interpretation. For some companies, this was mentioned as a positive aspect, as it allows for own interpretations and therefore freedom to apply the GDPR in such a way that seems fit for the company. Company 3 mentions:

"*When regulations are published it is always hard to interpret, because even enforcement agencies can interpret it differently. But at some point, as a company you just have to make the decision for yourself where you set the bar and with the plenty of existing guidance and through monitoring the market and competitors, we decide if we have set the bar correctly, or whether we need to do more or less*."

Interesting to note is that all companies also mention the use of other regulations such as the ISO standards (e.g. ISO 27001, ISO 29134) the Medical Device Regulation or the In-Vitro Diagnostic Regulation (IVDR) as guidelines to help interpret and also implement similar aspects of the GDPR, as those guidelines are often considered a bit more specific. Company 2 mentions:

"*The GDPR is a bit vague, but you have the ISO standards, for example ISO 27001, which often are a lot clearer, however these cannot be super specific, otherwise they cannot be used by thousands of companies so there is always some vagueness in it. It does however provide a lot more clarity than the GDPR, especially when it comes to information security*."

When considering the general understanding of the GDPR within companies, the general awareness of data privacy protection between employees also needs to be considered. All companies mention providing some form of training for employees when it comes to increasing the awareness of data privacy protection. These forms of training vary from more formal on boarding training, together with yearly awareness trainings, to more informal trainings, such as close communication with the product development leader and the rest of the team on the topic of how personal data and data privacy should be dealt with within the company. As far as the experience of increasing this awareness within the company concerns, which can be seen in *Figure 1*, most companies mention that it is considered a relatively easy process. This is with the exception of Company 3, which mentions:

"*I think it is hard because the total load of compliance is very high so it takes a lot of resources away from the rest of the company. Why should we spend so much resources on compliance?*"

Overall, despite the general consensus of the ambiguousness of the GDPR, all companies consider themselves to be sufficiently GDPR compliant. However, an aspect mentioned by the vast majority of the companies is the way a lack of resources, such as time, expertise or money, affects how these companies go about complying to the GDPR. It is mentioned by these companies that often times, other regulations such as the IVDR and the MDR, are prioritized over the GDPR. These companies therefore also clarify to often make use of the least amount of resources necessary in order to be considered compliant. Company 4 mentions:

"*Complying to the GDPR and all the other regulations takes up a lot of resources. Because of limited resources, we are always looking for the kind of way to implement a particular rule with the least amount of resources, which sometimes means that you might be following the latter of the law. We have something in place so we can check that off of the box so we meet that requirement and the auditor is happy, however it is not necessarily a very helpful way of implementing it. That is more the focus instead of something that would actually be useful for the users."*

The processing of special categories of personal data:

More than half of the companies mention that the requirements of the GDPR in regards to the processing of special categories of personal data, affects their ability to access the needed health data for the AI technology they provide, as can be seen in *Figure 1*. These companies argue that, in order to deal with these restrictions and work around them, they spend a lot of their time anonymizing and limiting access to health data as much as possible. It is especially this anonymization process that is mentioned by these companies to be very time consuming, especially since there are not yet large teams assigned to this task. Mainly the access to data that can be used for training the algorithms is mentioned as a struggle, which is why some companies mention other forms of accessing data, such as through using US data or purchasing data sets from trusted sources.

One company (Company 3) also mentioned that smaller, upcoming companies often struggle more with accessing the necessary data, as a sense of trust between hospitals and vendors (meaning the small innovative companies) is also crucial in order to be able to access data from hospitals, together with competitivity between vendors. Company 3 mentions:

"*In the beginning it is hard because hospitals do not know you and do not trust you yet because you have not yet made a name for yourself in the market. But over time, once you show the market that you have good products in place, it becomes easier to access this data. However, it is still difficult because it is competitors as well that want to have access to the data.*"

The remaining companies that do not seem to consider the requirements of Art. 9 of the GDPR in regards to the processing of special categories of personal data a challenge, mention no issues when it comes to accessing medical data from hospitals. Company 2 additionally mentions that Art. 9 (2)(h) of the GDPR allows for the access of special categories of personal data when it is for the sake of preventive medical diagnoses.

When it comes to deciding on the legal basis, on which personal data is being processed by companies, all companies state to not have experienced any specific trouble setting this legal ground, and mention to process the necessary health data either on explicit consent or for the sake of preventive medical diagnoses.

The rights of data subjects:

All companies claim to find no difficulty in dealing with requests of data subjects when it comes to their right to obtain information about the data that is being collected and processed from them. The vast majority of the companies however, mention that this is mainly because these requests go through the respective hospitals that make use of the AI technologies these companies provide. It is therefore very rare for the companies to get such requests, as most of these companies claim to primarily take on the role of the processor and therefore processes the personal data in the name of the controller. However, despite rarely receiving such requests, all companies do clarify to be able to deal with any requests, if needed, well enough, as can be seen in *Figure 1*. Company 4 mentions:

"*The right to be forgotten is extremely rare and usually just happens because a nurse entered a wrong patient. It is rare for us to get any requests. It is usually the hospitals and in turn they might ask us to submit our part of that information, however I do not think that happens often.*"

The implementation of the privacy by design and default principle:

When it comes to how companies have implemented the privacy by design and default principle, all companies state to work with data on an anonymized level, to ensure the data cannot be linked to any natural person. Besides anonymizing, companies clarify that time is also spend on data minimization, through carefully assessing the purpose of the data and whether it is necessary for the purpose of the technology they provide. For some companies, this process was not described as very difficult. Company 1 mentions:

"*We describe the types of data and analyze the purposes of each of the data and we discuss whether we really need the data for the outcomes or whether we can use the system without this data. It is assessed by the development teams that take different kinds of data they think could be useful in the future. We sometimes need to explain to them that you can only process data that are necessary at the moment and not data that you somehow might need in the future. It is not so difficult, you just take out few of the data that you do not need.*"

However, while for some companies, the privacy by design and default principle is not considered a hard aspect to implement, other companies do clarify to struggle with its implementation, as can be seen in *Figure 1*. These companies mention that it is often the high volume of data, together with the regulatory bodies that strictly go about ensuring that no key can be found that can end up linking to a natural person, that make the implementation of the privacy by design and default aspect of the GDPR challenging. This also ties into the aforementioned problem that smaller companies face when it comes to a lack of resources, such as the employees that can be assigned towards this task. Company 3 mentions:

"*This is where the data team is important that consists of about 6/7 people. They analyze data we have and mark and anonymize it. Where we can, we try to anonymize it so that there is no kind of linkage, that is our core strategy. It is not easy, we have a lot of records from all the different records, really thousands, and it is only 6/7 people working to anonymize this, so costs a lot of time and effort but this is the only way to do this correctly, so that you know what truly happens with the data.*"

Conducting a DPIA:

When it comes to the conduction of a DPIA, there seems to be quite differing experiences, as can be seen in *Figure 1*. As some companies take on the role of a processor, these companies clearly mention to not have made a DPIA assessment. However, interestingly, one company (Company 2), despite taking on the role of the processor, clearly mentions to conduct this assessment. Company 2 mentions:

"A *DPIA only needs to be created by the controller. What should be included in the GDPR is not really clear in my opinion, it is generally described. However, there is ISO 29134 for it and it is written a lot clearer and in more detail. Hospitals find it more difficult because we have implemented all security and technical measures that they do not necessarily know about or have access to, so what we have done is to make a DPIA, even though this is not necessary as a processor and hospitals often ask for it to see if we have adequate protection.*"

Other companies also all clearly mention that other regulations, such as ISO standards and the MDR provide more and also clearer information on how to conduct a DPIA assessment, as opposed to the GDPR that is mentioned to be quite vague.

When it comes to data protection concerns that might occur during a project, most companies mention to not recall any moment where privacy concerns have led to a change of project plans. The two companies that do clarify to have such an experience, clearly mention this to have happened in the very early stages of development and either had to do with receiving too much information from a client or deciding on what data to store. Company 4 mentions:

"*I think definitely where we said that we would like to store certain data of a patient, but it was very tricky to get consent or find a good cause on why to store this data. It was something that had to do with medical devices where we would have to get the data from a third part like Apple Watch and that had some privacy concerns. This usually happened in an early stage, so before fully starting the project is when these discussions took place.*"

Record keeping of all actions relating to processing:

When it comes to the record keeping of all actions relating to processing, most companies mention the GDPR to be relatively vague when it comes to how to go about

record keeping and how to maintain and update these records, as can be seen in *Figure 1*. This is why these companies clarify to look at other sources, such as data protection boards, supervisory advice, as well as other regulations such as the MDR. Company 4 mentions:

"*I think our company spends little time on record keeping for GDPR and are more focused on record keeping for MDR and others. And it might be that those overlap sufficiently to just look at the other standards.*"

How this record keeping process is implemented, is mainly through the implementation of a data processing registry, or any other form of a list that is able to register what data is recorded for each of the data subject. Company 1 mentions:

"*We made a table or list what should be recorded for each of the subject and each of the data. In the beginning we prepared the privacy policy and based on this policy we are recording the personal data, because it depends how long their prescribed purpose is. In the system, the data is recorded based on the privacy policy because when the policy is updated, then the system needs to be updated as well.*"

The notifying of a supervisory authority:

When it comes to notifying the supervisory authority in case of a data breach, all companies clarify to have set up some sort of procedure of what needs to be done and who needs to be contacted within the company in case a data breach happens. For some companies this procedure is based on a clearly set up communication plan, whereas other companies state to not yet have implemented a very formalized plan as of yet. However, all companies mention this procedure to be very clear and well known within the company, where it is usually the DPO or any legal counsel or responsible person within the company that is contacted first and decides on what steps to take next based on the situation. Company 3 mentions:

"*We have a procedure in place. First, is always to contact the DPO and based on certain criteria it can escalate to management to see what we are going to do with this. There are more steps on how to deal when something goes wrong with the data. So, there is a plan but currently it needs to be formalized a bit more, we are working on getting all the procedures and templates correct. But within the company it is clear what needs to be done when we have such breaches if something does go wrong with the data.*"

In order to get an overview of the aforementioned results in regards to the experience of the innovative companies when it comes to complying to the GDPR, the following diagram has been generated:

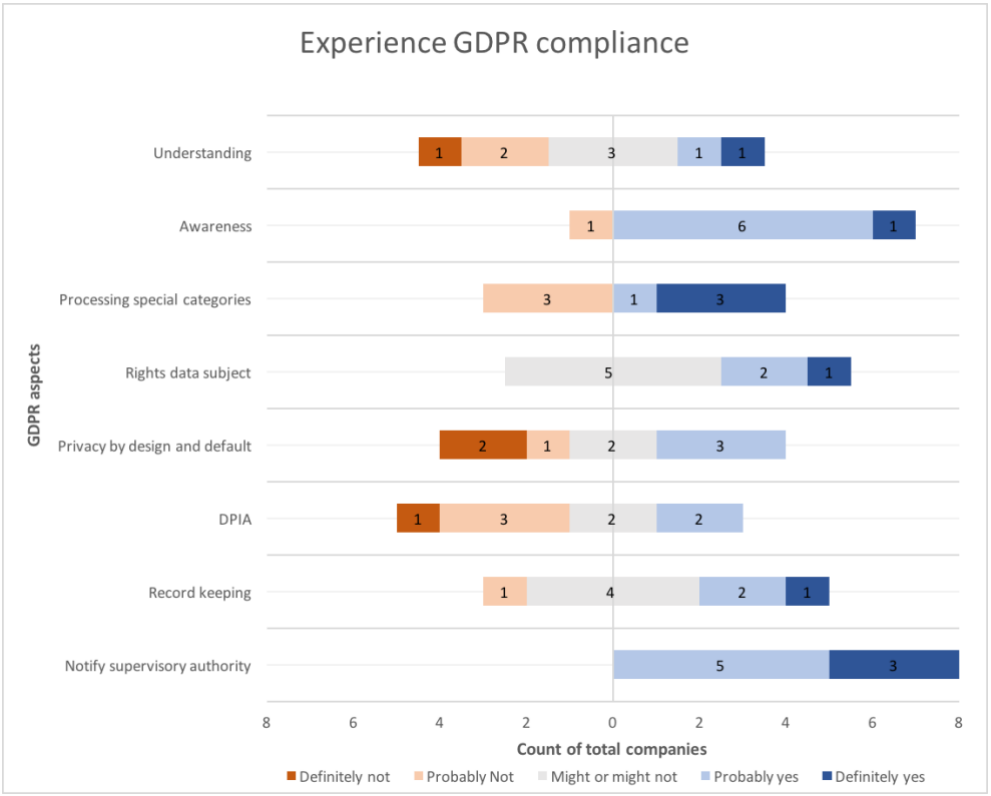

Figure 1. Experience GDPR compliance.

5.2 Compliance to the proposed AIA

Now that the insights in regards to how small innovative tech companies researching AI for the healthcare sector in the Netherlands experience complying to various aspects of the GDPR have been discussed, the interview results when it comes to such companies currently comply to the AIA before its implementation, will be discussed. As aforementioned, the scope of this research concerns several aspects of the newly proposed AIA, namely the implementation of a risk management system, post-market monitoring system, technical documentation, how data is governed and managed, how security, accuracy and robustness are ensured, and the implementation of a log system and human oversight measures.

The interviews have provided the following insights in terms of how innovative companies researching AI for the healthcare sector in the Netherlands have implemented the aforementioned aspects of the AIA, before its implementation.

The implementation of a risk management system:

All companies mention to have some form of a risk management system in place that is able to identify and analyze possible risks that might occur from the use of their specific AI technologies, as can be seen in *Figure 2*. The companies all mention this system to be used on a daily basis and the majority of the companies mention to follow relevant ISO standards such as ISO 13485 and ISO 27001 as guidelines for their risk management system. Company 2 mentions:

"*There are procedures in place for risk management, mainly based on the medical regulations. From a medical point of view, we have ISO standards to comply with, also for risk management. Extensive risk management is in place because it is very important, as it is the backbone of ensuring that the device is safe. It is very broad, so from product safety for patients, to the algorithms to the security.*"

When it comes to the use of standard risks, the companies all mention security risks, clinical risks and usability risks that are always considered. When it comes to implementing a risk management system, the majority of the companies clarify that it is extremely important for risk management systems to be updated as well, in case a product has been changed in any way, in order to ensure that it will still be possible to identify possible risks of the use of the system. Company 3 mentions:

"*The core of the product will not change, we might make changes to the algorithms. We have procedures in place and based on the procedures we say whether we need to have a risk management plan for each product (also for each revision of a product). In case of a revision, we will utilize what we have done in the past but we will update it based on the changes that have been made in the product to ensure that also the risk management documentation align with the changes that are made in the product*."

The implementation of a post-market monitoring system:

All companies also mention to have some form of a post-market monitoring system in place, as can be seen in *Figure 2*. Three of the companies clearly mention to have set up this system based on the guidelines of the MDR, as it is considered a requirement for the company to comply with the guidelines of the MDR. These companies split up the post-market monitoring process in two different aspects, namely active and passive forms of monitoring. Active monitoring refers to closely analyzing competitors, databases etc. in order to get an overview of possible faults or problems that could possibly relate to the device that is used by the company. Passive monitoring however, is mentioned to refer to the feedback given by health specialists and therefore helps assess the performance of the device in practice. For the remaining company, the monitoring process can also be split up in the same manner, however, the company additionally mentions to make use of software usability surveys that patients fill in. Company 2 mentions:

"*It can be passively monitored. The requirements for this are described in the MDR. We also have feedback from radiologists that we receive in case they see anything*

strange. However, we also actively monitor and have set up studies that actively look more at the literature or at certain databases whether adverse events are reported. Through these databases or literature, you can look at whether there are any problems that could relate or be relevant for the type of device we use and then you can analyze whether it may or may not be a problem for us."

The publication of a technical documentation:

When it comes to the publication of a technical documentation, all companies clarify to publish details when it comes to the different data that is used and how the used algorithms work exactly. These details are mentioned to be documented and published in the form of scientific publications, such as papers or journals. Company 3 mentions:

"*We have a lot of publications in order to know how it works, more than 30 for our devices and how it works in practice. We have documentations of how the algorithms specifically work. Since we use Machine Learning (ML), we describe how the algorithm is made, how we ensure that there is no bias etc. So, there is a lot of documentations to ensure that the algorithms are in place, and this serves two purposes, one is for ourselves in case someone new joins the company, so they can see how everything works, however also for requirement reasons, for the MDR we need to explain to external people (ex. FDA, notified bodies) how our algorithms work.*"

However, when it comes to details about the source code, all companies mention to not have this information publicly available, as can be seen in *Figure 2*. This is an interesting finding, as the source code is not specifically mentioned in the AIA, and is also considered the only aspect all companies clearly claim not to have implemented. Company 3 specifically mentions why this is the case:

"*We do not share this information publicly, because this is our proprietary knowledge and the core of the company, we have it internally but not publicly."*

The implementation of appropriate data training, testing and validating measures:

All companies state to thoroughly test the AI technologies they provide before they are implemented. This process can be characterized into two different aspects for each of the companies, namely a technical part and a medical part. The technical part is mentioned to refer to various tests in regards to software, such as immigration tests, unit tests or whether the algorithms and data flows function properly, that are conducted by the engineering team within the company. The medical part is mentioned to refer to whether the software requirements, meaning what exactly the software needs to be able to do, are able to fulfill the user requirements, and is checked by medical professionals in order to ensure that the recommendations made by the systems are actually accurate. Company 4 mentions:

"*We have technical testing within the engineering team and we have medical people like former doctors for example, who are testing the content of the product to see whether the recommendations make sense.*"

In terms of data, the companies clarify that access to large amounts of data is crucial when it comes to being able to properly train the algorithms of the respective AI technologies and therefore also in order to avoid possible biases and other shortcomings. The companies mention buying data sets from reliable sources as one possible way to access the needed data for properly training the algorithms. However, the companies also mention having an internal team of medical professionals who annotate the scans, which also serves as part of the testing process before the system is actually used in practice and therefore also helps assess the suitability of used data sets. Company 2 mentions:

"*You can have a dataset, but that does not mean you can train an algorithm. Scans of lung nodules, for example, must be annotated. We have our own tool that allows radiologists to annotate. There is a technical aspect to this, which checks whether we can use the scan at all. In addition, we always look at what kind of algorithm we want to build and whether the scan is clinically applicable for that.*"

This is with the exception of Company 4, who clearly states to currently use very limited algorithms and therefore make use of health assessment index scores in order to help indicate possible biases or inconsistencies within the data.

The implementation of appropriate accuracy, robustness and security measures:

When it comes to ensuring accuracy, robustness, as well as security, all companies clarify to have implemented the appropriate measures needed to ensure this, as can be seen in *Figure 2*. Measures mentioned by the companies vary, from having a dedicated internal team that reviews all the data and makes sure that it cannot be accessed by any unauthorized users through two-step verification, to third party companies that work together with internal teams and perform monthly penetration tests. Company 3 mentions:

"*We have a data team of 6/7 people. For us this is quite large team and there is a process in place of reviewing data and making sure that it is stored in the right place where it cannot be tinkered with and only limited access. That way we limit the possibilities of what could go wrong.*"

The implementation of a log system:

When it comes to the implementation of a log system that is able to record the operations of the respective AI technologies, all companies clearly mention that everything that has to do with the data of patients or practitioners, is logged and that access to these logs is strictly limited to only authorized persons through two-step verification, as can be seen in *Figure 2*. Company 4 mentions:

"*The architecture of the software is very event based, so everything that happens through a patient or a practitioner results in an event and all these events are logged.*"

However, when it comes to the amount of time these records are stored, the companies mentioned this to be very dependent on the hospitals they are in contract with, however a general time period of ten years was given. Company 4 mentions:

"*I think the mandatory time is about ten years, but it also depends on the hospital, because they are the ones that have the patients sign the agreements. So, it is in close contact with the hospitals because they are the ones that are in charge of those records and we just have to maintain them in order to have the hospital meet its requirements.*"

The implementation of human oversight measures:

When it comes to implementing human oversight measures, all companies have clarified to have implemented measures within the company in order to ensure human oversight. However, two of the companies in particular mention this human oversight process to not be one that is very formalized and extensive as of yet. Company 3 mentions:

"*I think it is very limited, they look in the right place and see whether everything is as it should be and what recent changes have been made and I think that is about the extent it goes to.*"

Company 4 gave a similar response namely:

"*I think there is a procedure where a person is supposed to check backups every month. But I do not think it is a very involved process. It is more a courtesy check to check if it is okay because it is difficult to verify the accuracy in detail. It is engineered in and guaranteed in design but not so much verified after*.

In order to get an overview of the aforementioned results in regards to the implementation of the proposed AIA by the interviewed innovative companies, the following diagram has been generated:

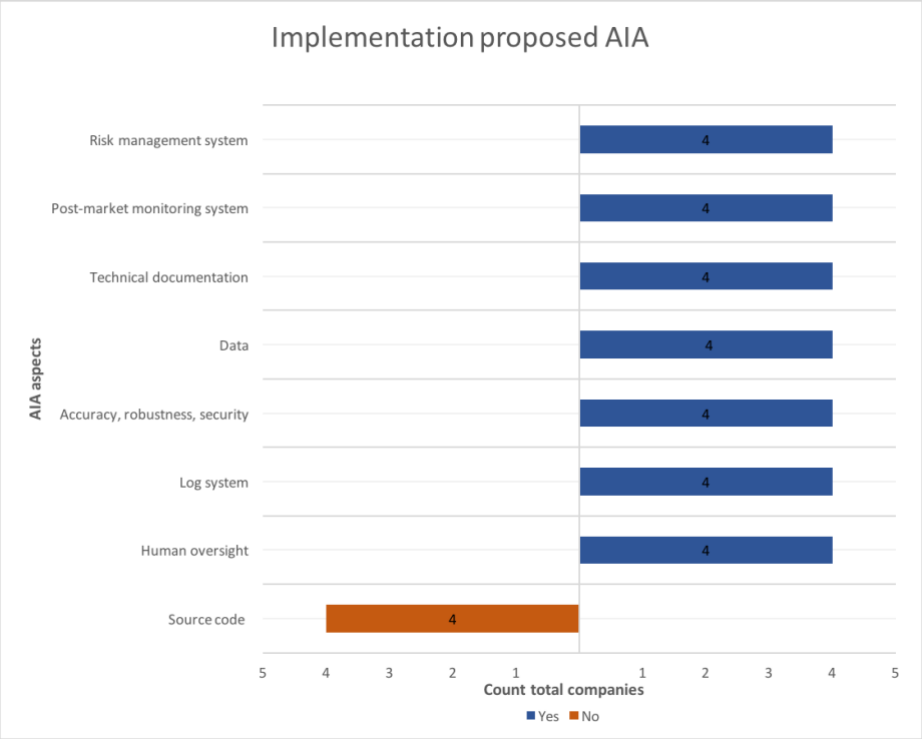

Figure 2. The implementation of the proposed AIA.

6 Discussion

6.1 Research goal

The aim of this research is to investigate in what manner small innovative tech companies in the Netherlands can conduct AI research on healthcare data while being compliant with both the AIA and the GDPR. In order to achieve the necessary insights, several companies that research or provide AI in the healthcare sector have been interviewed, in an attempt to get a better insight of what their experience is when it comes to trying to comply to the GDPR, while conducting AI research on healthcare data, as well as how these companies currently comply to the AIA, before its implementation. Before answering this main question however, it is important to first have a good overview of both the GDPR and the AIA, and understand what exactly the differences between these regulations are when it comes to regulating AI, as well as the use of health data.

Both the GDPR and the AIA take on a risk-based approach, with the AIA recognizing possible risks, associated to the use of an AI technology. The AIA additionally

categorizes these risks into four different categories, namely minimal risk, limited risk, high-risk and prohibited AI technologies, whereas the GDPR takes a more general approach, and instead of specifying exactly which technologies need to be regulated, the GDPR simply addresses possible issues or risks that might occur when it comes to the processing of personal data from data subjects.

When it comes to the use of health data, it is important to note that there are not necessarily any specific regulations for both the AIA and the GDPR. For the AIA, AI technologies that make use of health data are considered high risk. This is defined in Article 6 of the AIA, where the use of AI that could pose possible risks when it comes to the health and even the life of the data subjects, is specifically defined as high risk. The use of health data for AI therefore falls under this category, as the manner in which a person's health is diagnosed or monitored etc. could result in possible life or death situations.

In case a technology is deemed high risk according to the AIA, additional requirements come into play that companies have to abide by. For companies researching or providing AI that makes use of health data and are therefore considered high risk, it is necessary to have implemented the several aspects, and that is a risk management system that can identify the risks of the respective AI technology, a post market monitoring system that ensures the AI technology operates accordingly, proper data governing and managing principles, a log system that is able to log all operating activities and human oversight measures.

For the GDPR, according to Article 4(15) of the GDPR, health data is considered a special category of personal data, as it provides information about a person’s health status. As aforementioned, these special categories can only be processed or used according to Art. 9 of the GDPR under several specific legal bases, the most relevant ones being the use of explicit consent and the provision of healthcare services. In case any of these conditions or legal bases apply, the processing of health data is allowed, and the general measures that are clarified within the GDPR will also apply for the use of health data.

In order to make recommendations when it comes to how manner small innovative tech companies in the Netherlands can conduct AI research on healthcare data while being compliant with both the AIA and the GDPR, it is also important to understand how these companies currently comply to both the GDPR and the AIA. Having a good understanding of a company’s current situation, allows for the identification of way to improve possible issues when it comes to researching or providing AI technologies geared towards the healthcare sector.

Experience complying to the GDPR:

For the first part, namely the experience of companies when it comes to complying to the GDPR, eight different companies have been interviewed in order to get a better understanding of possible struggles they face when it comes to being able to research

or provide AI technologies in the healthcare sector. Initially, before conducting the research, it was assumed that mainly Article 9 of the GDPR, the processing of special categories of personal data (e.g. health data), would prove to greatly affect companies when it comes to their ability to access the necessary health data in order to properly train and eventually use their respective AI technologies.

However, research has shown that opinions greatly vary. Some companies do not experience any trouble accessing the necessary data, as measures such as processing based on explicit consent of patients, buying data sets from trusted sources, as well as anonymizing and limiting data access are seen as sufficient measures to satisfy the volume of data that is needed for their respective AI technologies. Other companies, however, mention the anonymization process of data to be very time consuming, as these companies often do not have dedicated teams assigned that can deal with this process. Also, when it comes to accessing the necessary data, companies also mention that a sense of trust is also considered very important, as hospitals need to trust in the product that is provided, which is often considered quite hard for relatively small companies that have not yet made a big name for themselves.

In general, all companies claim to sufficiently comply to the laws and regulation of the GDPR and mention the importance of compliance in order to ensure hospitals and patients of a safe product. When it comes to conducting AI research on healthcare data, the majority of the companies mention it to be a process that gets easier over time through trial and error. Through experience and the many guidelines and information available, the companies mention to be able to navigate their way on how to properly conduct AI research on healthcare data. However, an aspect mentioned by the vast majority of the companies is the way a lack of resources, such as time, expertise or money, affects how these companies go about complying to the GDPR. As the GDPR is known for its interpretability and "vagueness", many companies mention to use this flexibility to their advantage, and only implement measures necessary to comply to the so-called "bare minimum", which is often mentioned to be due to a lack of prioritization of the GDPR, compared to other regulations such as the IVDR or MDR.

Compliance to the AIA, before its implementation:

For the second part, namely the manner in which companies currently comply to the laws and regulations of the proposed AIA, four companies have been interviewed in order to get an overview of how these companies currently comply to the AIA, before it is officially implemented. As these companies make use of health data for their respective AI technologies, these AI technologies fall under the high-risk category of the AIA, which is the scope of this research as aforementioned. As the AIA is currently still considered a draft and therefore not yet implemented, it was initially assumed that most companies would most likely not yet have properly implemented many aspects of the AIA in much detail. However, research has shown that most aspects of the AIA, have been implemented. The results also show however, that this is mainly due to the overlap between the AIA and other medical regulations, such as the IVDR and the

MDR, that also provide similar rules when it comes to, for example, the implementation of both a risk management and a post-market monitoring system.

Due to the existence of earlier implemented regulations that require similar measures to be taken as the AIA, the majority of the companies seemed to have already implemented many of the AIA aspects in quite high detail. However, when it comes to the proper human oversight measures, most companies actually mentioned to not have implemented very formalized measures as of yet, although the companies do mention having natural persons oversee their respective AI technologies. Also, when it comes to the implementation of a log system, many different ways have been identified when it comes to how this log system has been implemented, from more formalized to less formalized manners. Another interesting insight when it comes to the implementation of a log system, was that there is often still some unclarity when it comes to how long the records are stored, which was mainly explained to be because of the close relationship with hospitals, who are often the ones that are in charge of the data.

6.2 Recommendations

Now that it has been recognized how innovative companies in the Netherlands, that are researching or providing AI for the healthcare sector, go about complying to both the GDPR and the AIA, it is now possible to recognize potential recommendations when it comes to the main research question, namely "*In what manner can innovative tech companies in the Netherlands conduct AI research on healthcare data while being compliant with both the GDPR and the AIA?*".

As aforementioned, trust is considered an important aspect, not only when it comes to the adoption of a respective AI technology in the healthcare sector, but also way before that, when it comes to the development phase, as these technologies need to be trained with a large volume of data in order to eventually be able to provide accurate results. In order to achieve this level of trust, there are a few measures that have been identified to be especially important, and are therefore measures that especially need to be considered by companies researching or providing AI in the healthcare sector.

The first measure that can be recognized is to have a proper implementation of the privacy by design and default principle, and therefore ensure to properly anonymize and minimize the needed health data. Ensuring that personal data is being handled with care and is only used for the necessary purposes, can increase the willingness of hospitals or other healthcare providers to make use of AI technologies, allowing them to share the necessary health data of their patients with the respective companies.

Another measure to be especially mindful of that could greatly improve a company's ability to researching or providing AI for the healthcare sector, is the publishing of technical documents. This is another important measure that can greatly improve trust between healthcare providers and AI technology providers as it shows a sense of transparency, and provides healthcare providers with the necessary information about

how the AI technologies operate exactly, as well as what data is used and how this data is protected.

Although compliance to the GDPR is already mandatory, whereas compliance to the AIA is not as of yet, for a small innovative company that might not have all the necessary resources to implement all rules and regulations on a higher scale than "just sufficient", putting a large focus on especially the aforementioned aspects might make a difference when it comes to researching or providing AI for the healthcare sector and might help further increase the trust between healthcare providers and AI technology companies.

6.3 Limitations

When it comes to discussing the findings of a research, it is also important to recognize possible limitations that could have proven to have affected the insights generated from the research.

One of the first limitations of the research that can be recognized, has to do with the fairly limited sample size on which the findings are based. This is especially the case for the AIA part of the research, which was based on the findings generated from four different small innovative companies in the Netherlands that are researching or providing AI in the healthcare sector. When it comes to the results, there does seem to be some consistency when it comes to how these companies go about implementing aspects of the AIA. However, it is undeniable that a possible larger sample size might have resulted in even more interesting or even conflicting results. Also, important to note is that the scope was limited to the respective companies that reside in the Netherlands, which could prove to have some implications when it comes to the challenges that these companies might face, as a larger scope consisting of companies from multiple countries might help identify other possible challenges these small companies might face.

Another limitation that can be recognized, has to do with the fact that the AIA is not yet a regulation that has been implemented. At this point, the regulation is considered a draft, meaning that it is currently very plausible for aspects of the AIA to change by the time it is actually implemented.

Lastly, a limitation that can be recognized, has to do with the fact that other relevant regulations, such as ISO standards, the IVDR and the MDR are not included in the scope of the research. The results have shown that these regulations do have an impact when it comes to how companies go about complying to both the GDPR and the AIA. However, in order to keep to scope of the research more concise, these implications have not been included in the generated results and insights of the research, which could be a good initiative when it comes to possible future works.

7 Conclusion

When it comes to how small innovative tech companies in the Netherlands go about complying to the rules and guidelines of both the GDPR and the AIA, it can be concluded that these selected companies comply sufficiently to the GDPR, as well as most aspects of the AIA.

Although the GDPR is known for its "vagueness" and interpretability, most companies do mention to manage fine when it comes to researching and providing AI in the healthcare sector. This is mainly mentioned to be because of already existing guidance and information, such as advisory boards, publications of competitors and other existing regulations that are mandatory to abide to as well. However, a recognized issue when it comes to compliance to the GDPR is that it is often not prioritized, leaving companies to only implement the necessary measures in order to be considered sufficiently compliant, which is also a factor that takes into place because of the often-limited resources these small innovative companies have.

As far as the AIA concerns, it can be concluded that the respective companies seem to sufficiently comply to most aspects of the AIA, which can be explained by the overlap between the AIA and other, already implemented, regulations. Compared to the "vagueness" of the GDPR, the AIA is considered more straightforward in its approach, which could help improve the willingness to adopt AI in the healthcare sector.

Besides investigating how these companies go about complying to both the GDPR and the AIA, this research also aimed to identify possible recommendations when it comes to how AI companies geared towards the healthcare sector in the Netherlands can go about improving their ability to research or provide technologies based on the use of healthcare data. Properly anonymizing and minimizing data, as well as and providing the necessary information in regards to how the data is used might make a difference when it comes to researching or providing AI for the healthcare sector and might help further increase the trust between healthcare providers and AI technology companies.

Furthermore, important to note is that this research is limited to only innovative tech companies in the Netherlands, as well as a select few companies. The focus is also solely on the GDPR and the AIA, which means that the impact of other relevant regulations such as the IVDR and MDR are not considered. However, as much as these aspects can be considered limitations of the research, it provides a good framework for possible future research.

As for the scientific contribution of this research, a clear overview has been given when it comes to what exactly the relevant aspects of both the GDPR and the AIA are in regards to the use of AI in the healthcare sector, while highlighting the most evident differences when it comes to regulating the use of AI, as well as the use of health data. Furthermore, investigating specific AI technologies, through conducting interviews with small innovative tech companies in the Netherlands additional insights have been obtained, especially in regards to how these companies exactly go about complying to

the GDPR and the AIA, which provides beneficial information about what can be done to improve how small innovative tech companies in the Netherlands can conduct AI research on healthcare data, that is not found through solely reviewing existing literature.

8 References

1. Alugubelli, R.: Exploratory Study of Artificial Intelligence in Healthcare. International Journal of Innovations in Engineering Research and Technology. 3, 1, 1–10 (2016).
2. Bergholm, J.: The GDPR and the Artificial Intelligence Regulation – it takes two to tango? (2021).
3. Bessen, J.E. et al.: GDPR and the Importance of Data to AI Startups. SSRN Electronic Journal. (2020). https://doi.org/10.2139/ssrn.3576714.
4. Britten, N.: Qualitative Research: Qualitative interviews in medical research. BMJ. 311, 6999, (1995). https://doi.org/10.1136/bmj.311.6999.251.
5. Davenport, T., Kalakota, R.: The potential for artificial intelligence in healthcare. Future Healthcare Journal. 6, 2, 94–98 (2019). https://doi.org/10.7861/futurehosp.6-2-94.
6. Ferretti, A. et al.: Machine Learning in Medicine. European Data Protection Law Review. 4, 3, (2018). https://doi.org/10.21552/edpl/2018/3/10.
7. Forcier, M.B. et al.: Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers? Journal of Law and the Biosciences. 6, 1, 317–335 (2019). https://doi.org/10.1093/jlb/lsz013.
8. Gellert, R.: The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual? Journal of Ethics and Legal Technologies. 3, 2, 15–33 (2021).
9. Jokic, K.: Concept of consent under the GDPR in the light of AI based medical diagnostic applications. Tilburg University (2021).
10. Knox, S., Burkard, A.W.: Qualitative research interviews. Psychotherapy Research. 19, 4–5, (2009). https://doi.org/10.1080/10503300802702105.
11. Martin, N. et al.: How Data Protection Regulation Affects Startup Innovation. Information Systems Frontiers. 21, 6, (2019). https://doi.org/10.1007/s10796-019-09974-2.
12. Mökander, J. et al.: Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation. Minds and Machines. 32, 2, 241–268 (2022). https://doi.org/10.1007/s11023-021-09577-4.
13. Mourby, M. et al.: Transparency of machine-learning in healthcare: The GDPR & European health law. Computer Law & Security Review. 43, 105611 (2021). https://doi.org/10.1016/j.clsr.2021.105611.
14. Norval, C. et al.: Data Protection and Tech Startups: The Need for Attention, Support, and Scrutiny. SSRN Electronic Journal. (2019). https://doi.org/10.2139/ssrn.3398204.

15. Pakdemirli, E.: Artificial intelligence in radiology: friend or foe? Where are we now and where are we heading? Acta Radiologica Open. 8, 2, (2019). https://doi.org/10.1177/2058460119830222.
16. Reddy, S. et al.: A governance model for the application of AI in health care. Journal of the American Medical Informatics Association. 27, 3, 491–497 (2020). https://doi.org/10.1093/jamia/ocz192.
17. Schryen, G.: Writing Qualitative IS Literature Reviews—Guidelines for Synthesis, Interpretation, and Guidance of Research. Communications of the Association for Information Systems. 37, (2015). https://doi.org/10.17705/1CAIS.03712.
18. Schuler, M.: Health Data and Data Privacy: Challenges for Data Processors under the GDPR.
19. Spyridaki, K.: GDPR and AI: Friends, foes or something in between?
20. Stöger, K. et al.: Medical artificial intelligence. Commun ACM. 64, 11, 34–36 (2021). https://doi.org/10.1145/3458652.
21. Tietjen, D. et al.: Artificial Intelligence Act (AIA) - Legal uncertainty for medical device manufacturers. (2021).
22. Veale, M., Zuiderveen Borgesius, F.: Demystifying the Draft EU Artificial Intelligence Act.
23. The new EU Regulation on the protection of personal data: what does it mean for patients? https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf