Data Protection Impact Assessment

Submitting controller details

Name of controller	MSD Italia Srl., a subsidiary of Merck & Co., Inc. Rahway, New Jersey, USA("MSD")
Subject	Name of Study: CARE Study - Epidemiology of Triple Negative Breast CAncer in Italy: ChaRacterization of Patients and TrEatment Patterns Protocol Number: RevOps ID NO: *NIS102061*
Name of Global Privacy Office point of contact / Data Protection Officer for Italy	[redacted]

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.

CARE Study - Epidemiology of Triple Negative Breast CAncer in Italy: ChaRacterization of Patients and TrEatment Patterns

It is a Retrospective- Multicenter Observational study (the "Study") and it will be held in Italy as required under the applicable legislation on Observational Studies such as:

- AIFA guideline March 2008, as applicable;
- DM 30/11/2021, as applicable;
- Good Clinical practices, as applicable;
- Good Pharmacoepidemiology Practices (GPP)
- European Regulation 679/2016 (GDPR);
- Legislative Decree 196/2003 as modified by Legislative Decree 10 August 2018, n. 101 (the Italian Privacy Code);
- General provisions and relevant prescriptions issued by the Italian Data Protection Authority including the Provision containing the requirements relating to the processing of particular categories of data, pursuant to art. 21, paragraph 1 of Legislative Decree 10 August 2018, n. 101" issued on June 5, 2019 (Provision n.146/2019 annex 4 and 5)
- Deontological rules for the processing for statistical or scientific research purposes issued by the Italian Data Protection Authority pursuant to art. 20, paragraph 4, of Legislative Decree 10 August 2018, n. 101 - 19 December 2018:
- Deontological rules for the processing for statistical or scientific research purposes issued by the Italian Data Protection Authority pursuant to art. 2-quarter and 106 of Legislative Decree 196/2003 (Provision n. 298 of May 9th , 2024)

[redacted]

[redacted]

Objective of the Study as further described in the attached protocol:
Primary objective
The primary objective of this observational study is to describe baseline demographics and clinical characteristics of patients with TNBC, to describe treatment patterns, healthcare resource utilization of different therapeutic approaches and direct medical costs.

Secondary Objective & Hypothesis
The secondary objectives of this study are to describe the following items:
- the impact of TNBC on the National Healthcare System (in terms of healthcare resource utilization of different therapeutic approaches and direct medical costs)
- the main features of centers participating to the study
- the patients' survival outcomes and treatment response (for those undergoing neoadjuvant therapy)
- the first line patterns of care of patients with relapsed disease
- the time from diagnosis to obtaining BRCA or multigene panel result, and access to risk reducing surgeries

Exploratory Objective
To explore possible factors associated with patients' survival, including the choice of the neoadjuvant and adjuvant setting

Data collecting of Study participant healthcare data will be conducted by the study team at each hospital site retrospectively from clinical charts. Retrospective data capture from January 2018 to December 2021 period.

Monitoring of subject data and processing of patients pseudonymised data will be managed by the Clinical Research Organization (CRO) and will be shared, remotely, with few MSD (Sponsor) authorized personnel. Healthcare data may be shared with the Regulatory Authority (for inspection purposes as per legislation). Pseudonymisation of healthcare data will occur prior to transfer patient data to the Sponsor. Storing and archiving of data are required as per Good Pharmacoepidemiology Practice (GPP) and all applicable local laws, rules and regulations relating to the conduct of the observational studies.

Step 2: Data Collection

What Personal Data will be Collected?		
With regard to patients data		Select as applicable:
Information that identifies the individual and their personal characteristics	Date of birth (year)	☒
	Age (the informed consent form signature date is collected, so Age can be resumed even if not directly collected)	☐
	Gender	☒
	Physical description (height, weight, BMI, …)	☒
	Other health informations – such as number of MRI, X-Ray, PET, CT, menopausal status, …	☒
	Health symptoms and informations (smoking habits& Comorbidities)	☒
	Diagnosis	☒
	Date and cause of death	☒
	Genetic Data (g/sBRCAm, …)	☒
	Date of surgery, Type of surgery	☒

What Sensitive Personal Data will be collected?	
	Select as applicable:
Information relating to the individual's physical or mental health or condition and information relating to genetic information (biological samples such as chromosomal or DNA samples) and biometric information (such as fingerprints or facial recognition)	☒ genetic data will be collected.
Is the Research Study/Clinical Trial being conducted on a rare condition?	☐
Does the research involve a recorded interview or photographs that could identify the participant?	☐
Information relating to the individual's sex life.	☐
Information relating to the individual's sexual orientation	☐
Information relating to the individual's lifestyle (only smoking habits no alcohol consumption)	☒
Information relating to any offences committed or alleged to be committed by the individual	☐
Information relating to criminal proceedings, outcomes and sentences regarding the individual	☐
Information which relates to the education and any professional training of the individual	☐
Employment and career history	☐
Information relating to the financial affairs of the individual	☐
Information relating to the individual's religion or other beliefs	☐
Information relating to the individual's membership of a trade union.	☐

[redacted]

What is the lawful Basis for Collecting this Information?	
Explicit Consent Art. 6, (1))(a) of the GDPR in conjunction with art. 9 (2) (a) for the purpose to process the data of living patients for the Study purposes.	☒
Legitimate interests of the Hospital (Controller of Medical Records)	☐
Legitimate interests of the Study Sponsor (Controller of Study Data)	☐
Vital Interests of the data subject or another person	☐
Carried out (internally) by a not-for-profit organisation	☐
Information that has been already made public by data subject	☐
Necessary for substantial public interest	☐
Necessary for reasons of public interest in the area of public health Article 6(1)(c) legal obligation in conjunction with Article 9(2)(i) of the GDPR processing is necessary for reasons of public interest in the area of public health, such as pharmacovigilance This lawful basis will apply in relation to the processing of data of all patients involved in the Study for pharmacovigilance purposes.	☒
Archiving purposes in the public interest/ Scientific or Historical Research purposes/ Statistical purposes Article 9(2) (j) for scientific research purposes in accordance with applicable law and the Italian Supervisory authority decisions including the favorable opinion of the Italian Supervisory Authority pursuant to art. 110 of the Italian Privacy Code. This lawful basis in conjunction with the favorable opinion of the Italian Supervisory Authority will apply in relation to the processing of the data of all deceased or untraceable patients for the study purposes.	☒
Other For deceased and untraceable patients where consent cannot be collected the legal basis is the provision n. 298 of May 9th, 2024 of the Italian Supervisory Authority issued in accordance with art. 110 of Legislative Decree 196/2003 as amended together with the favourable opinion of the competent EC.	☒

[redacted]

Step 3: Describe the processing

Describe the nature of the processing:
How will you collect, use, store and delete data?
In consideration of the fact that the disease evaluated in the study affects subjects with old age and affected by comorbidities, presents a significant mortality rate based on the stage of the disease, and given the retrospective nature of the study and the large sample sizes need for the study, also patients passed way and untraceable will be included. This approach will allow to avoid bias resulting from the exclusion of such subjects (patients selected for the outcomes) that could compromise the scientific quality of the study and the purpose of the research. In such cases, Italian Privacy Law (Art. 110 of Legislative Decree 196/2003 as modified by Decree 19/2024 (the "Privacy Code")), with regard to the processing of personal data, for medical, biomedical and epidemiological research, states that consent is not necessary when, due to particular reasons, informing the data subjects is impossible or involves a disproportionate effort, or risks making it impossible or seriously compromise the achievement of the research objectives. In such cases, the data controller shall a) adopt appropriate measures to protect the rights, freedoms and legitimate interests of the data subject; obtain the favourable opinion from the competent ethics committee at local level; c) adopt and comply with the safety measures identified by the Italian Privacy Authority pursuant to article 106, par. 2, d) of the Privacy Code. Therefore, before starting the Study, the Protocol shall have obtained the favourable opinion of the local Ethics committee and the Sponsor shall comply with the Italian privacy aAuthority provision 298 of May, 9th /2024 that provides among other things the obligation to publish this DPIA and notify the Privacy Authority accordingly. For patients enrolled into the observational study only data needed for the purposes of the study will be collected. For living patients, the data will be collected by the Principal Investigator (or delegated clinical staff) from the Hospital medical records after explicit consent is given by the patient. For **deceased patients and untraceable patients** the data controller shall obtain the prior favourable opinion from the competent ethics committee at local level and shall adopt and comply with the safety measures identified by the Italian Privacy Authority pursuant to article 110 of Legislative Decree 196/2003 as modified by Law Decree 19/2024, including the publication of this DPIA. Furthermore the data will be collected by the Principal Investigator (or delegated clinical staff) from the Hospital medical records only after he adopted and documented all necessary measures to contact the patients such as browsing through their clinical records, contacting such telephone numbers as may be available at site, or obtaining contact information from population and/or health care registers in order to ensure compliance with the applicable Privacy Law and he gave evidence of the practical impossibility to collect the patient consent. Clinical patient data will be pseudonymized at the beginning prior to sharing with the Sponsor. The key for the pseudonymisation will be maintained by the Study site. The Sponsor cannot access the key to identify the patients. The study data will be entered in the eCRF with Remote Data Entry mode by the Investigators of the sites, who will be authorized by the Principal Investigator and suitably trained by Sponsor's representatives (CRO). For the HCP's data, names and work contact details will be uploaded into validated, secure Sponsor systems used for the purposes of managing clinical trials [redacted]

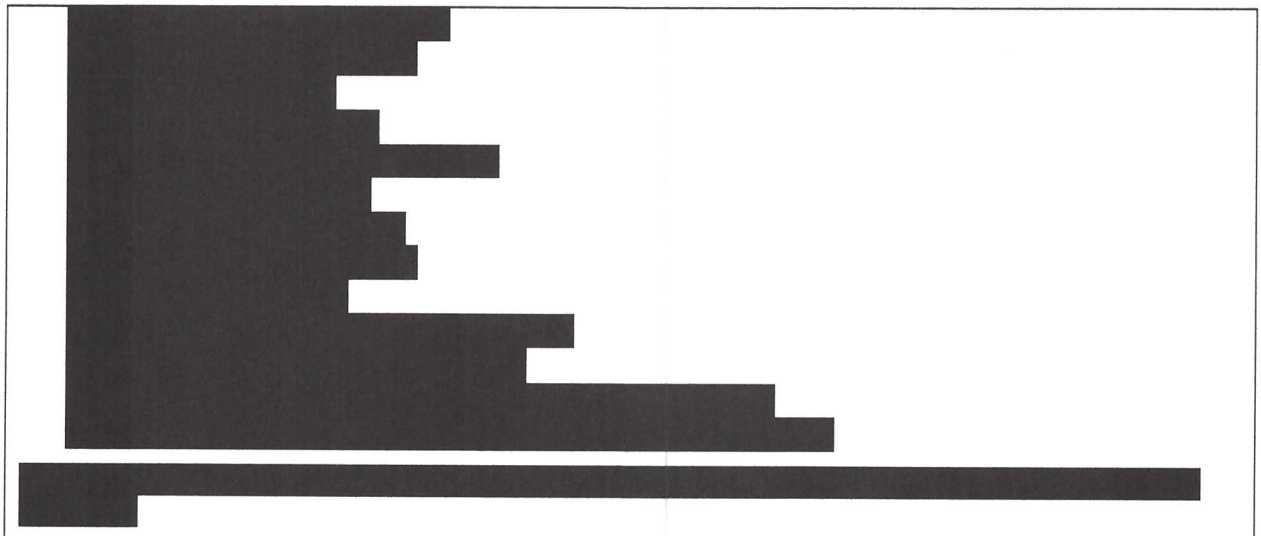
At the end of the Study the CRO will transfer to Sponsor the pseudonymised Study data through [redacted] with the appropriate protections to the manager designated by MSD. The Sponsor may retain the pseudonymized Study data for 5 years as per GPP; the Sponsor representatives (CRO) and its vendor will delete all data at the end of the Study. The Sponsor will not transfer pseudonymised Study data outside EU. Pseudonymised Study data will be stored at Sponsor facilities in accordance with its internal procedure. Data at the Study sites will be stored as per the hospital policy and regulatory requirements for observational studies. Information on how the Sponsor collects, uses, stores and deletes data is provided to the Study participant in the privacy notice and Informed Consent Form.
What is the source of the data?
Patient data will be collected directly from the patient medical records by the Principal Investigator (or delegated clinical Staff)
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.
Data collected at the study sites by the investigators (clinical Staff) will be entered into the eCRF (electronic Case Report Form). The data will be managed by the CRO (Clinical Research Organization which is the qualified Sponsor representatives which will act on behalf of the Sponsor) through the system [redacted] This system complies with the following requirements (ICH GCP, 21 CFR part 11) and for the cyber security standards (OSSTMM, OWASP, NIST 800-115, ISO-IEC 27:000 2016, ISO/IEC 27001:2017, ISO/IEC 27002:2013). [redacted] The data report will also be shared with research ethics committees and competent authorities when completing safety reporting as required per the legislation and when reporting the aggregate data results of the Study.

[redacted]

What types of processing identified as likely high risk are involved?
The Study involves the collection of Study participants data including deceased or untraceable subjects not providing explicit consent prior to their personal data being processed. The processing done by MSD will only take place after approval of the competent EC and after the publication of the DPIA and of the Information notice pursuant to art. 14 of GDPR.. MSD will only collect the pseudonymised data and will not be able to re-identify the individual. There is a risk related to monitoring activities where monitors may be able to access, at site, the subject identifiable data. However Monitors are designated by the CRO as subject authorised to process the data in compliance with GDPR and shall act in accordance with the instruction of the controller. Monitors are trained by the CRO on the functioning of the [redacted] eCRF system and e-CRF. They are required not to share identifiable data nor copy or record or bring outside sites data records. They also have to follow sites policy when accessing data records for monitoring purposes.

Describe the scope of the processing:
What is the nature of the data?
Having regard to patients' data the data to be collected will be information relating to eligible oncological patients who have been treated by the hospital as described in STEP 2 to this DPIA. [redacted]

[redacted]



Does the data include special category or criminal offence data?
Data relating to criminal offences will not be collected.
How much data will you be collecting and using? How often?
Data associated with patients medical and cancer history including information on diagnosis, treatment, intercurrent illnesses, test results (including genetic data) and healthcare will be collected and used throughout the duration of the observational study.
How long will you keep it?
The Sponsor may retain the pseudonymised study data for 5 years as per GPP.
How many individuals are affected?
[redacted]
What geographical area does it cover?
Data will be collected from participants in Italy and from HCPs at the associated Italy sites. Data processing will take place within Italy and the EU. Standardised safeguards will be put in place for data transfers from the CRO to the Sponsor. No data will be transferred outside the EU and between subsidiaries. Exclusively for Pharmacovigilance purposes, the Patients personal data may also be shared with Sponsor's parent company (Merck & Co., Inc.) and/or its Group companies in accordance with the Binding Corporate Rules. Vendor contracts include contractual clauses and data processing agreements to define the terms for data processing.

Describe the context of the processing:
What is the nature of your relationship with the individuals?
The individuals whose information will be collected and processed are patients at the Study sites. Living patient will consent to be part of the observational Study. For deceased and untraceable patients the Sponsor shall have obtained the favourable opinion of the local Ethics Committee and

shall publish the Data Protection Impact Assessment (DPIA) or an extract in advance on the MSD website, notifying the Italian Data Protection Authority accordingly, before commencing the Study in order to collect their data. This is in accordance with article 110 of the Privacy Code, as amended, as well as with the Italian Data Protection Authority decision of May 9th, 2024 n. 298. Please note that the processing of deceased and untraceable patients is necessary since it allows to avoid bias resulting from the exclusion of such subjects (patients selected for the outcomes) that could compromise the scientific quality of the study and the purpose of the research.
How much control will they have? Would they expect you to use their data in this way?
With regard to **Living subjects**: Before agreeing to take part in the Study, the study doctor or one of his clinical staff explains the study information to each participant as outlined in the participant information sheet, so they understand how their information will be shared for the purposes of the Study. Participants provide explicit consent prior to participating in the Study. Participants can withdraw from the Study at any time without giving a reason. The patient data will be deleted if patient withdraws consent. With regard to **Deceased patients / Untraceable patients:** The Investigator before collecting the data shall adopt all measures necessary to contact the patient such as browsing through their clinical records, contacting such telephone numbers as may be available at site, or obtaining contact information from population and/or health care registers in order to ensure compliance with the applicable Privacy Law and shall give evidence of the practical impossibility to collect the patient consent. For patients who, as a result of the research carried out, should be untraceable, the information referred to in art. 14 of the GDPR will be made public through suitable methods, such as their publication on the Sponsor's and Investigator's site website through specific information panels at Investigators' sites. In any case, if during the course of the study, as soon as the untraceable patients will contact the relevant site for any reason, including for check-ups, the Investigator will collect the informed consent signature for eligible patient and written privacy consent in order to allow him to exercise his rights under Privacy law. This DPIA will also be published on the Sponosr's website. HCPs are provided with a privacy notice related to the processing of their personal data for the purposes of conducting the Study. Their data cannot be withdrawn as it will be needed to support the results of the Study according to the regulations.

[redacted]

Do they include children or other vulnerable groups?
YES, Patients
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)?
With regard to **Living subjects:** There are no prior concerns over this type of processing, sharing or security flaws. Novel methods are not being used. The technology is appropriate for the data processing. There are no current issues of public concern. With regard to **Deceased patients / Untraceable patients** the concern lay on the fact that the data will be collected without the consent of the subjects. There are no security flaws, novel methods are not being used. The technology is appropriate for the data processing. There are no current issues of public concern. Data will be collected and processed in accordance of art. 110 of the Italian Privacy Code. The Sponsor will obtain the prior local Ethic Committee approval and will adopt the security measures identified by the Italian Data Protection Authority in its decision of May 9th, 2024, and will publish this Data Protection Impact Assessment (DPIA) in advance on the MSD website, notifying the Italian Data Protection Authority accordingly.

Describe the purposes of the processing:
What do you want to achieve?
Data will be used for analysis and reporting to regulatory authorities. Participant data will be in an aggregated and anonymised form.
What is the intended effect on individuals?
There is no direct intended effect related to the data processing on the individuals.
What are the benefits of the processing – for you, and more broadly?
The Study may be of benefit of the Sponsor during the procedures with Regulatory Authorities in relation to its products. The Study may also be of benefit to the public, as to date, no Real-World data are available in Italy regarding the characteristics of patients diagnosed with TNBC, the patterns of care in terms of administered anticancer treatments, and the impact of the disease on the National healthcare System. Real-world data will be essential to further improve the care of these patients and to guide future scientific discussion among physicians on how to choose the best treatment's pathway in this setting. This study will provide a complete and real picture of the health care journey of patients with TNBC in Italy, across the different Regions. Data deriving from this study will be also used to implement health-economic tools, as cost-effectiveness model and budget impact model at a local level. Data processing will assist in determining treatment options increasing opportunities.

Step 4: 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.
With regards to **living subject:** Explicit consent will be sought from the Study participants to process their healthcare data. The management of their data is extensively outlined in the patient privacy notice and informed consent form (ICF) for the Study, which has to be approved by the ethics committee. No Study data will be collected or processed until the ICF is reviewed, understood and signed by the patient to be enrolled into the observational study. With regards **untraceable patients:** The investigators shall adopt all necessary effort to contact participants before collecting their data. The privacy notice referred to in art. 14 of the GDPR will be made public. The management of their data is extensively outlined in the patient privacy notice and informed consent form (ICF) for the Study, which will be approved by the ethics committee. Moreover, if during the course of the Study, as soon as the untraceable patients will contact the relevant site for any reason, including for check-ups, the Investigator will collect the informed consent signature for eligible patient and written privacy consent in order to allow him to exercise his rights under GDPR. Finally for untraceable and the **deceased patients** the processing of their data will be subject to the prior favourable opinion of the sites' Ethic Committees and this DPIA will be rendered public and notified to the Italian Privacy Authority as provided by Provision 298/2024 of the Privacy Authority. With regards to **HCPs:** Data will only be collected in accordance with applicable law and Sponsor requirements. A privacy notice will be provided to all applicable personnel.
Who else do you need to involve within your organisation?
Data processing arrangements have been discussed as appropriate by the Medical Affairs observational study team, Sponsor representative, Data Protection Officer and the Global Privacy Office.
Do you need to ask your processors to assist?
An IT Risk assessment has been conducted with regard to the CRO. A Data Management Plan is in place between the CRO and the Sponsor. The CRO assisted the Sponsor in relation to this document. In addition to their routine data privacy training per the sites internal processes, the Study sites will be trained by the CRO acting on behalf of the Sponsor on appropriate data processing methods and data privacy at their site initiation visit and/or subsequent training sessions.
Do you plan to consult information security experts, or any other experts?
Information and technologies Risk Assessment team has been involved. No additional consultations are deemed necessary at this time.

Step 5: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:
What is your lawful basis for processing?
The sharing of information is the minimum necessary to achieve the goals of the Study. Processing will be minimised in conformance with the GDPR. With regard to **Living subjects:** The processing is carried out under the GDPR lawful basis of 6(1)(a) (consent) in conjunction with 9(2)(a) (explicit consent) With regard to **Deceased patients/Untraceable patients:** In case of Deceased patients or Untraceable patients, where there is impossibility to inform the patient, the processing will be carried out under art. 110 of the Italian Privacy Code in conjunction with GDPR lawful basis 9(2)(j) (for scientific research purposes) and the Italian Privacy Authority Provision n. 298/2024 provided that the Study protocol has obtained the prior favourable opinion of the local Ethics Committees.
Does the processing actually achieve your purpose?
The processing and sharing of the data will achieve the objectives of the observational study described above (please refer to STEP 1 entitled: Identify the need for a DPIA).
Is there another way to achieve the same outcome?
No.
How will you prevent function creep?
Study staff at sites, Sponsor representatives (CRO) and third parties will ensure that everyone is aware of the regulations, privacy requirements and contractual obligations. This is achieved through training and other organisational controls. In collecting, processing, transmit and store the data, the necessary measures will be adopted by the CRO and its suppliers to increase the level of data security as shown in the attached PIA as document 2 which are summarized hereto. The data of the patients will be pseudonymized by assigning a unique identification code so as not to be able to trace the interested party in any way. The investigators will be the only ones to keep the identification key (subject identification list). The [redacted] ecrf platform were the CRF will be managed and stored during the Study has been tested to ensure that data is recorded and attributed to the correct patient. The use of a dedicated database is envisaged with a user who can access only that database, further guaranteeing data protection and segregation and the inability to mix data even within the same project. The system resides on servers located in Italy with encrypted hard drives. The CRO and its suppliers will adopt suitable [redacted] protocols with access via username and password to ensure high levels of security and confidentiality of information, ensuring data transmission via a secure and encrypted connection channel. The system provides a backup system ([redacted] that allows a complete recovery of the data. Backup files are encrypted and copied to different locations via encrypted connections to preserve data privacy and confidentiality. There is a disaster recovery system. The computer system keeps track of any unauthorized access that has in any case been blocked. Data transmission will always take place in protected mode. Any transmission by means of portable storage media can only be made to the person in charge of receiving indicated by the Company. Any portable computing device or any portable storage medium including all backup data is kept in encrypted form, using a commercially supported encryption solution. The

[redacted]

encryption solutions will be implemented with [redacted], which will be transmitted only to the specifically indicated subjects MSD Italia using a transmission channel other than that used for Personal Data.
With specific reference to the processing operations of the data stored in the database, logical access to the e-CRF system takes place by entering a personal username and password. Users are not allowed to write down the password on the terminal or in any other place accessible to others. The password must consist of a combination of numbers and letters with a minimum of 8 characters. The password has a configurable validity period [redacted] After a predetermined number [redacted] of consecutive login attempts with incorrect username and/or password, the system automatically disables the user. Procedures are also provided for periodically checking the quality and consistency of the authentication credentials and the authorization profiles assigned to the persons designated for processing [redacted]

The pseudonymised data will be stored in a place protected by MSD for the time provided for in the Protocol at the end of which they will be destroyed. Access to the data will be allowed only to personnel authorized for this purpose and exclusively for the purposes related to the Study.

How will you ensure data quality and data minimisation?

Data quality is ensured through Good Clinical Practice (GCP), Good Pharmacovigilance Practice (GPP), training, system functionality, monitoring processes, audit and inspection. Data minimisation is undertaken by specifying data requirements in the observational study protocol and within the submission executed to Regulatory Authorities (including the Italian Privacy Authority) and Ethics Committees. The data capture system (eCRF: electronic case report form) used for observational study is programmed to only collect the necessary data required for the purpose of the Study.

What information will you give individuals?

Participants in the Study will be given information about the Study and the associated data processing in the patient privacy notice and information sheet and consent form prior to agreeing to participate in the Study. HCPs will be given information about the data usage in the data privacy form.
For patients who, as a result of the research carried out, should be untraceable, the information referred to in art. 14 of the GDPR will be made public through their publication on the website of the Sponsor's and of the investigator's site as well as through specific information panels at Investigators' sites. In any case, if during the course of the study, as soon as the untraceable patients will contact the relevant site for any reason, including for check-ups, the Investigator will collect the informed consent signature for eligible patient and written privacy consent in order to allow him to exercise his rights under Privacy law.
The DPIA will also be published on the Sponsor's website.

[redacted]

How will you help to support their rights?
The Study participants will be given details of the site's data protection officer in the privacy notice and patient information sheet and consent form, should they wish to discuss the use of their information. Sponsor contact details are also listed. The CRO (which will act on behalf of the Sponsor) will monitor activity at the Study site to ensure data is processed according to the regulations, policies, processes and contractual obligations.
What measures do you take to ensure processors comply?
Site activities are routinely monitored by the CRO to ensure compliance. CRO and Sponsor have drafted a Data Management Plan and entered into a Data Processing Agreement which provides auditing activities by Sponsor on CRO in order to ensure CRO compliance to its obligations. An IT Risk assessment has been conducted on CRO in order to assess the confidentiality, integrity and availability of the data by measuring both technical and organisational controls. CRO is allowed to partially sub-contract Study related activities or services to its Vendor appointed as sub-processors who has entered into a written agreement with CRO with terms that are at least as protective of Personal Information as the obligations set out in the DPA between Sponsor and the CRO. Consultants (i.e. HCPs involved in the study) untrusted by MSD or by the CRO for drafting scientific articles or the final reports will be appointed as processor or sub-processor through a Data Processing Agreement with MSD or the CRO.
How do you safeguard any international transfers?
Exclusively for Pharmacovigilance purposes, the patients personal data may also be shared with Sponsor's parent company (Merck & Co., Inc.) and/or its Group companies in accordance with the Binding Corporate Rules. The signature and the name of the HCP can be stored into the [redacted] The information will remain in our corporate network where we applied the appropriate security controls. Our Cyberfusion centre continuously monitor the network for unauthorised access.

Step 6: Identify and assess risks

INHERENT RISKS			
Risk description	**Initial Severity**	**Initial Likelihood**	**Overall risk**
Study subjects not providing explicit consent prior to their personal data being processed.	High	High	High
Data collection and storage; Data records compromised at the Study site.	High	Low	Medium
Data collection; additional data collected over what is required for the research objective.	low	Low	low
Data sharing and storage; Sponsor or sponsor representatives' (including Study vendors) systems compromised/accessed/miss-used by unapproved persons. Personal data disclosed outside of those that need to know.	medium	Low	Low

[redacted]

Data not securely deleted or destroyed when the retention period expires (from sponsor or sponsor representatives' [including study vendors] systems)	medium	Low	Medium
Malicious attack on IT infrastructure that may result in a loss of the Confidentiality, Integrity or Availability e.g. Hacking, Ransomware or any type of Cyber incident	High	Low	Medium
Data security incidents are not reported or reacted to, meaning that incidents are not addressed or appropriately processed.	High	Low	Medium
There is a potential risk that some individuals may be able to identify patients from the published data relating to this study.	High	Low	Medium

RATIONAL FOR RATING

Risk	Severity	Likelihood
Data subjects (i.e. Study participants) not providing explicit consent prior to their personal data being processed.	High: If patients are not aware that the controller is processing their information and they would not be able to exercise their rights.	High (Study participants) Limited (site researchers) As mentioned the Study protocol includes deceased and untraceable patients.
Data collection and storage; Data records compromised at the Study site	High: Risk is considered to have a maximal severity, given data records at Study sites are fully identifiable and contain sensitive healthcare data on Study participants.	Low: Data records stored at Study sites have restricted access as per the institutional robust policies and SOPs. Access is only permissible to appropriate HCPs, other limited staff members where necessary, and to Sponsor representatives (monitors) as outlined in the participant information sheet.

RATIONAL FOR RATING		
Risk	**Severity**	**Likelihood**
Data collection; additional data collected over what is required for the research objective.	low: Under GDPR and associated local regulations, data must only be collected where required for the research objective (data minimisation). Thus, any deviation from this requirement would be considered an important non-compliance.	Low: The Sponsor, also through CRO, ensures (and routinely oversight and control) that the databases have been carefully designed to only collect information required by the approved protocol, and in line with ICH-GCP, GPP and applicable legislation. Data of site researchers will only be collected as per applicable legislative obligations and Sponsor requirements, and a privacy notice will be issued to all applicable personnel.
Data sharing and storage; Sponsor or sponsor representatives' (including study vendor) systems, compromised/accessed/miss-used by unapproved persons. Personal data disclosed outside of those that need to know.	medium: Whilst the data may contain sensitive healthcare information, all participant data transferred out of the study site would be pseudonymised per GCP, which would limit any potential harm.	Low: The 'coded' data which is provided to the Sponsor is maintained electronically (web hosted) and linked to a secure database located in the EU (Italy) managed by the CRO and its vendor. Written agreements are in place over any sub-contracted activities, including database management and archiving. The database is fully validated in accordance with Good Clinical Practice guidelines and clinical trial legislation, a . This includes security, access permissions, change control, audit trail, data integrity and archiving. Furthermore, all third-party vendors used by MSD are assessed for data protection requirements which extends to their systems used for the Study. This process provides confirmation that the systems meet acceptable standards.

RATIONAL FOR RATING		
Risk	**Severity**	**Likelihood**
Data not securely deleted or destroyed when the retention period expires (from sponsor or sponsor representatives' [including study vendors] systems)	medium: The confidentiality of personal data could be breached where the data is improperly deleted or retained for longer than necessary. This could have an impact on the individuals and cause them distress.	Low: The Sponsor has data retention policies in place which align with regulatory requirements for the maintenance of clinical trial data. The Sponsor also conducts assessments on any vendors utilised to ensure their policies are acceptable prior to vendor employment.
Malicious attack on IT infrastructure that may result in a loss of the Confidentiality, Integrity or Availability e.g. Hacking, Ransomware or any type of Cyber incident	High: Individuals may be caused distress if their medical information is made public.	Low: The technical maintenance of the information systems of the Sponsor, the CRO and site are governed by policies and process to ensure up-to-date data security is always in place.
Data security incidents are not reported or reacted to, in meaning that incidents are not addressed or appropriately processed.	High: Our contracts require our vendors to report incidents as soon as they become aware.	Low: Data security incidents are identified through Sponsor and its vendors monitoring and assigned to responsible persons. Processes exist for reporting and managing incidents.

[redacted]

RATIONAL FOR RATING		
Risk	**Severity**	**Likelihood**
Potential Identifiability of the Anonymised data in particular when the data are shared for the purpose of drafting final reports or scientific articles.	High: Some study related factors such as small population [redacted], the patients' location throughout the country, their pathology (in particular if rare), may increase the risk of patient re-identification.	Low: The Sponsors will adopt anonymization techniques that considers all factors related to the study including the size of study population, in order to ensure adequate personal data protection and compliance with the applicable EU legislation in this area (including 05/2014 opinion of the Article 29 working party). In order to analyse the data, the CRO will apply the aggregation techniques by using a validated statistical software and will compute the following summary measures according to the type of data: -mean, standard deviation, minimum and maximum, for quantitative data; -absolute frequencies and percentages, for qualitative data. Furthermore, the CRO will adopt the technique of data aggregation and k-anonymization, which consists of preventing a trial participant from being singled out since it is grouped with, at least, k (with $k \geq 3$) other trial participants in that range. Processing exists for identifying and managing re identifications risks .

Step 7: Identify measures to reduce risk

Measures to mitigate the identified risks above	**Residual Severity**	**Residual Likelihood**	**Overall residual risk**
For living and traceable patients the explicit consent is collected by site personnel before collecting data. Informed consent of Study participants will be routinely checked by CRO representatives acting on behalf of the Sponsor during site monitoring visits. The Sponsor before starting the Study conducts regular data privacy training internally and to CRO, to allow Sponsor and CRO personnel to have appropriate oversight of site activities, and to ensure Sponsor and CRO personnel	Medium	Low	Medium

[redacted]

maintains compliance with regards to the collection of study participants data. In case of Deceased patients or Untraceable patients, the HCP will collect patient data from medical chart and data entry into the database of the study, provided that the protocol has obtained both the prior favourable opinion of the local Ethics Committee and of the Italian Data Protection Authority in accordance with the provisions set forth in the relevant Italian Privacy Law. The privacy notice pursuant to art.14 of the GDPR will be published on the MSD Italia website andclinical site and physically published at the clinical site. As soon as the patients will go to the clinical site for any reason, the clinical staff will submit the privacy notice and the consent to the subjects. Furthermore, as prescribed by the Italian Privacy Authority the following measures are in place: All patient data will be pseudonymized including the genetic information [redacted] The relative reference documentation that allows codes to be associated with patients' names will be secured and stored separately from the remaining study documents by the Investigator, accessible only to parties specifically authorised by him/her and will, at the end of the study, be kept in the site's archive. The [redacted] eCRF platform where the e-CRF will be managed and stored during the Study has been tested to ensure that data is recorded and attributed to the correct patient. The use of a dedicated database is envisaged with a user who can access only that database, further guaranteeing data protection and segregation and the inability to mix data even within the same project. The system resides on servers located in Italy with encrypted hard drives. All the processes for the development, management, administration and maintenance of the system are defined having as input the requirements of the European Data Protection Regulation, the ISO 27001 standard and all the most stringent best practices in terms of information security. The connection to the application and the transmission of data take place via the certified line (HTTPS). The data are stored on encrypted hard drives and are destroyed at the end of the study in order to limit data processing to what is really necessary and			

[redacted]

indispensable (minimization process - privacy by default). The CRO and its suppliers will adopt suitable [redacted] with access via username and password to ensure high levels of security and confidentiality of information, ensuring data transmission via a secure and encrypted connection channel. The system provides a backup [redacted] that allows a complete recovery of the data. Backup files are encrypted and copied to different locations via encrypted connections to preserve data privacy and confidentiality. There is a disaster recovery system. The computer system keeps track of any unauthorized access that has in any case been blocked. Data transmission will always take place in protected mode. [redacted]			

[redacted]

[redacted] The data may be sent by [redacted], with the appropriate protections. Password to documents will be provided separately. The pseudonymised data will also be delivered to the Sponsor on [redacted] with the appropriate protections to the manager designated by MSD Italia. The files [redacted] The receipt and correct readability of the files will be documented. The pseudonymised data will be stored in a place protected by MSD Italia for the time provided for in the Protocol at the end of which they will be destroyed. Access to the data will be allowed only to personnel authorized for this purpose and exclusively for the purposes related to the Study.			
All data at the Study sites will be maintained in accordance with the applicable institutions policies and SOPs. Access will be restricted to authorised personnel only. [redacted] The Study staff are trained as required per the institutions policies on data privacy. Where trial data is to be viewed by the Sponsor representatives (CRO and its monitors), the Sponsor representatives has thorough processes in place to determine that this activity can be done whilst maintaining compliance with the relevant legislation. Monitors are designated by the CRO as subject authorised to process the data in compliance with GDPR and shall act in accordance with the instruction of the controller. Monitors are trained by the CRO on the functioning of the [redacted] eCRF system and e-CRF. They are required not to share identifiable data nor copy or record or bring outside sites data records. They also have to follow sites policy when accessing data records for monitoring purposes. If remote review of medical records is completed (if agreed by the Sponsor and Study site DPO), the Sponsor will follow the Study site policies and procedures for remote access to participant's medical records. The method used to remotely view the medical records will vary between the sites, for example by using video calls, screen sharing,	medium	Low	Medium

[redacted]

[redacted] or by directly accessing electronic medical records systems. In all cases the site will use secure systems and maintain access control so that viewing is restricted to records of site Study participants only in a confidential environment. The same data sharing restrictions in existing agreements will apply while remotely viewing the medical records. The Sponsor will not record or print screen from the remote monitoring session. All privacy requirements (e.g., GDPR,) to protect participant's medical records and other personal health information will be complied with.			
The Sponsor and Sponsor representatives (including trial vendors) have designed their databases to only collect information required to fulfil regulatory requirements and meet the research objectives. The Sponsor and Sponsor representatives have processes in place to ensure that site researchers data will only be collected as per applicable legislative obligations and Sponsor requirements. Sponsor personnel receive regular data privacy training which would include the requirement to ensure data minimisation, that is, to only collect data where necessary and appropriate.	Low	Low	Low
Data stored in Sponsor or Sponsor representatives system have safeguards in place to prevent any unauthorised access (please refer to answer 1 of STEP 7) including appropriate authentication systems. Access to physical premises are controlled via appropriate security measures. Only pseudonymized Study subject data is maintained, thus minimising the risks associated with any breaches.	Low	Low	Low
The Sponsor has detailed data retention policies in place which are compliant with regulatory requirements for observational studies data retention and GDPR.	Low	Low	Low
Sponsor and CRO have technical support services to maintain the confidentiality, integrity and availability of their IT systems according to their policies and procedures. They have appropriate intrusion detection and firewalls rules in place.	Low	Low	Low
Site staff are trained at the start of the study on data privacy requirements. Monitoring of the Study conduct by site is performed on a regular basis by CRO representatives to assess quality, compliance and issues. Any incidents will be handled as per site and Sponsor processes.	Low	Low	Low
MSD provides for the carrying out of periodic checks aimed at assessing the persistence of the effectiveness of the data anonymisation measures with respect to technological evolution and will remove any singularity should it become aware of it at a later stage after the application of the anonymisation measures and will keep track of these	High	Low	Low

[redacted]

events in order to repeat the re-identification risk assessment upon reaching 1% of singularities identified out of the total number of records included in the dataset, as required by the provisions of the Italian Supervisory Authority..			

Step 8: Sign off and record outcomes

Item	Name/position/date	Notes
[redacted] [redacted] DPO	Signature/Date: [redacted]	
Summary of DPO advice: The study follows our standard process where patients can be contacted for their consent. In this study both untraceable and deceased patients are also included. In accordance with Italian Applicable law, the processing of the personal data relating to untraceable and deceased patients can take place only after obtaining the prior favorable opinion of the local Ethical committee and in accordance with applicable law including the Italian Privacy Authority provisions and prescriptions. Compliance with the data protection authority prescriptions shall be in place for all the duration of the processing. This DPIA and the information notice pursuant to article 14 of the GDPR must be published.		
DPO advice accepted by [redacted] [redacted]	Signature and date [redacted] 10/10/2024	
This DPIA will kept under review by: [redacted] [redacted]	[redacted] 10/10/2024	

[redacted]