Radar Healthcare – DPIA

radar healthcare

Title:	Radar Healthcare -DPIA
Owner:	Jonathan Alsop - Data Protection and Quality Lead
Approver:	Lee Williams- Chief Operating Officer
Target Audience:	All Staff
Issue:	1
Issue Date:	24/05/2023
Review Date:	24/05/2024

Version	Date	Comment	Updated by
1	24/05/2023	Document Creation	Jonathan Alsop

Contents

Submitting controller details

Name of controller	Smartgate Solutions Limited T/A Radar Healthcare
Subject/title of DPO	Quality and Data Protection Lead
Name of controller contact /DPO (delete as appropriate)	Jonathan Alsop

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
A Data Protection Impact Assessment (DPIA) is essential when implementing an integrated system for healthcare providers aiming to improve the quality of care for patients and residents. The need for a DPIA arises from the expectation that sensitive information will be included in the system, although it ultimately depends on how the partner utilizes the system. Given that the integrated system aims to transform unreliable processes and inconsistent communications into a streamlined and centralized approach, it is likely to involve the collection, storage, and processing of various types of personal data, including sensitive information related to patients and residents. This sensitive data may include medical records, treatment plans, diagnostic reports, and other confidential information. In summary, a DPIA is necessary when implementing an integrated system in healthcare, particularly when sensitive information is expected to be included. It ensures compliance with data protection laws, protects individuals' privacy, manages risks associated with data processing, considers partner-related aspects, enhances security measures, and demonstrates accountability and transparency.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
At Radar Healthcare, our top priority is maintaining the confidentiality and security of our partner's data. We want to assure our partners that we strictly adhere to a data storage policy, wherein we only retain partner data and refrain from utilizing or deleting it unless explicitly requested by the partner. The data we store consists of information that is migrated into our system or entered after its initial use. However, we acknowledge that there are inherent risks associated with data centres, including the potential unavailability, compromise, or technical issues that could impact the integrity of the database. To mitigate these risks, we have implemented stringent security measures and continuously monitor our data infrastructure. Our data is entered into our secure Software-as-a-Service (SAAS) system and stored at Redcentric in Harrogate, with backups maintained at a secondary data centre in Reading. We may also transfer data outside the UK/EEA, but we assure our partners that appropriate UK GDPR safeguards are implemented to ensure the protection and legal compliance of their data throughout any international transfers.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
At Radar Healthcare, we understand that our system may include special category and criminal offense data, depending on how our partners utilize the platform. The amount of data captured is directly influenced by our partners' usage and is updated whenever they require system updates. Retention policies for this data also depend on our partners' specific requirements and preferences regarding how long they wish to retain the data. It is important to note that all our partners' data is securely stored at the Redcentric Data Centre, which serves as the central hub for all partners within the United Kingdom. We prioritize the highest standards of data protection and work closely with our partners to ensure compliance with relevant regulations, including the handling of sensitive information.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
At Radar Healthcare, we maintain contracts with our partners, granting them ultimate control over their data. However, we reserve the right to process this data in accordance with the contractual arrangements for purposes such as support and marketing. Such processing is expected within the scope of our contractual agreements. Our partners have the flexibility to decide whether their data is held in the cloud or on-premise, although the latter option is less frequently utilized. It is important to note that our system is designed to accommodate data belonging to vulnerable groups, and depending on the type of service user, may include details related to children. As the system was built with these considerations in mind, there are no ongoing security concerns. Furthermore, both the system and the environment undergo annual penetration testing, and the results can be provided to our partners upon request. While system usage is not uniform among partners, as Radar Healthcare offers high configurability, the technology employed at Radar Healthcare and within our data centre adheres to current industry recommendations. In addition, our ISO9001 and ISO27001 certifications highlight our commitment to data security and the consistent management of our partners' data in a secure manner, in line with the service users' agreements with their respective care facilities.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
At Radar Healthcare, our ultimate goal is to enhance patient safety and support our partners in achieving compliance. We firmly believe that by providing a robust system, we contribute to making healthcare a safer environment for everyone involved. We are committed to developing and maintaining a platform that empowers healthcare providers to deliver high-quality care while adhering to regulatory standards and best practices. Through our comprehensive suite of tools and features, we aim to streamline processes, improve communication, and facilitate accurate and timely decision-making. By enabling our partners to effectively manage and track patient data, ensure adherence to protocols, and identify potential risks, we actively contribute to the overall safety and well-being of patients. We are dedicated to collaborating with our partners and continuously enhancing our system to meet the evolving needs of the healthcare industry and drive positive outcomes for all.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
At Radar Healthcare, we prioritize collaboration with our partners throughout the implementation and ongoing usage of our system. Our project managers and customer success managers work closely with our partners, ensuring effective communication and support. We involve our partners in decision-making processes, seeking their input to align the system with their specific requirements and workflows. During the rollout of Radar Healthcare, we maintain a streamlined approach and typically do not require consultation with additional stakeholders unless technical changes are necessary to support how our partners utilize the system. However, our dedicated compliance team is always available to provide assistance and guidance as and when required, ensuring that our partners navigate the compliance landscape seamlessly. We are committed to fostering strong partnerships and delivering exceptional customer experiences throughout the entire journey with Radar Healthcare.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
At Radar Healthcare, we process data based on the lawful basis of performance of a contract. Our processing activities aim to achieve the purpose of making data available to our partners in accordance with the contractual agreements we have in place. From a data storage perspective, the alternative option would be to store the data on-premises. It is important to note that the principles of data minimization are the responsibility of our partners, as they are the ones entering and administering the data within the system. As the Data Processor, it is the Controller's responsibility to provide information to users and ensure that their rights under the UK General Data Protection Regulation (GDPR) are respected and fulfilled. Any international transfers of data would be conducted in compliance with either the International Data Transfer Agreement (IDTA) or the European Standard Contractual Clauses (SCCs), ensuring the appropriate safeguards are in place.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. Risk of unauthorized access or disclosure: There is a risk of unauthorized access or disclosure of sensitive information if proper security measures are not in place. The integrated system may involve the collection, storage, and processing of various types of personal data, including sensitive information related to patients and residents, which could be at risk if not adequately protected.	Remote	Severe	Medium
2. Risks associated with data processing and retention: Processing and retaining partner data within the integrated system may pose risks if not handled appropriately. This includes the potential for data breaches, misuse, or non-compliance with retention policies, which could compromise the security and privacy of the data.	Possible	Significant	Medium
3. Risks associated with data centers: Inherent risks associated with data centers, such as potential unavailability, compromise, or technical issues, could impact the integrity of the database. Proper security measures and continuous monitoring of data infrastructure are necessary to mitigate these risks.	Remote,	Significant	Medium
4. Risks of international data transfers: Transferring data outside the UK/EEA may present additional risks if appropriate safeguards are not in place. Inadequate protection during international data transfers could lead to data breaches, unauthorized access, and non-compliance with data protection laws.	Possible	Significant	Medium
	Possible	Significant	Medium

5. Risks related to contractual data processing: While partners have ultimate control over their data, the organisation reserves the right to process the data in accordance with the contractual arrangements. Inadequate control or misuse of partner data during processing, such as for support and marketing purposes, could pose risks to data security and privacy.	Remote	Severe	Medium
6. Risks associated with vulnerable data: The system's accommodation of data belonging to vulnerable groups, such as children, requires special attention and robust security measures to protect their rights and privacy. Failure to adequately safeguard this sensitive information may lead to breaches or unauthorized access.	Remote,	Significant	Medium
7. Risks of non-compliance with data protection laws: Failure to conduct a Data Protection Impact Assessment (DPIA) and comply with relevant data protection laws may result in legal and reputational risks. Non-compliance could also lead to penalties or loss of trust from partners and service users.	Remote	Minimal	Low
8. Lack of transparency and accountability: Insufficient transparency and accountability in data handling practices may erode trust and expose the organization to reputational risks. Clear communication with partners, transparency regarding security measures, and providing penetration testing results upon request are essential to maintain trust.	Remote	Minimal	Low
9. Risks associated with stakeholder involvement: Limited involvement of additional stakeholders during the system rollout may result in overlooking certain security aspects or missing valuable insights. Adequate consultation with	Remote	Minimal	Low

stakeholders can help identify and address potential security risks.			

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
1.	We have implement strong access controls, including role-based permissions, and encryption of sensitive data. We conduct regular security audits and penetration testing to identify vulnerabilities and promptly address them.	Reduced	Low	Yes
2.	We have established clear data processing and retention policies aligned with data protection laws. We have implemented regular data backups, encryption, and secure deletion practices. We also provide training to employees on proper data handling and ensure compliance with retention policies.	Reduced	Low	Yes
3.	In Microsoft Azure (US) and Redcentric (UK) we have chosen reputable and secure data centers that follow industry best practices and standards. With this they will implement and monitor physical and logical security measures, implement robust disaster recovery plans and backups to mitigate potential data loss or unavailability.	Reduced	Low	Yes
4.	We ensure that appropriate safeguards for international data transfers are in place, such as implementing the European Standard Contractual Clauses	Reduced	Low	Yes

	(SCCs), ICO's IDTA or obtaining explicit user consent. We would also assess the data protection regulations in the destination country and ensure compliance with them.			
5.	We have clearly defined the purposes for which partner data can be processed in contractual agreements. We would obtain explicit consent from partners for any additional processing beyond the agreed-upon purposes. We will regularly review and update contracts to reflect evolving data processing practices.	Reduced	Low	Yes
6.	We have implemented additional security measures for data belonging to vulnerable groups, such as encryption, strict access controls, and regular monitoring for any unauthorized access attempts. Adhere to relevant regulations and guidelines specific to the protection of vulnerable data.	Reduced	Low	Yes
7.	With this DPIA we have conducted a comprehensive Data Protection Impact Assessment (DPIA) to identify and mitigate potential compliance risks. We have also established robust data protection policies and procedures, including regular audits and training to ensure compliance with applicable laws and regulations.	Accepted	Low	Yes
8.	We maintain transparency with our partners by clearly communicating data handling practices, security measures, and privacy policies. We provide regular updates and reports on security assessments, penetration testing results, and compliance audits. We also have a process for partners to	Accepted	Low	Yes

9.	request information about data usage and security measures. We engage relevant stakeholders, including security experts, privacy officers, and legal advisors, during the system rollout and ongoing usage. We conduct regular reviews and assessments with stakeholders to identify and address any potential security risks. We foster a culture of collaboration and communication to ensure a comprehensive understanding of security requirements and mitigate potential oversights.	Accepted	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Lee Williams/ Chief Operating Officer/ 18/07/2023	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Lee Williams/ Chief Operating Officer/ 18/07/2023	If accepting any residual high risk, consult the ICO before going ahead

DPO advice provided:	Jonathan Alsop/ Data Protection and Quality Lead/ 18/07/2023	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Based on the conducted DPIA for the system provided to customers in a healthcare setting, we have successfully addressed and mitigated the identified risks and concerns. Through the implementation of comprehensive security measures, adherence to data protection laws, and clear communication with our partners, we have taken significant steps to ensure the confidentiality, integrity, and availability of sensitive information. Our commitment to regular monitoring, strong access controls, encryption, and compliance with relevant regulations demonstrates our dedication to data security. By incorporating stakeholder input and conducting thorough assessments, we have proactively addressed potential security risks, enhancing the overall safety and privacy of the system.		
DPO advice accepted or overruled by:	Lee Williams COO	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Jonathan Alsop/Lee Williams	The DPO should also review ongoing compliance with DPIA