Assessment Details

ID 2598

Name PIA - MA Clinical Study: Non-interventional 7465-MA-3500

Organization Medical Affairs

Completed Date 27/02/24 07:58 PM

Last Update 27/02/24 07:58 PM

Result Approved with Risk Mitigation

Template Version 19

Open Risk Count 4

Assessment Questions

1 Project Information

1.1 **Please select the processing activity which is the subject of this project or change.**

Response

MA Clinical Study: Non-interventional | Astellas Group

1.2 **Project Name (if applicable)**

Response

MA Non-Interventional study 7465-MA-3500

1.3 **Has there been a High-Risk Category identified ?**

Response

MA Clinical Study: Non-interventional | Astellas Group

Response

Sensitive Personal Data

2 PIA is Required?

2.1 **According to the facts of the processing activity as presented in the relevant entry is a PIA required?**

The following criteria should be considered in order to determine whether a Project triggers an obligation to conduct a DPIA, namely it may result in a high risk to the rights and freedoms of the data subjects impacted by the Project:

1. Sensitive Personal Information: The Project involves processing of special categories of data such as data that identifies racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, sex life or sexual orientation, criminal information, genetic data or biometric data where processed to uniquely identify a person. It may include also some other categories of data that can be considered as increasing the possible risk to the rights and freedoms of individuals. These Personal Information are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud);
2. Automated Decision Making: The Project has the capability of making decisions that produce a legal or similarly significant effect, solely by utilizing automated means (i.e., without any human involvement in the decision-making process);
3. Systematic Monitoring: The Project involves the systematic observation, monitoring, or control of individuals, from which Personal Information can be gathered and processed;
4. Large Scale Processing: the Project involves processing of large volumes of Personal Information. There is no definite number to set a threshold. The following factors, in particular, shall be considered when determining whether the processing is carried out on a large scale: (a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; (b) the volume of data and/or the range of different data items being processed; (c) the duration, or permanence, of the data processing activity; (d) the geographical extent of the processing activity;
5. Matching or combining various databases or datasets: for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject;
6. Evaluation or scoring of data subjects including profiling and predicting, especially from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements;
7. Processing of data concerning vulnerable data subjects such as children, ethnic minorities, patients, etc.;
8. Innovative use of technological or organizational solutions: The Project introduces a novel technology or an innovative organizational solution;
9. A Project, which involves a processing activity, which may prevent data subjects from exercising a right or using a service or a contract: this includes processing operations in a Project that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract;
10. A Project which involves a processing activity, which is not falling within any of the above categories, for which a relevant data protection authority has officially declared that a PIA is required;
11. A Project, which involves a processing activity, which is not falling within any of the above categories, but still, according to the evaluation of the Project Owner, presents a high risk to data subjects.

Response

Yes

Justification

Pseudonymized/coded personal data of patients will be processed by the sponsor to run the study.

3 Personal Information Collection

3.1 **Does this processing activity involve the monitoring or surveillance of data subjects?**

Monitoring & Surveillance: the watching, listening to, or recording of a data subject's activities or behavior

Response

No

3.7 **Does this processing activity involve inquiries about individuals' personal information?**

Inquiries: asking individuals to divulge personal information or in general taking actions to find out data about a data subject. This includes both direct inquiries like e.g. application or registration forms or questionnaires completed by data subjects, but also indirect efforts to collect data about data subjects from third parties or from the public domain.

Response

Yes

3.8 **Do inquiries collect personal information that may be not strictly necessary or irrelevant to the purpose for which they are being collected? Is there a risk that the personal information collected under this processing activity will not be proportional to the purpose that is sought?**

Response

No

Justification

The required personal information specified under the protocol and are necessary to achieve the objectives of the study.

3.9 **Do inquiries collect personal information that may be perceived by data subjects as not being of good enough quality for the purposes it is used for?**

Response

No

Justification

Data collection will be carried out by means of EDC systems whereby data recorded in an eCRF are directly registered in the study database. The eCRF for the study eCRF) will be provided by the CRO .
Only the study investigators/study coordinators have access rights to enter and to modify the data. It is the responsibility of the investigator to maintain adequate and accurate eCRFs to record all observations and other data pertinent to the study.
Appropriate edit checks will be developed to identify the discrepancies in the entered data, embedded in the database, to ensure data validity. Discrepancies may be due to inconsistent data, missing data, range checks and deviations from the protocol. The data validation process will be run every night and queries will be released in the eCRF for identifying discrepancies. These discrepancies (queries) will be resolved by investigators after logging into the system. It is the investigator's responsibility to respond by confirming or modifying the data questioned.
Ongoing quality control of data processing is undertaken at regular intervals during the course of the study. A study-specific data management plan will be produced describing the data entry and data tracking guidelines, quality control measures, discrepancy management, data transfer/extraction and database locking guidelines.

Astellas will provide oversight of study activities that have been assigned to the CRO , responsible for site management including monitoring, data management, data analysis and PRO activities. The Sponsor's designees implement and maintain quality assurance and QC systems with written SOP to ensure that the study is conducted and data are generated, documented and reported in compliance with the protocol, GCP, GPvP and applicable regulatory requirements. The CRO will be responsible for the programming of the eCRF as well as for ensuring that data queries generated during these processes are maintained in the study QC log.

3.10 **Can any inquiries be perceived by a data subject as unjustifiably coercive or excessively probing? (Keeping in mind that sometimes not answering an intrusive question may be perceived coercive in a given context)**

Data subjects may feel a degree of unjustifiable coercion because not answering a question might create the impression that they have something to hide, whereas this may not be the case but they may simply want to justifiably refuse answering a particular question. Asking excessively probing questions can thus make the data subjects being questioned feel uncomfortable or be concerned about how they will explain themselves or how even their refusal to answer will appear to others.

Response

(No)

Justification

The investigator or his/her representative will explain the nature of the study to the participant and answer all questions regarding the study. Participants will be informed that their participation is voluntary and shall have their protective rights and guarantees explained, including their privacy rights. In particular, their right to refuse to participate and the right to withdraw from the study at any time without any resulting detriment and without having to provide any justification shall be explained.

3.11 **If the prior consent of data subjects is sought to support any inquiries, is there a risk that the consent language is not clear enough to inform appropriately data subjects about the personal information collection and processing?**

Response

(No)

Justification

The consent form that will be used for the primary data collection will be reviewed by Astellas. Regarding the secondary data collection, Astellas will seek approval from Garante as it is expected that patients may have in the meantime been deceased.

3.12 **In this case of prior consent collection, is there any risk to data subjects from inadequate processes to collect, record and store the consent forms, so that they are easily retrievable especially if data subjects want to revoke their consent and exercise their rights?**

Response

(No)

Justification

The informed consent shall be kept in the Investigator's study file. The medical record must include a statement that written informed consent was obtained before the participant was enrolled in the study and the date the written consent was obtained. The authorized person obtaining the informed consent must also sign the ICF.

3.13 **Can such inquiries elicit answers that may be used to create arbitrary inferences or conclusions or impressions?**

Response

(No)

3.14 **If inquiries collect personal information not directly from data subjects but from third parties, does this method of inquisitiveness infringe any reasonable expectation of privacy of the data subjects impacted?**

Response

(Not Applicable)

3.15 **Does this processing activity run the risk to be perceived by the data subjects that it is not transparent and is unacceptably covert creating thus a sense of discomfort and powerlessness for the data subjects impacted?**

Response

No

Justification

An informed consent and privacy notice will be provided as part of the ICF which will inform patients about the processing of their personal data

3.16 **If there is a claim that there is an exemption from the duty to provide adequate privacy notice to data subjects, is this appropriately justifiable according to the applicable legislation without creating any unaccepted risk for data subjects?**

Response

No

Justification

For the secondary data collection where it may be impossible to provide privacy notice either because patients are deceased in the meantime or because patients do not attend follow up anymore, for this case Astellas will seek the favorable opinion of the data protection authority in Italy.

3.17 **Is there any risk that data subjects will not have capabilities or adequate resources in place to exercise their data protection rights?**

Response

No

Justification

Study participants will be informed about their data protections rights in the Informed Consent form. Regarding the deceased patients of whose data will be processed as part of the secondary data collection, Astellas will seek the opinion of the data protection authority in Italy.

3.18 **"Is there a risk associated with this processing activity that will not allow data subjects to submit DSRs or even complaints to the data controller? "**

Response

No

Justification

Same as the previous question.

3.19 **Is there a risk that personal information will be collected without the data controller having a legal basis to process such personal information in accordance with applicable legislation, depriving thus data subjects from effective control and ownership over their own data?**

Response

No

Justification

Participants will be able to provide consent which is the legal basis Astellas relies on. For the deceased patients, Astellas will seek authorization from the data protection authority.

3.20 **If the legal basis for the collection and processing of personal information is data controller's legitimate interest to conduct business in this business area, has a Legitimate Interest Assessment test completed which has established that there is no privacy right or freedom of individuals that overrides Astellas legitimate interest?**

Response

Not Applicable

4 Personal Information Processing

4.1 **Does this processing activity involve aggregation?**

Aggregation: the combination of various pieces of personal information about a data subject: the "whole becoming larger than the parts"

Response

Yes

Justification

The Sponsor will use the coded personal information collected from participants to run the study and to use and publish the results of the study in aggregated format.

4.2 **Does the combination of personal information happen in new, potentially unanticipated ways that reveal facts about a data subject that are not readily known and unsettle their expectations on privacy?**

Response

No

Justification

There is a protocol in place which defines what is collected and how/why is processed for research purposes only.

4.3 **Is there a risk that a data compilation will be ultimately inaccurate?**

Response

No

Justification

The data collected and processed are of a certain quality and they will be under a protocol.

4.4 **Is there a risk that data subjects will be treated with bias/prejudice/discrimination based on their identities if any pseudonimized data used in this processing activity is reversed?**

Response

No

Justification

The risk of reidentification is low.

4.5 **Can the identification of data subjects inhibit their ability to change and prevent their self-development?**

Response

Not Applicable

4.6 **Is there any indication of an increased risk of data loss and/or data leakage based on information available?**

Response

Not Sure

Justification

Mitigation action: to ensure that any system used to store data is assessed for security.

Risks

Risk Category

3rd Party Risk

Stage

Identified

Treatment Plan

Ensure that any system used by the vendor to store personal information is assessed for security.

4.7 **Is there a risk that there are no adequate and appropriate technical and organizational measures to ensure the integrity, confidentiality and availability of the personal information for data subjects?**

Response

Not Sure

Justification

Mitigation action: The data processor involved shall undergo the Astellas process regarding privacy due diligence.

Treatment Plan

Ensure that the vendor involved has undergone privacy due diligence.

4.8 **Is there a potential for secondary use that can have a significant negative effect on data subjects' lives?**

For example, secondary uses may undermine people's expectations about how the data they give out will be used. People might not give out data if they know about a potential secondary use. The harm to individuals may emerge from denying people control over the future use of their data, which can be used in ways that have significant effects on their lives.

Response

No

4.9 **If there is a potential for secondary use in a given case, are there circumstances revealing that the information may not fit well with the new, secondary use?**

Response

No

Justification

Data will be collected for scientific research purposes.

4.10 **Is there a risk to data subjects that their personal information will be retained for an unlimited period of time and without a link to the necessity principle creating thus an unacceptable degree of loss of control over their own data and the risk of using outdated data?**

Response

No

Justification

A retention period has been defined.

4.11 **Does this processing activity follow a set of documented processes and controls or does it create a risk to data subjects that there is a loose environment that cannot afford adequate protection to their personal information while it is at the possession of the data controller?**

Response

No

4.12 **Does this processing activity create a risk that it introduces increased complexity or novelty that can cause major disruption if only a minor glitch happens?**

Response

Not Applicable

4.13 **Does this processing activity involve the risk of personal information being altered or modified in a way that will not be accurate?**

Response

No

Justification

There is a scientific protocol that defines how data is collected and analyzed.

5 Personal Information Dissemination

5.1 **Is there a relationship between the data subject and another party involved in the activity that is built upon trust or a fiduciary duty that may be breached and cause to data subjects a sense of betrayal or embarrassment?**

Response

No

5.2 **Does this processing activity create a risk to confidentiality of the impacted personal information?**
Typical weaknesses in this area can be subsumed under the following four categories or use cases:

1. *Workplace: Personal information can be processed without authorization via the workplace, for example if the computer at the workplace is successfully attacked by malware or documents stored at the workplace are viewed without authorisation*
2. *Data transmission. – Personal information can be transmitted via digital interfaces, physical transport or orally and processed by unauthorized persons.*
3. *Data swapping. – Digital personal information can be exported and outsourced from the IT system in which the technical processing is carried out on an ongoing basis, even without the intention of transmitter (e.g. data printout on paper or export to digital media such as data backup tapes, USB sticks, laptop and log file) and then processed without authorization by accessing the outsourcing location.*
4. *Direct access to technical storage location. – Unauthorized persons can circumvent existing access protection and process personal information using the direct access they gain to the technical storage location (e.g. database).*

Response

(Not Sure)

Justification

Mitigation action: On the CRO (data processor) side, access to data shall only be allowed strictly and only to individuals with "a need to know".

Risks

Risk Category

Confidentiality, Availability, 3rd Party Risk

Stage

Identified

Treatment Plan

Ensure that on the CRO side only individuals with a strict need to know have access to data.

5.3 **Does this processing activity create a risk of disclosure of personal information that can prevent people from engaging in activities that further their own self-development or inhibit them from associating with others or impinge upon their freedom of association, or destroy anonymity, which is sometimes critical for the promotion of free expression?**

Response

(No)

5.4 **Does this processing activity create a risk of distorting our assessment for a data subject in a manner that will not be justifiable?**

Response

(No)

5.5 **Does this processing activity create a risk of spreading information beyond existing networks of information flows that are expected and anticipated?**

Response

No

5.6 **Is there a risk to data subjects that they lose the control of their data if it is shared with third parties or that personal information is not shared with third parties with adequate controls in place?**

Response

Yes

Justification

Mitigation action: Ensure that access to data on the CRO (data processor) side is only permitted strictly to individuals with "a need to know".

Risks

Risk Category

3rd Party Risk, Confidentiality

Stage

Identified

Treatment Plan

Ensure that access to data on the CRO side is restricted only to individuals with a need to know and that the CRO has adequate controls in place.

5.7 **Does this disclosure of personal information create a risk of a transfer of personal information of data subjects to organizations or entities located in third countries that do not afford adequate protection as per the privacy laws of the country of origin without an appropriate and adequate transfer mechanism?**

Response

Yes

Justification

Transfer Impact Assessment of the CRO involved is completed.

5.8 **Does this processing activity create a risk of impinging on a data subject's freedom in the authorship of his/her self-narrative and his/her self-development?**

Response

No

5.9 **Does this processing activity create a risk for data subjects being inaccurately exposed to the public, thus damaging their self-identify and ability to engage in public life?**

Response

No

6 Invasion

6.1 **Does this processing activity create a risk for data subjects being deprived a reasonable private space that provides to data subjects a reasonable and anticipated level of comfort, ease, and relaxation?**

Response

No

6.2 **Does this processing activity create a risk that people will feel powerless and/or be deprived from rights and/or feel biased or prejudiced from any automated decision-making process that does not involve them or any other human element?**

Response

Not Applicable

7 Collaboration & Communication with Stakeholders

7.1 **Have the individuals involved been given an opportunity to express their views on the activity?**

Response

Not Applicable

7.2 **Have you received the view of the Group DPO on this data processing activity?**

Response

The processing activity can be implemented - the controls are sufficient to guarantee the respect of data subjects' privacy, pending all controls being implemented.

7.3 **Have you involved other internal and external stakeholders in the assessment of this processing activity?**

Response

No

7.4 **Have you involved any data processors to assist in the risk assessment of this data processing activity? If yes, what was the outcome or the input received from data processors?**

Response

Yes

Justification

The CRO is assisting with the documentation prepared to submit to the Garante

7.5 **Is there a code of conduct which is applicable to this activity that has been taken into account?**

Response

No

8 Validation

8.1 **In the previous sections, have you identified any risks?**

Response

Yes

Justification

Risks have been flagged.

8.2 **If yes, are you planning to develop a treatment plan that will effectively mitigate the identified risks?**

Response

Yes

8.3 **What is the overall assessment of the processing activity?**

Response

The processing activity can be implemented only after the identified risk treatment plan is completed. This will be defined in the review phase of this Assessment by raising a Risk and the defining the underlying Tasks to mitigate the Risk.