Data Protection Impact Assessment (DPIA)

Overview

The purpose of this DPIA is to assess the privacy-related risks associated with the data processing activities in the context of a retrospective observational study to describe baseline characteristics and clinical outcomes of patients treated with palbociclib plus an aromatase inhibitor as first-line treatment for metastatic breast cancer (MBC) in Italy (hereinafter, the "**Study**").

The purpose of this DPIA is to identify the privacy and data protection risks associated with the Study. To that end, there are four sections to this DPIA:

- **Part I** (which appears in a table with the headline row in blue - □) describes the Relevant Personal Data and the Relevant Processing Activities in detail. It aims to be sufficient for a person reasonably familiar with the underlying technologies to understand the scope and function of the Relevant Processing Activities. It also sets out the legal responsibilities of the relevant Pfizer entities under Applicable Laws relating to privacy and data protection.
- **Part II** (which appears in a table with the headline row in green - □) analyses the relevant security measures and the potential risks posed by breaches of security.
- **Part III** (which appears in a table with the headline row in purple - □) considers whether all identified risks have been addressed, whether any risks remain and what their practical implications are.
- **Part IV** (which appears in a table with the headline row in orange - □) records the outcomes and sign-off of the DPIA by the DPO .

Defined terms used in this DPIA are set out in Appendix 1 below.

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data		
1. Details of the Controller(s)		
Controller(s) in respect of the Relevant Processing Activity:		Pfizer S.r.l., a company established under the laws of Italy, with registered office at Latina, Via Isonzo n. 71 and administrative office at Via Valbondione 113, 00188 Rome (Italy) (hereinafter "**Pfizer**").
Details of the DPO (or equivalent person)		Ms. Chiara Formenti-Ujlaki (Chiara.Ujlaki@pfizer.com)
Date of this DPIA:		***18 July 2025***
2. Completing this DPIA		
2.1. Details of the person responsible for this Form	**Full name:**	Elena Iattoni
	Email address:	Elena.Iattoni@pfizer.com
	Job title:	Sr Oncology Medical Affairs Scientist
	Name of the legal entity that employs you or has engaged your services:	Pfizer S.r.l.

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data		
3. Details of the Relevant Processing Activity		
3.1. Details of the Relevant Processing Activity	**Name of the Processing activity:**	Palbociclib plus aromatase-inhibitor as first-line treatment for Hormone Receptor (HR)-positive/Human Epidermal Growth Factor Receptor 2 (HER2)-negative locally advanced or metastatic breast cancer patients in Italy: a retrospective observational study (Palbo-Italy)
	Purpose of the Processing activity:	The processing activities are aimed at achieving the following objectives of the Study: PRIMARY OBJECTIVE: • Real-world Time to Treatment Discontinuation (rwTTD) in the overall cohort SECONDARY OBJECTIVES: • rwTTD in potential subgroups of interest (if sample size allows;) • Real-world Progression Free Survival (rwPFS) in the overall cohort and potential subgroups of interest • Real-world Time to Chemotherapy (rwTTC) in the overall cohort and potential subgroups of interest • Real-world Time to Next Treatment (rwTTNT) in the overall cohort and potential subgroups of interest • Description of dosing patterns in the overall cohort EXPLORATORY OBJECTIVES • Landmark overall survival (at 1-, 2-, 3-, 4-, 5-year) in the overall cohort • Characterization of long responders and correlation with baseline characteristics in the overall cohort • Description of second and third- line therapies in terms of type of therapy used and time to treatment discontinuation in the overall cohort
	Number of Relevant Data Subjects:	The estimate sample size counts about 600 HR+/HER2- metastatic breast cancer patients eligible for the study purpose; this number should be considered flexible, with scope to increase the sample size if feasible.
	Geographical scope of the Processing Activity:	The Study is a non-interventional, retrospective, single arm cohort study in Italy. Therefore, eligible patients must meet Italian reimbursed indications and inclusion criteria. Moreover, the patients treated with palbociclib will be recruited from Oncology wards or Oncological Centers with high expertise in breast cancer treatment across the entire geographical Italian territory.
	Reason for DPIA:	The purpose of this DPIA is to analyse the Relevant Processing Activities and address privacy and data protection issues arising from those activities.

	Additional context	**Rationale and Background of the Study**: CDK4/6-inhibitors are the standard of care as first line treatment of HR+/HER2- locally advanced (LA) or metastatic breast cancer (MBC) patients, as a consequence of positive results from large phase III trials showing a statistically significant and clinically meaningful progression-free survival (PFS) benefit favouring these agents compared to endocrine therapy (ET) alone. Real-world studies provide evidence that complements randomized controlled trials (RCT) with the opportunity to evaluate broader populations, generate more evidence, and ask/answer more clinical questions. Multiple factors are contributing to the increased interest in RWE, including changes in technology and advancing analytical methods, novel types and variety of RWD and the increasing acceptance of RWE from regulatory agencies, Health Technology Assessment (HTA) bodies, and payers. For these reasons, the collection of RWD on approved drugs is of clinical interest and can help the decision-making process at many levels. Although there are many real-world studies evaluating palbociclib in the real-life context, the Italian population is often absent or underrepresented. Thus, there is an additional need to generate local patient data specific for palbociclib, in particular in first-line treatment as per current standard of care with regard to daily routine clinical practice. **Study design:** Non-interventional, retrospective, single arm cohort study in Italy. **Population:** HR+/HER2- locally advanced or metastatic breast cancer patients starting treatment with first-line Palbociclib + aromatase inhibitor (+/- GnRH analog according to menopausal status) between January 1st, 2018 and February 28th, 2023 in Italy. **Variables:** Key variables include: **Baseline variables** (at index date: date of palbociclib treatment start) being collected in this Study include but are not limited to patient demographics, medical history, prior antineoplastic therapies, relevant concomitant medications, ECOG PS, stage at breast cancer diagnosis, type of MBC, baseline tumor characteristics, biological characteristics of the metastases (if available), metastatic spread, menopausal status (women), duration of follow-up. Medical diagnosis registered 90 days before the index data as reported in clinical records/HER will be extracted and then classified using condition categories based on ICD9-CM, Italian version 1997 **First-line documentation** includes but is not limited to treatment patterns, aromatase inhibitor combination partner palbociclib starting dose, palbociclib dose adjustment with reasons and date, real-world time to dose adjustment, proportion of patients with one or two dose adjustments, real-world time to treatment discontinuation, date and reason for end of treatment with palbociclib and/or aromatase inhibitor (if palbociclib was discontinued before).

Follow-up documentation includes but is not limited to type and duration of next two line antineoplastic therapies, real-world time to next treatment, real-world time to discontinuation of second and third-line subsequent treatments, real-world time to chemotherapy and type of chemotherapy used, real-world progression -free survival, yearly landmark overall survival from 1 to 5 years after start of palbociclib.

The above-mentioned list of variables is not exhaustive and may be subject to changes.

Data source:

The principal investigator or authorized medical staff will extract and collect clinical and treatment data from patients' existing medical records/EHR into an electronic Case Report Form (eCRF). As specified above, patients will be recruited from Oncology wards or Oncological Centers with high expertise in breast cancer treatment across the entire geographical Italian territory. Patients' data will be entered into the appropriate sections of the eCRF only by the center staff authorized by the principal investigator. Centers' users will receive their login credentials to the eCRF only after they have successfully completed the specific training and learning test. Data will be collected from medical records and laboratory reports available at clinical centers in paper or electronic format, depending on the local practice in use at each clinical center (since it is expected that clinical centers will not all have the same way of recording original data, at initiation visits the typology of source data will be identified and documented for each variable to be collected into eCRF). The eCRF must be regularly signed by the principal investigator. The signature serves to attest that the information contained on the eCRF is true. At all times, the investigator has the final responsibility for the accuracy and authenticity of all clinical and laboratory data entered into the eCRFs from the site source data.

Study Size:

As said above, based on a feasibility survey, the estimated sample size counts about 600 HR+/HER2- metastatic breast cancer patients eligible for the Study purpose; this number should be considered flexible, with scope to increase the sample size if feasible. The objectives do not state any hypotheses and therefore, no formal statistical testing is planned. All the analyses will be descriptive and so sample size calculations are not required.

Data Analysis:

Due to the retrospective observational nature of the Study data, descriptive statistics will be used to summarize all endpoints. No formal hypothesis will be tested.

Descriptive analyses will be performed to gain an understanding of the patient's characteristics. Summary statistics for continuous variables will include N, mean, median, standard deviation, interquartile range and range. Categorical variables will be summarized as frequencies and proportions (n, %).

Time-to-event outcomes will be assessed using time-to-event analyses (e.g. Kaplan-Meier (KM)) in the entire study cohort and across the prespecified subgroups of interest. KM curves will be shown to visualize time-to-event distributions for

each respective endpoint. The median time (and interquartile range) to event will be reported for each of these outcomes. Probabilities of an event at particular timepoints will be estimated with corresponding 95% Cis.

Milestones

Milestone	Planned date
Registration in the HMA-EMA Catalogues of RWD studies	30 September 2024
Completion of administrative activation of study sites	31 March 2026
Start of data collection	01 December 2025
Study progress report at 300 patients included	01 May 2026
End of data collection (600 patients)	01 October 2026
Final study report	01 February 2027

3.2. Applicable sector-specific standards	**Standards applicable to the Relevant Processing Activity:**	The Study will be conducted in accordance with legal and regulatory requirements, as well as with scientific purpose, value and rigor and follow generally accepted research practices described in Good Pharmacoepidemiology Practices (GPP) issued by the International Society for Pharmacoepidemiology (ISPE), Good Outcomes Research Practices issued by the International Society for Pharmacoeconomics and Outcomes Research (ISPOR), International Ethical Guidelines for Epidemiological Research issued by the Council for International Organizations of Medical Sciences (CIOMS), European Medicines Agency (EMA), European Network of Centres for Pharmacoepidemiology and Pharmacovigilance (ENCePP) Guide on Methodological Standards in Pharmacoepidemiology (http://www.encepp.eu/standards_and_guidances/methodologicalGuide.shtml) and the GDPR. Moreover, Pfizer uses a broad range of technical controls, security hardware and software, processes, detection techniques, response procedures, disaster recovery and business continuity capabilities to protect personal and business (GxP) data and manage operational risks. Preference is given to leading industry standards present in International Organization for Standards (ISO), Health Information Trust Alliance (HITRUST), American Institute of Certified Public Accountants (AICPA) System and Organization Controls (SOC), Payment Card Industry (PCI), Center for Internet Security (CIS), and National Institute of Standards and Technology (NIST), and Cybersecurity & Infrastructure Security Agency (CISA) or National Cyber Security Centre (NCSC) Cyber Essentials frameworks. **Industry Standard** **ISO 27001** **ISO 27002** **ISO 27018** **CSA STAR Level 1/Level 2** **PCI Data Security Standard (PCI DSS)** **HITRUST Common Security Framework (CSF)** **AICPA SOC 1 Type II** **AICPA SOC 2 Type I** **AICPA SOC 2 Type II** **CIS Controls** **NIST Cybersecurity Framework (CSF)** **NIST Special Publication 800-53** **CISA or NCSC Cyber Essentials**

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data		
3.3. Details of any Processors	**Name(s) of Processors:**	CRO Latis Srl – Piazza Colombo 3, int 1/b, 16121 Genova (hereinafter, the "**CRO**" or the "**Processor**").
	Is there a valid Processing Agreement in place for each Processor? (A valid Processing Agreement is one that sets out all of the requirements stipulated in Art. 28 of the GDPR, including duration, scope, purpose, documented processing instructions, prior authorisation (where relevant), provision of any documentation providing evidence of compliance with the prompt notification of any data breach)	Yes ☒ / No ☐

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data			
4. Categories of Relevant Data Subjects and Relevant Personal Data			
	Categories of Relevant Data Subjects:	**Categories of Relevant Personal Data:**	**Data retention Period:**

4.1. Details of the Relevant Personal Data	The Study involves the processing of personal data related to HR+/HER2- locally advanced or metastatic breast cancer patients starting treatment with first-line Palbociclib + aromatase inhibitor (+/- GnRH analog according to menopausal status) between January 1st, 2018 and February 28th, 2023 in Italy.	In order to conduct the Study, Pfizer - by means of the CRO acting as Pfizer's Processor - will extract and collect clinical and treatment data from patients' existing medical records/EHR into an eCRF, from Oncology wards or Oncological Centers with high expertise in breast cancer treatment across the entire geographical Italian territory.	Study's records must be kept for a minimum of 15 years after completion or discontinuation of the Study, or as required by applicable local regulations. In particular, pursuant to specific regulatory obligations applicable to clinical studies (*inter alia*, Commission Directive 2003/63/EC of 25 June 2003 amending Directive 2001/83/EC of the European Parliament and of the Council on the Community code relating to medicinal products for human use), Pfizer will retain the Study records for 15 years after completion or discontinuation of the Study. Records will be retained for longer than 15 years if required by applicable local regulations. To enable evaluations and/or inspections/audits from regulatory authorities or Pfizer, the participating physician agrees to keep records, including the identity of all participating patients (sufficient information to link records, e.g., CRFs and hospital records), all original signed informed consent/assent documents, copies of all CRFs, safety reporting forms, source documents, detailed records of treatment disposition, and adequate documentation of relevant correspondence (e.g., letters, meeting minutes, and telephone call reports). The records should be retained by the participating physician according to local regulations or as specified in the Clinical Study Agreement (CSA), whichever is longer. The participating physician must ensure that the records continue to be stored securely for so long as they are retained. If the participating physician becomes unable for any reason to continue to retain Study's records for the required period (e.g., retirement, relocation), Pfizer should be prospectively notified. The Study's records must be transferred to a designee acceptable to Pfizer, such as another participating physician, another

			institution, or to an independent third party arranged by Pfizer. The participating physician must obtain Pfizer's written permission before disposing of any records, even if retention requirements have been met. Where required, additional indication and/or instruction on data retention could be provided by Ethical Committees and/or by the Italian Data Protection Authority ("**IDPA**").

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data			
5. International transfers			
5.1. Details of transfers of Relevant Personal Data outside the EEA	Will the Relevant Personal Data be transferred outside the EEA?	Yes ☒ / No ☐	
5.2. Implementing safeguards for transfers of Relevant Personal Data outside the EEA	Does the Controller have safeguards in place for transfers of the Relevant Personal Data to listed jurisdictions at 5.1? (i.e., has the Controller put in place safeguards such as binding corporate rules or standard contractual clauses)	Yes ☒ / No ☐	In particular, due to retention purposes, Pfizer will transfer the eCRF to Pfizer Inc. in the United States of America, where the Group's archives are located. The personal data that will be involved in the intra-group transfer, will be pseudonymized, so as the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Transfers of personal data between Pfizer's group companies take place in compliance with the level of personal data protection required by the GDPR. The Controller involved in data transfers has provided appropriate transfer mechanisms, thus agreeing on adequate safeguards in the case of transfers to third countries, such as the United States of America, in accordance with Article 46(2)(c) of the GDPR.
6. Legal bases for the Relevant Processing Activity			
	Processing Activity:	**Applicable?**	**Justification:**

6.1. Legal basis for Processing	**Consent:** The data subject has freely given his or her specific, informed and unambiguous consent to the Relevant Processing Activity.	Yes ☒ / No ☐	According to the GDPR and local laws, processing of health data is prohibited unless the data subject has provided an explicit written consent. Therefore, alive patients must be able to understand and sign consent indicating that the patient (or a legally acceptable representative) has been informed of all pertinent aspects of the Study. However, as the Study has a retrospective observational design, there is a high likelihood that at the time where the in-scope patients were checked in at the Oncology departments, the purpose of the data processing was only limited to provide medical assistance to such patients and a specific consent for the purpose of conducting studies has not been harvested. In furtherance, due to the natural clinical history of oncological disease including metastatic breast cancer, it may not be possible to obtain their consents today (e.g. patients may be dead; they could be difficult to locate since patient contact details may be not up to date or false). Therefore, notwithstanding the data have already been gathered by the hospitals in the first place for another purpose, the in-scope data subjects' health data processing shall fall under art. 110 of Legislative Decree n. 196 of 2003, as further amended (the "**Italian Privacy Code**") which governs the patient consent in case of scientific research. In particular, the aforementioned article states, among other things, that: *"[…] consent is also not necessary when, due to particular reasons, informing data subjects is impossible or would entail a disproportionate effort or the risk to render impossible or seriously jeopardize the purpose of the scientific research. In such cases, the data controller takes appropriate measures to protect rights, freedoms and legitimate interests of the data subjects, the scientific research is submitted to the competent Ethical Committee*

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data			
			at local level for their motivated favorable opinion. In the above-mentioned cases, the IDPA identifies the safeguards to be implemented according to Article 106(2)(d) of this code". Therefore, for patients that are not alive or lost to follow-up and, thus, unable to sign informed consent, Pfizer will acquire the motivated favourable opinion of the competent Ethical Committees and will, prior to Processing, carry out a data protection impact assessment of the impact of the envisaged processing operations on the protection of personal data, pursuant to article 35 of the GDPR, highlighting the reasons why it is not possible to inform the patients, as well as the measures to protect their rights and freedoms. Pfizer will publish and/or communicate to the IDPA the outcome of the data protection impact assessment, where required according to the applicable guidance provided by the IDPA on the safeguards to be adopted pursuant to article 110 of the Italian Privacy Code.
	Contractual Necessity: The Relevant Processing Activity is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.	Yes ☐ / No ☒	
	Compliance with law: The Relevant Processing Activity is necessary for compliance with a binding legal obligation to which the Controller is subject under the laws of the EU or an EU Member State.	Yes ☐ / No ☒	
	Vital interests: The Relevant Processing Activity is necessary to protect the vital interests of any person (i.e., in life-or-death situations).	Yes ☐ / No ☒	
	Public interest: The Relevant Processing Activity is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller	Yes ☐ / No ☒	

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data			
	Legitimate interests: The Relevant Processing Activity is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Relevant Personal Data, in particular where the data subject is a child.	Yes ☐ / No ☒	
7. Data minimisation			
7.1. Steps taken to minimise the extent to which Relevant Personal Data are Processed	Has the Controller implemented any measures to ensure that Relevant Personal Data are adequate, relevant and not excessive?	Yes ☒ / No ☐	
	If "**Yes**", please explain what measures have been implemented.	Pfizer - by means of the CRO - collects and processes only the Relevant Personal Data that are strictly necessary to achieve the purposes of the Processing and no additional and excessive data is collected, in accordance with the opinion issued by the geographically competent Ethical Committees. In particular, the CRO drafts reports that include only the information that are relevant for the Study. In addition, patients' names and surnames are replaced by ID numbers through a pseudonymization activity so that they are not even communicated to Pfizer. Furthermore, even if the CRO will access identifiable personal information, it will remove patients' names and other directly identifiable data in any reports, publications or other disclosures when sent to Pfizer, except where required by applicable laws.	
8. Data quality			
8.1. Steps taken to ensure that the Relevant Personal	Has the Controller implemented any measures to ensure that the Relevant Personal Data are accurate and up to date?	Yes ☒ / No ☐	

Data are accurate and up to date	If "**Yes**", please explain what measures have been implemented.	The Relevant Personal Data processed for the purpose of the Study are accurate. The CRO - on behalf of Pfizer - adopts measures to verify the accuracy and quality of the Relevant Personal Data Processed, erasing or updating Personal Data considered out-of-date and/or filtering out inconsistent, incomplete and inaccurate data. Moreover, data cleaning activities will be performed by the CRO. Both automated and manual checks will be performed. The delegated CRO will perform checks to support the participating physicians in the data entry to assess the appropriateness and consistency of data entered in the eCRF system. These checks will be implemented as warnings, i.e., in case of data entry error, an alert appears, inviting to make a correction. The participating physician will have the option to correct data or to ignore the warning. Checks on exported data will be run in order to verify that no inconsistent data are entered in the eCRF. A few automated checks will be performed on the data before and after the Source Data Verification (SDV) by Data Manager (DaM) using software (SAS) while other checks will be performed manually by DaM/Clinical Research Associate (CRA). The consistency with source data will be assessed through Source Data Verification during the monitoring visits. Checks on exported data will be run in order to verify that no inconsistent data are entered in the eCRF. A few automated checks will be performed on the data before and after the SDV by DaM using software (SAS) while other checks will be performed manually by DaM/CRA. Details about the source data verification process will be provided in the Monitoring Plan.

9. Data Retention

9.1. Details of the applicable retention periods for Relevant Personal Data

Categories of Relevant Personal Data:	**Applicable retention period**	**Justification for retention period**	**Mechanism for ensuring deletion at the end of the retention period:**
Production data (i.e., data use)	According to the Study protocol, the Study's records must be kept by Pfizer and the Site for a minimum of 15 years after completion or discontinuation of the Study, as specified above.	The specific period has been chosen based on the Study protocol and the relevant applicable regulations, *inter alia*, the Commission Directive 2003/63/EC of 25 June 2003 amending Directive 2001/83/EC of the European Parliament and of the Council on the Community code relating to medicinal products for human use.	The CRO will certify to Pfizer the deletion at the end of the Study when requested by Pfizer. The CRO must obtain Pfizer's written permission before disposing of any records, even if retention requirements have been met.
Backup or archived data	Not applicable.	Not applicable.	Not applicable.
Metadata	The metadata will be retained in compliance with the agreement entered into by and between the CRO and Pfizer and the applicable law.	The CRO will retain data as agreed under the agreement entered into by and between the CRO and Pfizer.	The CRO will certify to Pfizer the deletion at the end of the Study when requested by Pfizer.

	Technical logs	The technical logs will be retained in compliance with the agreement entered into by and between the CRO and Pfizer and the applicable law.	The CRO will retain technical logs as required by the agreement entered into by and between the CRO and Pfizer.	The CRO will certify to Pfizer the deletion at the end of the Study when requested by Pfizer.

10. Proportionality and necessity			
10.1. Explanation of how controls are implemented in respect of the Relevant Processing Activity to ensure proportionality and necessity	**Controls guaranteeing the proportionality and necessity of the Processing:**	**Are suitable controls in place?**	**What improvements or corrections should be implemented?**
	Purposes: Are controls in place to ensure that Relevant Personal Data are only Processed for specified, explicit and legitimate purposes? (see section 3 above).	Yes ☒ / No ☐	-
	Legal basis: Are controls in place to ensure that there is a valid legal basis for the Relevant Processing Activity (see section 5 above).	Yes ☒ / No ☐	-
	Data minimisation: Are controls in place to ensure that Relevant Personal Data are adequate, relevant and not excessive? (see section 6 above)	Yes ☒ / No ☐	-
	Data quality: Are controls in place to ensure that Relevant Personal Data are accurate and kept up to date? (see section 7 above)	Yes ☒ / No ☐	-
	Retention period: Are controls in place to ensure that Relevant Personal Data are stored for a limited period only?	Yes ☒ / No ☐	-

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data		
11. Rights of Data Subjects		
11.1. Exemptions	Does the Relevant Processing Activity benefit from any exemptions with respect to the rights of Data Subjects under the GDPR?	Yes ☒ / No ☐
	If "**Yes**", please explain exemptions apply.	As mentioned above in Section 6, according to GDPR and local laws, processing of health data is prohibited unless the data subject has provided an explicit written consent. As this Study has a retrospective observational design, there is a high likelihood that at the time when the in-scope patients were checked in at the Oncology department, the purpose of the data processing was only limited to provide medical assistance to such patients and a specific informed consent for the purpose of conducting studies has not been harvested. In furtherance, due to the natural clinical history of oncological disease including metastatic breast cancer, it may not be possible to obtain their consent today (e.g. patients may be dead; they could be difficult to locate since patient contact details may be not up to date or false). On this regard, the Study protocol will be submitted to the Ethical Committee for approval considering that, notwithstanding the data have already been gathered by the hospitals in the first place for another purpose, the in-scope data subjects' health data processing shall fall under art. 110 of the Italian Privacy Code. Therefore, in order to process in-scope data subject' health data without the ordinary informed consent process, Pfizer will acquire the motivated favorable opinion of the competent Ethical Committees and will publish and/or communicate to the IDPA the outcome of the data protection impact assessment, where required according to the applicable guidance provided by the IDPA on the safeguards to be adopted pursuant to article 110 of the Italian Privacy Code.
11.2. The right to information	Are the Relevant Data Subjects provided with suitable notice of the Relevant Processing Activity?	Yes ☒ / No ☐

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data		
	If "**Yes**", please explain how that notice is provided, including links to any online notices or policies. If "**No**", please explain why suitable notice is not provided.	As explained above, for alive patients that do not match with the conditions covered by art. 110 of the Italian Privacy Code as described above, the informed consent form and the privacy consent form must be in compliance with local regulatory requirements and privacy and legal requirements. The informed consent form and the privacy consent form used in the Study, and any changes made during the course of the Study, must be prospectively approved by Pfizer and the Ethical Committee before use. The participating physician must ensure that each Study's patient, or his/her legally acceptable representative, is fully informed about the nature and objectives of the Study and possible risks associated with participation and also about the nature of the process of his/her personal data. The participating physician, or a person designated by it, will obtain written informed consent and privacy consent from each patient or the patient's legally acceptable representative before any study-specific activity is performed. The participating physician will retain the original of each patient's signed consent form and privacy consent. One copy of both must be given to the subject. It is the responsibility of the participating physician to obtain written informed and privacy consent from each patient or from the patient's legal representative prior to the collection of any data from the patient's records. The forms must be signed before data collection starting. Consents must be documented by the subject's dated signature. The signature confirms that the consents are based on information that has been understood. Moreover, the participating physician must sign and date the consent forms too. Each subject's signed informed and privacy consent must be kept on file by the participating physician. For Data Subjects falling under art. 110 of the Italian Privacy Code who cannot be contacted directly will be provided through the publication of a specific online publication, via the website www.pfizer.it.
	Where Relevant Personal Data are obtained directly from the Relevant Data Subjects, does the relevant notice satisfy the requirements of Article 13 of the GDPR?	Yes ☒ / No ☐
	If "**No**", please explain which aspects are not compliant with Article 13.	
	Where Relevant Personal Data are not obtained directly from the Relevant Data Subjects, does the relevant notice satisfy the requirements of Article 14 of the GDPR?	Yes ☒ / No ☐
	If "**No**", please explain which aspects are not compliant with Article 14.	

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data		
	Does the Controller have in place suitable mechanisms to ensure that the erasure, rectification, or restriction of Processing of Relevant Personal Data is communicated to the Relevant Data Subjects, in accordance with Article 19 of the GDPR?	Yes ☒ / No ☐
	If "**Yes**", please describe the mechanisms. If "**No**", please explain why not.	According to sections 10.2 of the Study protocol, Data Subjects are informed that the correction and integration of the Relevant Personal Data can be annotated to the extent the result of these operations does not produce significant impact on the research result, as set forth under the Ethical rules for processing for statistical or scientific research purposes published pursuant to Article 20, paragraph 4, of Legislative Decree No. 101 of August 10, 2018 of December 19, 2018 issued by the IDPA (*Article 12. Exercise of the rights of the Data Subjects - If, in the event of the exercise of the rights referred to in Art. 15 et seq. of the Regulation, changes are required to the data concerning the data subject, the data controller shall record the changes requested by the data subject in the appropriate spaces or registers, without changing the data originally entered in the file*). Please note that the data received by Pfizer and the Processor are pseudonymized.
11.3.The right of access	Does the Controller have mechanisms in place to ensure that Relevant Data Subjects are able to obtain access to, or a copy of, their Relevant Personal Data?	Yes ☐ / No ☒
	If "**No**", please explain why not.	The data received by Pfizer and the Processor are pseudonymized and it won't be technically feasible to address the request for them. In particular, to protect the rights and freedoms of natural persons with regard to the Processing of the Relevant Personal Data, all Study's data will be pseudonymized before collection in the eCRF by any authorized party. Patient names will be removed and will be replaced by a single, specific, numerical code, based on a numbering system defined by CRO and Pfizer. All other identifiable data transferred to Pfizer or other authorized parties will be identified by this single, patient-specific code. The site will maintain a confidential list of patients who participated in the Study, linking each patient's numerical code to his or her actual identity.
	Does the Controller have sufficient controls in place to ensure that such access can be granted within one month of receipt of a valid request from a Relevant Data Subject?	Yes ☐ / No ☒

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data		
	If "**No**", please explain why not.	See answer to 11.3 above.
11.4. The right to rectification	Does the Controller have mechanisms in place to ensure that errors in Relevant Personal Data are rectified promptly upon the Controller becoming aware of those errors?	Yes ☒ / No ☐
	If "**Yes**", please describe the mechanisms. If "**No**", please explain why not.	According to sections 10.2 of the Study protocol, Data Subjects are informed that the correction and integration of the Relevant Personal Data can be annotated to the extent the result of these operations does not produce significant impact on the research result, as set forth under the Ethical rules for processing for statistical or scientific research purposes published pursuant to Article 20, paragraph 4, of Legislative Decree No. 101 of August 10, 2018 of December 19, 2018 issued by the IDPA (*Article 12. Exercise of the rights of the Data Subjects - If, in the event of the exercise of the rights referred to in Art. 15 et seq. of the Regulation, changes are required to the data concerning the data subject, the data controller shall record the changes requested by the data subject in the appropriate spaces or registers, without changing the data originally entered in the file*). Please note that the data received by Pfizer and the Processor are pseudonymized.
11.5.The right to erasure	Does the Controller have mechanisms in place to ensure that Relevant Personal Data are deleted within one month after a valid deletion request is made by a Relevant Data Subject?	Yes ☐ / No ☒
	If "**Yes**", please describe the mechanisms. If "**No**", please explain why not.	Due to the nature of the Processing, i.e., a clinical study, some or all of the Relevant Personal Data may be retained and used where deletion would seriously undermine the Study (e.g. where deletion would affect the consistency of the Study's results) or where the Relevant Personal Data are necessary to comply with legal requirements. Please note that the data received by Pfizer and the Processor are pseudonymized.
11.6. Restriction of Processing	Does the Controller have mechanisms in place to ensure that the Processing of Relevant Personal Data can be restricted where appropriate in accordance with Article 18 of the GDPR?	Yes ☒ / No ☐

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data			
	If "**Yes**", please describe the mechanisms. If "**No**", please explain why not.	The restriction of processing of the data can be annotated to the extent the result of these operations does not produce significant impact on the Study's result, as set forth under the Ethical rules for processing for statistical or scientific research purposes published pursuant to Article 20, paragraph 4, of Legislative Decree No. 101 of August 10, 2018 of December 19, 2018 issued by the IDPA. To protect the rights and freedoms of Relevant Data Subjects, when Study's data are compiled, any patient names will be removed and will be replaced by a single, specific, numerical code by the Principal Investigator of the single Site.	
11.7. The right to data portability	Does the Controller have mechanisms in place to give effect to the right to data portability?	Yes ☐ / No ☒	
	If "**Yes**", please describe the mechanisms. If "**No**", please explain why not.	Not applicable.	
11.8.The right to object	Does the Controller have mechanisms in place to give effect to the right of Relevant Data Subjects to object to the Processing of their Relevant Personal Data in accordance with Article 21 of the GDPR?	Yes ☐ / No ☒	
	If "**Yes**", please describe the mechanisms. If "**No**", please explain why not.	Processing of Relevant Personal Data concerning Relevant Data Subject is not based on point (e) or (f) of Article 6(1) of the GDPR.	
12. Consent			
12.1. Obtaining consent from	**When the Controller relies on consent as its legal basis for the Relevant Processing Activity:**		**Explanation:**

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data			
Relevant Data Subjects	Does that consent obtained on an **opt-in basis**? (i.e., the Relevant Data Subject makes a positive choice to consent – as opposed to passive acquiescence or failure to un-tick a pre-ticked box)	Yes ☒ / No ☐	As explained above, for alive patients that do not match with the conditions covered by art. 110 of the Italian Privacy Code, the participating physician, or a person designated by it, will obtain written informed consent and privacy consent from each patient or the patient's legally acceptable representative before any study-specific activity is performed. The participating physicianwill retain the original of each patient's signed consent form and privacy consent. One copy of both must be given to the Data Subject. It is the responsibility of the participating physicianobtain written informed and privacy consent from each patient or from the patient's legal representative prior to the collection of any data from the patient's records. The forms must be signed before data collection starting. If the subject and his/her legal representative are unable to read, the informed and privacy consent will be obtained in the presence of an impartial witness, e.g., a person independent of the study who will read both consent forms for the subject. Consent must be documented by the Data Subject's dated signature. The signature confirms that the consent is based on information that has been understood. Moreover, the participating physicianmust sign and date the consent forms too. Each Data Subject's signed informed and privacy consent must be kept on file by the participating physician.
	Is that consent **freely given**? (i.e., obtained without any element of compulsion or undue influence, and not obtained in exchange for a product or service)	Yes ☒ / No ☐	See previous answer.
	Is that consent **specific**? (i.e., clearly limited to a specified purpose)	Yes ☒ / No ☐	See previous answer.
	Is that consent **informed**? (i.e., the Relevant Data Subject is provided with sufficient information to understand the Relevant Processing Activity to which he or she is being asked to consent)	Yes ☒ / No ☐	See previous answer.
	Is that consent **unambiguous**? (i.e., there is no element of doubt as to whether the Relevant Data Subject consented or not)	Yes ☒ / No ☐	See previous answer.

Data Protection Impact Assessment – Part I: Processing of Relevant Personal Data			
	Does the Controller have **evidence of consent**? (i.e., does the Controller keep records to demonstrate that valid consent was obtained from the Relevant Data Subjects)	Yes ☒ / No ☐	See previous answer.

Data Protection Impact Assessment – Part II: Security Measures

1. Potential privacy breaches

Risk	Source of risk	Likelihood of harm	Severity of harm	Overall risk
Illegitimate access to Relevant Personal Data	Pfizer Personnel or third parties gaining unauthorised access to Relevant Personal Data.	Remote ☒ / Possible ☐ / Probable ☐	Minimal ☐ / Significant ☐ / Severe ☒	Low ☒ / Medium ☐ / High ☐
Unwanted change to Relevant Personal Data	Unauthorised access to Relevant Personal Data could result in unwanted changes.	Remote ☒ / Possible ☐ / Probable ☐	Minimal ☐ / Significant ☐ / Severe ☒	Low ☒ / Medium ☐ / High ☐
Disappearance of Relevant Personal Data	Unauthorised access could result in unwanted deletion of Relevant Personal Data.	Remote ☒ / Possible ☐ / Probable ☐	Minimal ☐ / Significant ☐ / Severe ☒	Low ☒ / Medium ☐ / High ☐

Data Protection Impact Assessment – Part II: Security Measures		
2. Security measures	**Categories of security measures**	**Examples of relevant data security measures**
		CRO will Process the Relevant Personal Data on behalf of and/or for the benefit of Pfizer under the agreement entered by and between Pfizer and CRO and the latter will operate in accordance with the requirements set forth under the attachments to the agreement entered into by and between Pfizer and the CRO, appointing CRO as Processor. The security measures listed below are implemented by the CRO in line with the data processing agreement and in accordance with the IDPA Ethical rules for processing for statistical or scientific research purposes published pursuant to Article 20, paragraph 4, of Legislative Decree No. 101 of August 10, 2018 of December 19, 2018 and the IDPA guidance on the processing of personal data carried out for scientific research purposes issued by the IDPA on June 5, 2019. Moreover, Pfizer uses a broad range of technical controls, security hardware and software, processes, detection techniques, response procedures, disaster recovery and business continuity capabilities to protect personal and business (GxP) data and manage operational risks. Furthermore, according to the Protocol, the treating physicians' site staff entering data will receive training on the system remotely, and after successfully passing the final test, each person will be issued a unique user identification and password. The initial access will be through a password generated by the system, to be changed after first access. For security reasons, only the person who owns the user identification and password will access the system using his or her own unique access codes. Access codes are nontransferable. Site personnel who have not undergone training may not use the system and will not be issued user identification and password until appropriate training is completed. Any personnel having access to the eCRF system will be traced in a list continuously updated during the study conduction. Access to eCRF will be deactivated once a person is no more part of the staff.

Data Protection Impact Assessment – Part II: Security Measures		
	(A) Pseudonymisation and encryption	**Measures of pseudonymisation and encryption of personal data:** ☒ State-of-the art encryption applied to all data 'in transit' ☒ State-of-the art encryption applied to all data 'at rest' ☒ Password databases are subject to strong encryption / hashing ☒ State-of-the art encryption on drives and media containing personal data ☒ Secure data networks (e.g., encrypted VPNs) ☒ State-of-the art encryption for all systems used to send personal data (e.g., encrypted email; encrypted FTP; etc.) ☐ Logging of all transfers of data across the network ☒ SSL encryption for all internet access portals ☒ Protection of data storage media and containers during physical transport ☐ Enforced encryption of all drives that are used to take data off the network
	(B) Ensuring confidentiality, integrity, availability and resilience	**Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:** ☐ Binding agreements in writing with all personnel who process personal data, imposing strict confidentiality obligations ☒ 'Read' rights for systems containing personal data restricted to specified personnel roles ☒ 'Edit' rights for systems containing personal data restricted to specified personnel roles or profiles ☒ Logging of all attempts to access systems containing personal data (e.g., recording IP addresses and attempted password and username combinations) ☒ Personnel training regarding access to personal data

Data Protection Impact Assessment – Part II: Security Measures		
	(C) Ability to restore and access Relevant Personal Data	**Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:** ☒ Documented disaster recovery procedures ☒ Secure backup procedures in place, with full backups run regularly ☒ Multiple backup facilities and locations ☒ Uninterruptible power supplies at backup facilities ☒ Physical security of backup facilities (e.g., secure premises; security personnel; etc.). ☒ Security alarm systems at backup facilities ☒ Electronic security of backup facilities (e.g., firewalls; antivirus software; etc.) ☒ Environmental controls at backup facilities (e.g., cooling; humidity controls; etc.) ☒ Fire protection at backup facilities (e.g., sprinkler systems; fireproof doors; etc.) ☒ Secure anonymisation or deletion of personal data that are no longer required for lawful processing purposes ☒ Personnel training regarding backups and disaster recovery
	(D) Testing of security measures	**Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing:** ☒ Regular review of IT systems and security measures ☒ Regular security compliance checks ☐ Regular penetration testing ☒ Effective reporting structures for escalating security issues and concerns ☒ Personnel training regarding access to IT systems
	(E) User identification and authorisation	**Measures for user identification and authorization:** ☒ IT security systems requiring individual users to log in using unique usernames ☒ 'Edit' rights for systems containing personal data restricted to specified personnel roles ☒ Regular reviews of compliance with the relevant agreements

Data Protection Impact Assessment – Part II: Security Measures		
	(F) Protection of data during transmission	**Measures for the protection of data during transmission:** ☒ Implementation of, and compliance with, appropriate data transfer mechanisms ☒ Use of encrypted transfer systems wherever possible ☒ Restrictions on transfer rights for systems containing personal data ☒ Personnel training regarding transfers of personal data
	(G) Protection of data during storage	**Measures for the protection of data during storage:** ☒ Logical separation of live or production data from backup data and development or test data ☒ Logical separation of drives containing relevant personal data from systems containing other data ☒ Separation of personnel processing the relevant personal data from other personnel ☒ Personnel training regarding data separation
	(H) Physical security	**Measures for ensuring physical security of locations at which personal data are processed:** ☒ Locked doors on all entrances / exits (e.g., electronic locks; physical locks; etc.) ☐ Presence of security personnel (e.g., security at the front desk). ☒ Access control systems (e.g., biometric security; access card security; etc.) ☐ CCTV systems ☐ Burglar alarm systems ☒ Additional physical security measures to protect IT systems (e.g., partitioned server room; etc.) (*please specify*): limited and logged access to any server room or data closet, and protections from environmental hazards
	(I) Events logging	**Measures for ensuring events logging:** ☐ Logging of all input actions in systems containing personal data ☐ Logging of all failed attempts to edit personal data ☐ Personnel training regarding editing of personal data

Data Protection Impact Assessment – Part II: Security Measures		
	(J) System configuration	**Measures for ensuring system configuration, including default configuration:** ☒ IT security systems requiring the use of strong / complex passwords ☒ IT security systems requiring the use of multi-factor authentication ☐ Additional system log-in requirements for particular applications ☒ Mandatory password changes at fixed intervals (e.g., every 6 months) ☒ Automatic locking of IT terminals and devices after periods of non-use, with passwords required to 'wake' the terminal or device ☐ Regular audits of security procedures (e.g., ISO 27000 series certification; SOC 2 certification; etc.)
	(K) Governance and management	**Measures for internal IT and IT security governance and management:** ☒ Implementation of appropriate internal governance structures ☒ Appointment of data protection roles at appropriate levels of seniority and oversight ☒ Implementation of appropriate internal reporting and escalation structures ☒ Implementation of, and compliance with, appropriate data processing policies
	(L) Certification / assurance of processes and products	**Measures for certification/assurance of processes and products:** ☐ Regular third-party audits of data processing activities ☐ Regular third-party audits of data processing products ☐ Regular audits of security procedures (e.g., ISO 27000 series certification; SOC 2 certification; etc.)
	(M) Data minimisation	**Measures for ensuring data minimisation:** ☒ Implementation of, and compliance with, appropriate data minimisation requirements in relevant policies ☒ Regular reviews of systems to ensure that the minimum necessary volume of personal data is collected and processed ☒ Functionality for locating and deleting data in accordance with applicable policies, or as required by applicable law ☒ Personnel training regarding data minimisation

Data Protection Impact Assessment – Part II: Security Measures		
	(N) Data quality	**Measures for ensuring data quality:** ☒ Implementation of, and compliance with, appropriate data quality requirements in relevant policies ☒ Regular reviews of systems to ensure, to the extent possible, that personal data are accurate and, where necessary, kept up to date ☒ Appropriate internal mechanisms for the reporting of inaccurate or outdated personal data ☒ Functionality for correcting or deleting inaccurate or outdated personal data ☒ Personnel training regarding data quality
	(O) Data retention	**Measures for ensuring limited data retention:** ☒ Provision of appropriate notice to data subjects regarding data retention periods ☒ Appropriate contractual provisions with processors regarding data retention and deletion ☒ Implementation of, and compliance with, appropriate data retention and deletion policies ☒ Personnel training regarding data retention and deletion
	(P) Accountability	**Measures for ensuring accountability:** ☒ Implementation of, and compliance with, appropriate data processing policies ☒ Enforcement and disciplinary measures in the event of non-compliance with applicable policies ☒ Binding agreements in writing governing the appointment and responsibilities of processors with access to the relevant personal data ☒ Binding agreements in writing governing the allocation of data protection compliance responsibilities between all controllers with access to the relevant personal data ☒ Regular reviews of compliance with the relevant agreements ☐ Personnel training regarding processing of personal data

Data Protection Impact Assessment – Part II: Security Measures		
	(Q) Data portability	**Measures for allowing data portability:** ☒ Implementation of, and compliance with, appropriate internal and external policies regarding data portability in compliance with applicable laws ☒ Functionality for effectively identifying relevant personal data ☒ Functionality for isolating relevant personal data and, where necessary, converting relevant personal data to a commonly used and machine-readable format ☒ Functionality for transmitting relevant personal data to another controller ☒ Personnel training regarding data portability
	(R) Erasure	**Measures for allowing erasure of data:** ☒ Implementation of, and compliance with, appropriate data retention and deletion policies ☒ Functionality for locating and deleting data in accordance with applicable policies, or as required by applicable law ☒ Personnel training regarding data retention and deletion

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
1. Details of the Relevant Processing Activity				
1.1. Details of the Relevant Processing Activity	The details of the Relevant Processing Activity must be clearly defined	Clear ☒ / Unclear ☐		
1.2. Applicable sector-specific standards	Any sector-specific standards must be clearly explained	Clear ☒ / Unclear ☐		
1.3. Details of any Processors	The details of any and all Processors must be provided in full	Provided in full ☒ / Incomplete ☐		
	For each Processor a compliant Processing Agreement must be in all cases	Implemented in all cases ☒ / Missing in some cases ☐		

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
2. Categories of Relevant Data Subjects and Relevant Personal Data				
2.1. Details of the Relevant Personal Data	The details of the Relevant Personal Data must be clearly defined	Clear ☒ / Unclear ☐		
3. Legal bases for the Relevant Processing Activity				
3.1. Legal basis for Processing	The legal basis or bases applicable to the Relevant Processing Activity must be clear	Clear ☒ / Unclear ☐		
4. Data minimisation				
4.1. Steps taken to minimise the extent to which Relevant Personal Data are Processed	Appropriate measures must be implemented to ensure that Relevant Personal Data are adequate, relevant and not excessive	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
5. Data quality				
5.1. Steps taken to ensure that the Relevant Personal Data are accurate and up to date	Appropriate measures must be implemented to ensure that Relevant Personal Data are accurate and up to date	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
6. Data Retention				
6.1. Details of the applicable retention periods for Relevant Personal Data	Relevant Personal Data must not be retained for longer than is necessary in connection with a lawful purpose of Processing	Data are only retained as appropriate ☒ / Data may be retained for too long ☐		
7. Proportionality and necessity				
7.1. Explanation of how controls are implemented in respect of the Relevant Processing Activity	In addition to the measures noted above, suitable controls must be in place to ensure that Relevant Processing Activity is limited to a specified purpose	Suitable controls are in place ☒ / Suitable controls are **not** in place ☐		
8. Rights of data subjects				
8.1. Exemptions	All exemptions claimed by the Controller must be clearly defined	Clear ☒ / Unclear ☐		
8.2. The right to information	The required information must be provided to the Relevant Data Subjects	The required information is provided ☒ / The required information is **not** provided ☐ Please refer to Section 11.2 above.		
8.3.The right of access	The Controller must implement appropriate measures to give effect to the right of access	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐ Please refer to Section 11.3 above.		
8.4. The right to rectification	The Controller must implement appropriate measures to give effect to the right of rectification	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐ Please refer to Section 11.4 above.		

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
8.5. The right to erasure	The Controller must implement appropriate measures to give effect to the right to erasure	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐ Please refer to Section 11.5 above.		
8.6. Restriction of Processing	The Controller must implement appropriate measures to give effect to the right to restrict Processing	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐ Please refer to Section 11.6 above.		
8.7. The right to data portability	The Controller must implement appropriate measures to give effect to the right of data portability	Appropriate measures are in place ☐ / Appropriate measures are **not** in place ☒ Please refer to Section 11.7 above.		
8.8.The right to object	The Controller must implement appropriate measures to give effect to the right to object to the Relevant Processing Activity	Appropriate measures are in place ☐ / Appropriate measures are **not** in place ☒ Please refer to Section 11.8 above.		
9. Obtaining consent from Relevant Data Subjects				
9.1. Obtaining consent	Consent must be freely given	Freely given ☒ / **Not** freely given ☐		
	Consent must be specific	Specific ☒ / **Not** specific ☐		
	Consent must be informed	Informed ☒ / **Not** informed ☐		
	Consent must be unambiguous	Unambiguous ☒ / **Ambiguous** ☐		
	Consent must be evidenced	Evidenced ☒ / **Not** evidenced ☐		

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
10. Consultation with Relevant Data Subjects or their representatives				
Seeking views from Relevant Data Subjects or their representatives	The Controller must implement measures to seek, where appropriate, the views of Relevant Data Subjects or their representatives on the intended processing	Appropriate measures are in place ☐ / Appropriate measures are **not** in place ☒	As explained above, the Ethical Committees will be involved in the approval process of the Study. Therefore, the views of Relevant Data Subjects will be taken into consideration through the opinion of the relevant Ethical Committee.	
11. Data Security				
(A) Pseudonymisation and encryption	The Controller must implement appropriate measures to ensure pseudonymisation and /or encryption of Relevant Personal Data, where appropriate.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(B) Ensuring confidentiality, integrity, availability and resilience	The Controller must implement appropriate measures to ensure the confidentiality, integrity, availability and resilience of Relevant Personal Data.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(C) Ability to restore and access Relevant Personal Data	The Controller must implement appropriate measures to ensure that it can restore and access Relevant Personal Data.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(D) Testing of security measures	The Controller must carry out testing of its data security measures.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
(E) User identification and authorisation	The Controller must implement appropriate measures to ensure identification and authorisation of users or Personnel accessing Relevant Personal Data.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(F) Protection of data during transmission	The Controller must implement appropriate measures to ensure the security of Relevant Personal Data during transmission.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(G) Protection of data during storage	The Controller must implement appropriate measures to ensure the security of Relevant Personal Data during storage.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(H) Physical security	The Controller must implement appropriate measures to ensure the physical security of Relevant Personal Data.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(I) Events logging	The Controller must implement appropriate measures to ensure logging of events affecting systems that Process Relevant Personal Data.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(J) System configuration	The Controller must implement appropriate measures to ensure the security of Relevant Personal Data through appropriate system configuration.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(K) Governance and management	The Controller must implement appropriate data governance and management measures.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
(L) Certification / assurance of processes and products	The Controller must undertake appropriate certification, assurance, or other reviews of its data security measures.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(M) Data minimisation	The Controller must implement appropriate measures to ensure that the principle of data minimisation is applied to Relevant Personal Data.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(N) Data quality	The Controller must implement appropriate measures to ensure that the principle of data quality is applied to Relevant Personal Data.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(O) Data retention	The Controller must implement appropriate measures to ensure that Relevant Personal Data are not retained for longer than is needed.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(P) Accountability	The Controller must implement appropriate measures to ensure that it can satisfy its accountability obligations.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		
(Q) Data portability	The Controller must implement appropriate measures to ensure that its security measures allow for the right of Data Portability.	Appropriate measures are in place ☐ / Appropriate measures are **not** in place ☒ Please refer to Section 11.7 above.		
(R) Erasure	The Controller must implement appropriate measures to ensure that Relevant Personal Data are erased once they are no longer needed.	Appropriate measures are in place ☒ / Appropriate measures are **not** in place ☐		

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**

Data Protection Impact Assessment – Part IV: Sign off and record outcomes	
Item	**Statement**
1. Outcomes of the DPIA	The data processing activities related to the Study may entail the following risks for Data Subjects' rights and freedoms: a) the access to patients' Personal Data without they are being aware, including data related to health, and the related loss of confidentiality. b) the use of Personal Data for purposes other than those of the Study; and c) unwanted erasure of Personal Data. The sources of risk for personal data processed may include: a) either internal sources, operating - accidentally or intentionally - inside Pfizer, such employees, users and/or IT administrators of Pfizer. b) or external sources, operating - accidentally or intentionally - outside Pfizer, including non-human sources, such as competing agents, water, dangerous materials, generic computer viruses, computer attacks, etc., or external sources, such as the Company's IT system.
2. Review of Consultation with Relevant Data Subjects or representatives	No specific consultation will be carried out. However, Pfizer, has requested the opinion of the geographically competent Ethical Committees, which will approve the Study and the underling Processing.

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
3. Summary of advice and sign-off by Data Protection Officer	In order to mitigate the above risks deriving from Processing (i.e., Illegitimate access to Relevant Personal Data, Unwanted change to Relevant Personal Data, Disappearance of Relevant Personal Data), Pfizer has adopted a series of technical and organizational security measures in accordance with the GDPR, the Rules of Ethics for processing carried out for statistical or scientific research purposes dated December 19, 2018 and the Guidelines for the processing of personal data in the context of clinical trials of medicines dated July 24, 2008 and issued by IDPA. In particular: a) Pfizer, also with the support of the CRO: ▪ identifies and appoints as persons in charge of the processing all employees and/or consultants of the company who process data that are relevant for the purposes of the Study as part of their work activities, providing them with specific instructions on the Processing of Personal Data. ▪ subjects the same persons in charge of the Processing to training in order to make them aware of the security measures to be taken for the proper and safe processing of Personal Data within the Study and of the obligations provided for by data processing legislation. ▪ identifies and appoints, giving appropriate instructions, the third parties involved - as data processors - in the performance of the activities related to the Study. ▪ adopts specific procedures and policies regarding the processing of personal data (i.e. Standard Operating Procedures (SOPs)); b) Pfizer adopts, and/or requires the CRO to adopt, measures which provide: ▪ the omission of patients' identified data (i.e. name, surname, date of birth, etc.) from any report, publication or other disclosure, except where required by applicable laws. ▪ the storage of patients' Personal Data in encrypted electronic form, protected by a password ensuring that only expressly identified and authorised personnel have access to data. ▪ the recovery of Personal Data Processed in the event of a catastrophe or any other event that may be qualified as a data breach. In the event of a potential or actual data breach, the CRO will be responsible for determining whether a data breach has actually occurred and, in such case, notifying Pfizer of the event, providing all information necessary to enable Pfizer to make the notifications required under Articles 33 and 34 of the GDPR, where necessary.			**DPO Sign off:** Name: Ms. Chiara Formenti-Ujlaki, Date: 31 Jul 2025 04:53:011-0400 Signature: Chiara Ujlaki 92683c9a-b065-4fbf-939c-cc308cce2648

Data Protection Impact Assessment – Part III: Review, remediation and mitigation				
Issue	**Risk**	**Are the applicable requirements satisfied?**	**Proposed mitigation**	**Residual Risk**
4. Monitoring ongoing compliance of processing with DPIA	**This DPIA will be kept under review by:** Elena Iattoni Sr Oncology Medical Affairs Scientist, Pfizer srl Via Valbondione 113, 00188 Rome (Italy)			

Appendix 1 – Definitions

- "**Applicable Law**" means any binding law, legislation, rule, regulation, order, or directive (as amended, re-enacted, consolidated or replaced from time to time) that is applicable to Pfizer or any Pfizer Personnel.

- "**Controller**" means the entity that decides how and why Personal Data are Processed. In many jurisdictions, the Controller has primary responsibility for complying with applicable data protection laws.

- "**Data Subject**" means a living individual to whom Personal Data relate.

- "**DPO**" means a Data Protection Officer.

- "**GDPR**" means Regulation (EU) 2016/679.

- "**Personal Data**" means information that is about any individual, or from which any individual is directly or indirectly identifiable, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

- "**Personnel**" means Pfizer's current, former and prospective consultants, employees, officers, temporary personnel, individual contractors, interns, secondees and other personnel.

- "**Process**", "**Processing**" or "**Processed**" means anything that is done with any Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- "**Processing Agreement**" means an agreement appointing a Processor in conformity with the requirements of Article 28 of the GDPR.

- "**Processor**" means any person or entity that Processes Personal Data on behalf of the Controller (other than employees of the Controller).

- "**Relevant Data Subject**" means a Data Subject whose Personal Data are Processed in the context of the Relevant Processing Activity.

- "**Relevant Personal Data**" means Personal Data that are Processed in the context of the Relevant Processing Activity.

- "**Relevant Processing Activity**" means the Processing activity to which this DPIA relates.

- "**Sensitive Personal Data**" means Personal Data about race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life, any actual or alleged criminal offences or penalties, national identification number, or any other information that are deemed to be sensitive under applicable law.