Johnson&Johnson	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Table of Contents

	N/A	
.		.

3 Data Protection Impact Assessment Regions and Associated Protocols

3.1 Protocols

3.2 Janssen Global Sponsor(s) and Regulatory Roles

Roles per the Clinical Trials Directive / Regulation

Global Sponsor:	N/A
☒ Sponsor in EU/EEA:	Janssen Pharmaceutica NV, 2340 Beerse, Turnhoutseweg 30, Belgium

☐ Representative in EU/EEA:	N/A

Roles per the General Data Protection Regulation

Data Controller:	Janssen Pharmaceutica NV, 2340 Beerse, Turnhoutseweg 30, Belgium who is a joint controller with IQVIA Ltd
☐ Data Controllers Representative in EU/EEA:	N/A

Is this a registrational study?

☐ Yes ☒ No

Are all Countries and Clinical Sites listed in CTMS?

☐ Yes ☒ No, provide comment

[redacted]

3.3 Types of Individuals and Collection of Special Categories of Personal Information

- Does the study involve data concerning study participants that belongs to the following categories of individuals?

☒ Trial participants - treatment population
☐ Trial participants - healthy volunteers
☐ Children (e.g., if the study is a pediatric study)
☐ Other: :

- Special Categories of Personal Information are data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

☐ Biometric Data for the purpose of uniquely identifying a natural person
☐ Political Opinions
☐ Data concerning a natural person's sex life or sexual orientation
☐ Racial or Ethnic Origin
☒ Data concerning health
☐ Religious or Philosophical Beliefs
☐ Genetic Data
☐ Trade Union Membership
☐ Other:

- Are the Special Categories of Personal Information indicated above required to be collected in accordance with the study protocol **and** does the protocol include a scientific rationale justifying the need for collecting the data?

  ☒ Yes

  ☐ No, provide rationale why the collection of the data is necessary

  Rationale: The protocol involves patients [redacted] which inherently requires the collection of health-related data such as diagnosis, treatment regimens [redacted] outcomes, and adverse events. This data is essential for evaluating treatment effectiveness and supporting regulatory and scientific objectives. Data concerning health is needed. Collecting health data is fundamental to the scientific validity, regulatory compliance, and operational execution [redacted]

3.4 Study Specific Risks Relating to Processing of Personal Information

- Identify risks which are specific for the study.
- Common risks related to the processing of personal information are included in the General DPIA. Consideration should be given to specific processes in a study which may pose additional risk or a higher likelihood of disclosure e.g., review by the sponsor of a document which is less likely to be redacted such as a pathology report of biopsied tissue.
- Study-specific risks may include, but are not limited to, risks identified in the General DPIA **where mitigation / controls are addressed differently** and risks not identified in the General DPIA. Specific attention should be given to risks related to process, disclosure, or transfer of directly identifiable study participant data.
- In the table below Residual Risk means risk remaining after mitigation and controls have been put in place.
- If a risk is identified, it will then be discussed with the stakeholders to resolve or determine if a privacy officer needs to be brought in for further guidance.

Are there any study specific risks that have been identified?

☐ No ☒ Yes, complete the table below

If "NO" is checked above, the table below does not apply and will remain blank

Risk Description / Scenario	Potential Impact to data subject (Study Participant)	Mitigation / Controls reducing the risk	Residual Risk (Low, Medium, High)

Data integrity may be damaged accidentally – Due to human error, technical outages or other reasons, the accuracy, completeness, and quality of data may be damaged and render the data unusable for the purposes of the study.	Inaccurate or incomplete data could lead to incorrect study conclusions, potentially affecting scientific validity and downstream healthcare decisions	Quality assurance processes are in place to ensure data accuracy and completeness; includes training, data validation, and technical safeguards	Low

Risk Description / Scenario	Potential Impact to data subject (Study Participant)	Mitigation / Controls reducing the risk	Residual Risk (Low, Medium, High)
Inaccurate data is provided by data provider – Even after providing training and written instructions, data received by IQVIA from the data provider is in accurate leading to incorrect study results.	Misinterpretation of patient outcomes or treatment effectiveness, potentially influencing future clinical decisions or research conclusions	Training and written instructions provided to data providers; quality assurance processes in place to identify and address data inconsistencies	Low
Data is damaged maliciously – an attacker could intentionally corrupt data (e.g., delete it, alter it, change the relationships between records).	Corrupted or altered data could lead to inaccurate study results, potentially affecting scientific conclusions and undermining trust in data protection	IQVIA has implemented technical safeguards including access controls, encryption, secure server environments, and monitoring systems to detect and prevent unauthorized data manipulation	Low
Disclosure control processes are not applied, and disclosive or disclosable data is released – A study site may inadvertently provide such data to IQVIA	Accidental exposure of identifiable data, compromising participant confidentiality	Site training on data specification and secure transfer (SFTP/HTTPS); incident reporting and deletion protocols	Low

Study subjects may be re-identified although only pseudonymised data is shared. – Study subjects may be re-identified by e.g. combining publicly available information with study data	Re-identification through data triangulation, violating privacy	Technical and organizational safeguards, restricted access, staff confidentiality agreements, and training	Low
The IT service may accidentally or deliberately remove data from the processing environment. – Data may be removed or deleted by IQVIA staff having access to the data – data may end up in the public domain.	Unauthorized deletion or exposure of sensitive data, leading to privacy breaches and potential misuse of personal health information	Access to data is restricted to authorized personnel only; secure server environment (L3), multi-factor authentication, logging of all access and data movement, and strict internal policies on data handling	Low

Risk Description / Scenario	**Potential Impact to data subject (Study Participant)**	**Mitigation / Controls reducing the risk**	**Residual Risk (Low, Medium, High)**
Users or administrators may deliberately copy or release data from the processing environment. – Data may be copied or released by IQVIA staff and due to that data may end up in the public domain	Unauthorized disclosure of sensitive health data, leading to privacy violations and potential reputational or psychological harm	All personnel are bound by confidentiality agreements and trained in data protection protocols. Data is pseudonymised, and only the minimum necessary information is processed, reducing the likelihood and impact of any unauthorized release.	Low
A physical intruder could steal data or equipment related to the processing environment. – Intruders could break into IQVIA's server rooms or offices and steal hardware with data stored on it	Unauthorized access to sensitive data via stolen hardware	Structural protections, password policies, visitor registration, and employee training	Low
External (Internet) hackers gain access to the dataand processing environment, resulting in theft or release of data.	Theft or exposure of sensitive data	Firewalls, MFA, access controls, penetration testing, and password complexity requirements	Low

Data is transferred to IQVIA using nonsecure way –Study sites are using unencrypted emails or other nonsecure ways of sharing data with IQVIA.	Shared data via unencrypted email or other insecure channels, there is a risk of interception or unauthorized access, potentially leading to a breach of confidentiality and harm to data subjects' privacy.	IQVIA requires all study sites to use secure, encrypted transfer methods (e.g., secure portals or encrypted email) for data exchange. Staff are trained on secure data handling, and any deviations are monitored and addressed through data protection protocols	Low
The Hospital (data supplier) may not have a legal basis to share the data or may not comply with GDPR.	Unlawful data processing, leading to regulatory noncompliance	Contractual obligations for informed consent and legal basis verification; MR-004 methodology adherence	Low

3.5 Systems

[redacted]

System Name	[redacted]	[redacted]	[redacted]

IQVIA Level 3 Enclave	See comment	See comment	

3.6 External Service Providers

Ensuring inspection readiness requires that we document all suppliers / external service providers that access, process and view patient data.

☐ Confirm all study suppliers accessing or processing study participant level data are on the List of Suppliers assessed to process personal data in clinical studies sponsored by Janssen Research & Development (see location above). Include the suppliers in the table below.

☒ Other Service Providers not listed, add them to the table below and provide information about the privacy qualification performed and countries in scope, as applicable.

If the Privacy Qualification conditions are not met, contact the Global Privacy group via the mailbox before finalizing the DPIA.

Name of External Service Provider / Third Party Supplier				

iQVIA LTD	Yes	Yes	Yes	[redacted]

4 Cross-Border Transfer and Data Localization

General statement on cross border transfers.

- Cross-border transfer from the European Economic Area (EEA), UK and Switzerland.
  - The data protection laws in the EEA, UK, and Switzerland require that contractual and other safeguards be put into place when personal data is transferred to countries which do not have adequate data protection laws as determined by the European Commission and government authorities in UK and Switzerland. Individuals in the countries referenced have rights to receive information about how their personal data is protected when transferred.
  - T[redacted]: Measures for Cross Border Transfer–Clinical Studies, summarizes the measures for cross-border transfer of personal data, including key-coded data that are transferred in Clinical Research in accordance with GDPR CHAPTER V, Transfers of personal data to third countries or international organizations.
- Other cross-border transfer and/or data localization requirements.
  - Countries other than the EEA, UK, and Switzerland may be subject to cross-border transfer restrictions and data localization requirements. Common examples include China and Russia. Identify cross-border transfer restrictions and localization requirements for the study and confirm adequate mitigation controls are in place.

1. Does this study have clinical sites in the EEA, UK, or Switzerland?

   ☒ Yes, see details below ☐ No, go to Question 2

   [redacted] Measures for Cross-Border Transfer–Clinical Studies been filed in the Trial Master File?

   ☐ Yes, V-TMF reference number[ ] ☒ No, The Cross Border Transfer is not necessary as data is only shared within the EU or adequate country (UK).

2. Have other cross-border transfer or data localization risks been identified for the study? ☐ Yes, see below for mitigation controls in place. ☒ No

Mitigation controls:

5 Legal and study-specific clarifications

[redacted]