

DATA PROTECTION IMPACT ASSESSMENT

CONCORDIA Project

Data Controller: Arbor Research Collaborative for Health

Table of Contents

- 1. Introduction
- 2. Essential Information
- 3. Risk Estimation and Pre-Assessment
- 4. Processing Information
- 5. Proportionality Assessment
- 6. Rights and Fundamental Principles
- 7. Risk Assessment
 - 7.1 Security Measures
 - 7.2 Risk Assessment Detail
- 8. Stakeholder Involvement
- 9. Notes

1. Introduction

This document, "Data Protection Impact Assessment – CONCORDIA Project", aims to assess the impact on data protection of the processing activity "CONCORDIA Project". The impact is evaluated with particular attention to the rights and freedoms of data subjects.

Data Controller: [Arbor Research Collaborative for Health](#)

2. Essential Information

Analysis creation date	23/02/2026
Document generation date	23/02/2026
Status	In progress

3. Risk Estimation and Pre-Assessment

3.1 Pre-Assessment

Type of Processing	Response
Evaluative or scoring treatments on a large scale, as well as treatments involving profiling of data subjects and predictive activities (also online or through apps), relating to professional performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of the data subject.	No
Automated processing aimed at making decisions producing "legal effects" or "significantly affecting" the data subject in a similar manner, including decisions that prevent the exercise of a right, prevent access to a product or service, or prevent continuation of an existing contract (e.g. screening of bank customers using credit bureau data).	No
Systematic use of data for observation, monitoring or control of data subjects, including data collection through networks (also online or through apps), as well as processing of unique identifiers capable of identifying users of information society services including web services, interactive TV, etc. with respect to usage habits and viewing data over extended periods. Also includes processing of metadata (e.g. in the telecommunications and banking sectors) carried out not only for profiling, but more generally for organisational reasons, budget forecasting, technology upgrades, network improvements, anti-fraud and anti-spam services, security, etc.	No
Processing of special categories of data pursuant to Art. 9 or data relating to criminal convictions and offences under Art. 10 of EU Regulation 2016/679 interconnected with other personal data collected for different purposes.	Yes
Large-scale processing of data of an extremely personal nature: this includes, among others, data related to family or private life (such as electronic communications data whose confidentiality must be protected), data affecting the exercise of a fundamental right (such as location data, whose collection calls into question freedom of movement), or data whose breach would have a serious impact on the daily life of the data subject (such as financial data that could be used to commit payment fraud).	Yes
Non-occasional processing of data relating to vulnerable subjects (minors, disabled persons, the elderly, the mentally ill, patients, asylum seekers).	Yes
Processing carried out through the use of innovative technologies, also with particular organisational measures (e.g. IoT; artificial intelligence systems; use of online voice assistants through voice and text scanning; monitoring via wearable devices; proximity tracking such as Wi-Fi tracking), whenever at least one other criterion identified in WP 248, rev. 01 (WP 29 criteria) also applies.	No
Processing carried out in the context of an employment relationship through technological systems (including video surveillance and geolocation systems) that allow remote monitoring of employees (see WP 248, rev. 01, criteria nos. 3, 7 and 8).	No
Processing involving large-scale exchange of data between different data controllers via electronic means.	No
Systematic processing of biometric data, taking into account in particular the volume, duration, or persistence of the processing activity.	No
Systematic processing of genetic data, taking into account in particular the volume, duration, or persistence of the processing activity.	No

3.2 Risk Estimation

Risk Estimation Criteria	Response
The processing involves evaluation or scoring including profiling and prediction	No
The processing involves automated decision-making that has legal or similarly significant effects	No
The processing involves systematic monitoring	No
The processing involves sensitive data or data of a highly personal nature	Yes
The processing of data occurs on a large scale	Yes
The processing involves the creation of matches or combinations of data sets	No
The processing involves vulnerable categories of data subjects	Yes
The processing involves innovative use or application of new technological or organisational solutions	No
The processing prevents data subjects from exercising a right or availing themselves of a service or contract	No
Overall Risk Level	HIGH

4. Processing Information

Identifier	Name	Creation Date	Last Modified
0000	CONCORDIA Project	13/02/2026	23/02/2026

Description	Retrospective, observational, multicentre, international study aimed at evaluating differences in clinical and biochemical outcomes between adult haemodialysis patients treated with medium cut-off dialysers (MCO, Theranova®, Baxter) versus patients treated with high-flux haemodialysis (HF-HD). The processing consists in the collection, elaboration and analysis of clinical, demographic, laboratory, and dialysis-related data of patients with end-stage renal disease (ESRD) on chronic renal replacement therapy. The research activity involves retrospective analysis of data already present in medical records and healthcare information systems for the period January 2018 – January 2023. The cohort includes both living patients and patients who died during the observation period. For living and reachable patients, written informed consent is obtained; for deceased patients (and for living patients who can no longer be reached), processing is carried out pursuant to Art. 110 of Legislative Decree 196/2003 as amended, in compliance with the guarantee measures set out by the Italian Data Protection Authority (Garante) under Provision no. 298 of 09/05/2024. The study is conducted by Arbor Research Collaborative for Health (USA) as the international promoter, in collaboration with European DOPPS centres and centres with high Theranova utilisation in Italy, France, and the United Kingdom. AOUI Verona participates as a non-DOPPS centre with high Theranova utilisation.
--------------------	--

Purpose of Processing	Scientific research in the medical-biomedical field aimed at the comparative evaluation of clinical and biochemical outcomes in adult patients with end-stage renal disease (ESRD) undergoing renal replacement therapy with haemodialysis.
Legal Bases	• Article 6(a) – the data subject has given consent to the processing of their personal data for one or more specific purposes • Article 6(e) – processing 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 • Article 9(a) – the data subject has given explicit consent to the processing of special category personal data for one or more specified purposes • Article 9(j) – processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) based on Union or Member State law
Regulatory References	For Italian Research Centres: • For living and contactable patients: - Article 6(a) GDPR – consent to the processing of personal data for specific purposes - Article 9(a) GDPR – explicit consent to the processing of special category personal data for specific purposes • For deceased patients and living patients who cannot be reached: - Article 110 of Legislative Decree 196/2003, as amended by Decree-Law no. 19/2024 (converted by Law no. 56/2024) – processing of personal data for scientific research purposes without consent, in the cases provided for by law (deceased patients and living patients who can no longer be reached) - Guarantee measures set out by the Italian Data Protection Authority (Garante) under Provision no. 298 of 9 May 2024 General references: • Art. 89, EU Regulation 2016/679 • Provision of the Italian Data Protection Authority no. 298 of 09/05/2024 concerning guarantee measures for the processing of personal data in the context of scientific research
Data Origin	Pre-existing data (data were originally collected for the purposes of diagnosis, treatment and healthcare of patients undergoing chronic haemodialysis at the participating centres. The study is based on the analysis of data extracted from medical records and healthcare information systems for the period January 2018 – January 2023.)
Processing Method	Paper-based and Electronic
Data Categories	Special category personal data: Health data Common personal data: Identification data (patient code)
Categories of Data Subjects	Patients; Deceased persons; Investigators
Data Controller	Arbor Research Collaborative for Health
Other Data Controllers	Antrim Area Hospital, Northern Health and Social Care Trust; Association ECHO; ASST DEI SETTE LAGHI; ASST Spedali Civili Brescia; Aural Lyon; Department of Nephrology and Dialysis CHU Poitiers; La Fondation Charles Mion – AIDER Santé; University

	Hospitals of Derby and Burton NHS Foundation Trust; Azienda Ospedaliera Universitaria Integrata Verona (AOUI Verona) – as an autonomous co-controller participating in the study
Data Processors	CRA – EDTNA/ERCA (international association of nephrology healthcare professionals) – acting as data processor and representative of the data controller for coordination activities
Representative of the controller	CRA – EDTNA/ERCA (international association of nephrology healthcare professionals) – acting as representative of the data controller established outside the European Union, pursuant to Art. 27 GDPR
Data Protection Officer	Compliance Officer and Data Protection Officer: AOUI Verona: Dr. Filomena Polito ASST dei Sette Laghi: rpd@asst-spedalivicili.it ASST Spedali Civili Brescia: _Rosa Coppola_ rpd@asst-spedalivicili.it
Data Dissemination	No data dissemination is carried out.
Retention Period	10 years from the conclusion of the study. Upon expiry of the retention period: irreversible anonymisation of data.
Applications / Systems	Excel files for research – Specific security measure for the protected management of Excel files used temporarily during data collection and organisation prior to their transfer to dedicated platforms. Includes file encryption, password protection, digital signature with hash to ensure integrity, access limited to authorised personnel, and storage on secure network servers with controlled authentication. REDCap (Research Electronic Data Capture) – A web-based platform designed to support data capture and storage for clinical research studies.
Notes	Arbor Research Collaborative for Health manages the study data on HIPAA-compliant AWS cloud infrastructure (North America zone), using the REDCap platform with MySQL database. The IT environment is designed and operated with alignment to FISMA Moderate and NIST 800-53 and HITRUST standards. Implemented security measures include: AES-256 encryption at rest and minimum TLS 1.2 in transit, multiple firewalls, strong authentication, weekly backups, comprehensive audit logs, web/database server separation and data pseudonymisation. Security management is entrusted to a dedicated Information System and Security Committee.

4.1 Communications and Transfers

Recipient	Notes	Lawful basis for third-country transfer
Transfer of data between participating centres (autonomous controllers) and CRA (data processor / representative of the controller)	Communication of data for coordination, monitoring and support activities for data collection at the Italian participating centres. Operates within the CONCORDIA research network activities as the designated entity for study coordination functions.	N/A (intra-EU transfer)

Data communication between Participating Centres (autonomous controllers) and the Promoter (autonomous controller – Arbor Research Collaborative for Health, USA)	Pseudonymised data are transferred to Arbor Research (USA) as independent data controller (study promoter), pursuant to the Data Use Agreement (DUA) incorporating Standard Contractual Clauses (SCCs) for transfer to a third country, pursuant to Arts. 44-46 GDPR.	Standard Contractual Clauses adopted by the European Commission (EU Standard Contractual Clauses), as supplemented by EDPB Recommendations 01/2020 (18/06/2021) – measures that supplement transfer instruments to ensure compliance with the level of protection of personal data.
---	---	---

5. Proportionality Assessment in Relation to the Purpose

Taking into account that the processing activity subject to this assessment involves the processing of the special categories of personal data mentioned above, in relation to the categories of data subjects previously identified, the Data Controller considers that those categories of data are necessary and proportionate to the pursuit of the following purpose:

Scientific research in the medical-biomedical field aimed at the comparative evaluation of clinical and biochemical outcomes in adult patients with end-stage renal disease (ESRD) undergoing renal replacement therapy with haemodialysis.

6. Rights and Fundamental Principles

6.1 Rights

Right	Description / Measures
Right of Access	The information required by Art. 13 and Art. 14(5)(b) GDPR is made available in a transparent and easily accessible manner to data subjects. It is included in the information notice provided to data subjects prior to enrolment. The same notice has been published on the company website to allow dissemination in the case of unreachable patients. Access requests are handled following a dedicated company procedure that ensures the proper organisation and management of such requests. To ensure that data are made available only to the data subject concerned, identity is carefully verified before processing any request.
Right to Rectification	Data subjects may at any time exercise the right to rectification of inaccurate personal data concerning them. In this regard, the provisions of Art. 110(2) of Legislative Decree 196/2003 apply, whereby "in the case of exercise of data subject rights under Article 16 of the Regulation in respect of the processing referred to in paragraph 1, the rectification and integration of data shall be noted without modifying them, where the result of such operations does not produce significant effects on the research outcome". The information required by Art. 13 and Art. 14(5)(b) GDPR is made available in a transparent and easily accessible manner to data subjects through the information notice provided prior to enrolment and published on the company website.
Right to Erasure	Data subjects have the right to obtain erasure of their personal data from the Data Controller where one of the grounds set out in Art. 17(1) GDPR exists. It is understood that, in the event of withdrawal of consent by the data subject, no further data concerning them will be collected, but data already collected may be used to determine, without altering them, the results of the

	research. Information is provided via the information notice delivered prior to enrolment and published on the company website.
Right to Data Portability	The information required by Art. 13 and Art. 14(5)(b) GDPR is made available in a transparent and easily accessible manner to data subjects through the information notice provided prior to enrolment and published on the company website.
Right to Object	Data subjects may exercise the right to object to processing where the conditions of Art. 21(1) GDPR are met. Furthermore, pursuant to Art. 21(6) GDPR, the data subject, on grounds relating to their particular situation, has the right to object to the processing of personal data concerning them, unless processing is necessary for the performance of a task carried out in the public interest and always subject to a written request. Information is provided via the information notice delivered prior to enrolment and published on the company website.
Right to Restriction of Processing	Data subjects have the right to obtain restriction of processing from the Data Controller where one of the situations set out in Art. 18(1) GDPR applies. Information is provided via the information notice delivered prior to enrolment and published on the company website.
Right to Withdraw Consent	The information required by Art. 13 and Art. 14(5)(b) GDPR is made available in a transparent and easily accessible manner to data subjects through the information notice provided prior to enrolment and published on the company website.
Right not to be subject to automated decision-making	No processing is carried out that involves a decision based solely on automated processing.

6.2 Principles

Principle	Description / Measures
Personal data are processed lawfully, fairly and transparently with respect to the data subject	Data are collected for use for scientific purposes relating to the Study. All information collected is adequate and relevant, as it is aimed solely at defining risk factors, clinical picture, prognostic factors and current or future therapeutic options. All collected data will be processed by competent personnel in the relevant conditions, previously authorised to process data pursuant to Art. 29 GDPR or designated with specific tasks pursuant to Art. 2-quaterdecies of Legislative Decree 196/2003, duly trained, who will assess their accuracy and compliance with the Study protocol. The database on which data are recorded features automatic validation systems capable of detecting possible inconsistencies. Prior to data acquisition, the investigator or an authorised delegate provides each contactable patient with an appropriate information notice and makes a public information notice available, pursuant to Art. 14(5)(b), in order to inform and obtain consents for: (a) participation in the Study; (b) processing of personal data necessary for the Study; (c) publication of personal data relating to the Study in pseudonymised form at scientific conferences or for scientific publications; (d) transfer of data to third countries [if applicable]; (e) knowledge of Study results where they represent a direct and concrete benefit in terms of therapy, prevention or reproductive choices [if applicable for studies involving genetic data]; (f) knowledge of unexpected findings where these represent a direct and concrete benefit in terms of therapy, prevention or reproductive choices [if applicable for studies involving genetic data]; (g) communication of Study results, where they represent a direct and concrete benefit in terms of therapy, prevention or reproductive choices, to members of the same genetic lineage of the data subject,

	upon their request [if applicable for studies involving genetic data]. Furthermore, the fundamental principles of Art. 5 GDPR are respected in the processing of data subjects' personal data during the Study.
Data are collected for specified, explicit and legitimate purposes and are not further processed in a manner incompatible with those purposes	The purposes of processing are those indicated above and are set out in the information notice provided to patients prior to the start of processing. As regards subsequent processing, data will be used to contact patients to assess willingness to participate in future research projects duly authorised by the competent Ethics Committee, following delivery of an information notice and collection of specific consent, or, in the case of deceased or unreachable patients, following completion of the obligations under Art. 110 of the Privacy Code and the guarantee measures set by the Garante on 09/05/2024.
Data are stored in a form that permits identification of data subjects for no longer than necessary to achieve the purposes for which they are processed	Data concern data subjects identified according to the inclusive criteria described in the study protocol. These data will be collected from the approval of the Study by the competent Ethics Committee and the completion of all obligations under Art. 110 of the Privacy Code and the guarantee measures set by the Garante. Data will be retained for the periods set out in the study protocol in a form that does not directly permit identification of data subjects; after this period, data will be destroyed. The pseudonymisation technique used with REDCap is the counter method (ENISA Guidelines, November 2019), which consists in replacing identifiers with a unique sequential number automatically generated by the system.
Data are processed in a manner that ensures adequate security of personal data	Data reside on the REDCap platform owned by AOUI Verona (https://redcap.aovr.veneto.it) and will be collected using an eCRF (electronic Case Report Form) created specifically for the Study. The REDCap software (Research Electronic Data Capture) is a web-based platform designed to support data capture and storage for research studies; it incorporates a user privilege management system to control data export, viewing and modification, and provides audit trails to monitor data manipulation and export procedures. Following the counter method of pseudonymisation as per ENISA Guidelines (November 2019), the platform generates a unique numeric code associated with each subject involved in the Study, allowing researchers to maintain locally the association with the respective identifying data. The possibility of re-identifying data is justified by the need to conduct follow-up studies for patients under treatment at the participating Units, or in the event of scientific results that may have a direct and concrete impact on the data subject, based on decisions expressed in the informed consent to participation in the Study. REDCap is installed on AOUI servers and daily backups are performed; the connection to the platform is encrypted with an SSL digital certificate and access to the database is permitted only to Study personnel via REDCap accounts with two-factor authentication (2FA). Access requires a username and password (first factor) of at least fifteen characters, including at least one number, one uppercase letter, one lowercase letter and one special character, changed monthly; the second factor is a time-limited numeric code sent to the email address linked to the account.

7. Risk Assessment

In order to calculate the magnitude of a risk, the following formula is adopted:

$$R_1 = f(M, p)$$

IMPACT (M)

Level	Value
MINOR	1
MODERATE	2
HIGH	3
VERY HIGH	4

PROBABILITY (p)

Level	Value
UNLIKELY	1
LOW PROBABILITY	2
PROBABLE	3
HIGHLY PROBABLE	4

INITIAL RISK (R)

Level	Range
LOW	1 – 2
MEDIUM	3 – 4
HIGH	5 – 8
VERY HIGH	9 – 16

Where:

- **R** – refers to the unmitigated risk level;
- **M** – refers to the impact on the rights and freedoms of data subjects, rated from 1 to 4;
- **p** – refers to the probability of the risk occurring, rated from 1 to 4.

Level	Description
Minor	Data subjects will not be affected, or at worst may encounter some inconveniences which they will overcome without any problem.
Moderate	Data subjects may encounter inconveniences which they will be able to overcome, albeit with some difficulty.
Severe	Data subjects may encounter significant consequences which they should be able to deal with, albeit with serious difficulties.
Very Severe	Data subjects may be confronted with significant or irreversible consequences.

Residual risk formula:

$$R_2 = R_1 - (M_n)$$

Where R_2 is the final risk (after security measures), R_1 is the initial risk, and M_n represents each control or security measure applied.

7.1 Security Measures

Cross-cutting Security Measures Relating to Processing Activities

No measures selected.

Cross-cutting Security Measures Relating to Assets

No measures selected.

Specific Security Measures Relating to the Processing

Category	Measure	Implementation Status
ENISA Security Measures	Existence within the organisation of a policy regarding the protection of personal data as part of the information security policy, taking into account the main aspects relating to data processing.	Implemented
	Clear definition and assignment of roles and responsibilities relating to personal data processing, in accordance with the security policy.	Implemented
	Clear definition of procedures for revoking user rights and responsibilities in the event of internal reorganisations, terminations or changes of employment, with the respective handover procedures.	Implemented
	Existence of a detailed and documented access control policy, with related role segregation.	Implemented
	Existence of a register of IT resources used for personal data processing (hardware, software and network), to be kept constantly updated.	Implemented
	Definition of formal guidelines and procedures, including appropriate forms, relating to the processing of personal data by data processors (contractors/outsourcers).	Implemented
	Definition of a security incident response plan, with detailed procedures to ensure an effective and orderly response to such incidents.	Implemented
	Definition of a procedure for the identification, management and recording of personal data breaches, including any notification to the Data Protection Authority and communication to data subjects.	Implemented
	Existence of procedures and controls to ensure the required level of continuity and availability of the IT system processing personal data (in the event of a security incident / personal data breach).	Implemented
	Ensuring that all personnel are adequately informed about the IT system security controls relating to their work activities. Personnel involved in personal data processing should also be adequately informed about data protection requirements and legal obligations through regular awareness campaigns.	Implemented

	Definition of documented procedures for the management of mobile and portable devices (e.g. smartphones, tablets, laptops).	Implemented
Organisational Security Measures	Existence of staff training procedures on data protection, including security profiles.	Implemented
	Confidentiality obligations for personnel with regard to personal data processed.	Implemented
	Existence of a procedure for managing security incidents.	Implemented
	Definition of roles and responsibilities with third parties in the area of IT security and data protection.	Implemented
	Issuance of appropriate instructions regarding personal data processing to all persons involved in the procedure.	Implemented
Technical Security Measures	Pseudonymisation of data.	Implemented
	Exclusive use of authorised storage and sharing solutions, with automatic blocking of unauthorised solutions from access to the company network.	Implemented

Specific Security Measures Relating to Assets Associated with the Processing

Asset	Category	Security Measure	Status
Excel files for research	Technical Security Measures	Assignment and management of access privileges according to the principle of least privilege (Role Profiling)	Implemented
		Existence of rules on the correct use and management of access passwords, with mandatory use of high-strength credentials	Implemented
		Assignment of personal encryption keys to each user	Implemented
		Encryption of the database	Implemented
		Creation of at least weekly backup copies necessary for system recovery	Implemented
		Guarantee of immutability of backup copies	Partial
		Digital signature of the database with hash. In order to guarantee the accuracy of data stored in Excel files, in particular those relating to enrolled patients, the Excel sheets will be digitally signed using a hash. The digital signature generated will be held by a person distinct from the data collection officer and will be repeated, where applicable, if data are modified or exported to other files. This measure reinforces safeguards aimed at ensuring the accuracy of data and ensuring that any subsequent alterations are promptly detected and corrected.	To be applied
	Organisational Security Measures	Access to resources based on authorisation profiles determined by the user's role, job duties, and the policies established by the Administration	Implemented

	ENISA Security Measures	Definition of documented backup and data recovery procedures	Implemented
	Logical Security Measures	Access to individual productivity tools via strong authentication credentials	Implemented
REDCap	Technical Security Measures	Assignment and management of access privileges according to the principle of least privilege (Role Profiling)	Implemented
		Existence of rules on the correct use and management of access passwords, with mandatory use of high-strength credentials	Implemented
		System access with strong authentication (e.g. MFA/CNS/smart card/certificate/digital signature)	Implemented
		Use of secure network protocols for application use, employing cryptographic protocols (SSL/TLS)	Implemented
		Pseudonymisation of data	Implemented
		Input validation at the application level (SQL Injection prevention)	Implemented
		Session timeout after N minutes of inactivity	Implemented
		Encryption of the database	Implemented
		Creation of at least weekly backup copies necessary for system recovery	Implemented
		Performance of multiple backups using different tools to counter possible failures during the restoration phase	Implemented
		Implementation of an audit log and privacy-preserving system to record activities performed by users and the system	Implemented
		Protected transmission channels. Use of protected transmission channels in line with the state of the art, ensuring, after verification, the digital identity of the server providing the service and the client workstation from which data access is performed, using digital certificates issued in compliance with the law by a certification authority.	Implemented
	Organisational Security Measures	Existence of a formal procedure for the issuance and deletion of credentials	Implemented
		Existence of periodic controls on issued user accounts to ensure their consistency	Implemented
	ENISA Security Measures	Recording of the actions of system administrators and system operators, including the addition/deletion/modification of user access rights	Implemented
		In a privacy-by-default approach, database and application servers must process only the personal data that are actually necessary for processing in order to achieve their processing objectives.	Implemented

		Application of privacy-supporting techniques at the database level, such as authorised queries, privacy-preserving database querying, searchable encryption, etc.	Implemented
		Use of secure network protocols for internet access, employing cryptographic protocols (SSL/TLS)	Implemented
		Definition of documented backup and data recovery procedures	Implemented

7.2 Risk Assessment per Threat

Threat	Malware (viruses, trojans, ransomware)	Category	Technical threats
Impact Areas	Availability; Confidentiality; Integrity	Risk Sources	Systems/Tools
Description	Malicious software that can steal, encrypt or destroy personal data		
Element		Initial Numeric Value	Initial Level
Impact		2	Moderate
Probability		1	Unlikely
INITIAL RISK LEVEL		2	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Existence of procedures and controls to ensure the required level of continuity and availability of the IT system processing personal data	Applied	Applied
Technical Security Measures	Use of secure network protocols, employing cryptographic protocols (SSL/TLS)	Applied	Applied
Technical Security Measures	Input validation at application level (SQL Injection prevention)	Applied	Applied
Technical Security Measures	Assignment of personal encryption keys to each user	Applied	Applied
Technical Security Measures	Encryption of the database	Applied	Applied
Technical Security Measures	Implementation of an audit log and privacy-preserving system	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Phishing and social engineering	Category	Technical threats
Impact Areas	Availability; Confidentiality	Risk Sources	Systems/Tools
Description	Fraudulent emails or messages that deceive users into disclosing access credentials or personal data		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Existence of a data protection policy as part of the information security policy	Applied	Applied
Logical Security Measures	Access to individual productivity tools via strong authentication credentials	Applied	Applied
Organisational Security Measures	Existence of staff training procedures on data protection	Applied	Applied
Technical Security Measures	Existence of rules on the correct use and management of access passwords	Applied	Applied
Technical Security Measures	System access with strong authentication (MFA/CNS/smart card/certificate/digital signature)	Applied	Applied
Technical Security Measures	Session timeout after N minutes of inactivity	Applied	Applied
Technical Security Measures	Assignment of personal encryption keys to each user	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Man-in-the-Middle (MITM) Attacks	Category	Technical threats
Impact Areas	Availability; Confidentiality	Risk Sources	Systems/Tools
Description	Interception of communications between two parties to steal information		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low

Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Logical Security Measures	Access to individual productivity tools via strong authentication credentials	Applied	Applied
Technical Security Measures	Assignment and management of access privileges (principle of least privilege)	Applied	Applied
Technical Security Measures	Existence of rules on the correct use and management of access passwords	Applied	Applied
Technical Security Measures	System access with strong authentication	Applied	Applied
Technical Security Measures	Use of secure network protocols (SSL/TLS)	Applied	Applied
Technical Security Measures	Pseudonymisation of data	Applied	Applied
Technical Security Measures	Assignment of personal encryption keys to each user	Applied	Applied
Technical Security Measures	Encryption of the database	Applied	Applied
Technical Security Measures	Implementation of an audit log and privacy-preserving system	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Web Application Vulnerabilities	Category	Technical threats
Impact Areas	Availability; Integrity	Risk Sources	Systems/Tools
Description	Techniques to access and manipulate databases containing personal data (e.g. SQL Injection)		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Application of privacy-supporting techniques at the database level (authorised queries, privacy-	Applied	Applied

	preserving database querying, searchable encryption, etc.)		
Technical Security Measures	Assignment and management of access privileges (principle of least privilege)	Applied	Applied
Technical Security Measures	Input validation at application level (SQL Injection prevention)	Applied	Applied
Technical Security Measures	Session timeout after N minutes of inactivity	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	IoT and Cloud Device Attacks	Category	Technical threats
Impact Areas	Availability; Confidentiality	Risk Sources	Systems/Tools
Description	Connected systems exposed to vulnerabilities that may compromise personal data		
Element		Initial Numeric Value	Initial Level
Impact		2	Moderate
Probability		1	Unlikely
INITIAL RISK LEVEL		2	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Technical Security Measures	Pseudonymisation of data	Applied	Applied
Technical Security Measures	Encryption of the database	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Supply Chain Disruption and/or Data Corruption	Category	Technical threats
Impact Areas	Availability; Integrity	Risk Sources	Systems/Tools
Description	Interruption of cloud service providers, network provider outages, power failures, medical device malfunctions, system saturation, system errors or hardware failures that alter information integrity		

Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Existence of procedures and controls to ensure continuity and availability of the IT system	Applied	Applied
ENISA Security Measures	Definition of documented backup and data recovery procedures	Applied	Applied
Technical Security Measures	Creation of at least weekly backup copies	Applied	Applied
Technical Security Measures	Performance of multiple backups using different tools	Applied	Applied
Technical Security Measures	Guarantee of immutability of backup copies	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	System Failures	Category	Technical threats
Impact Areas	Availability; Integrity	Risk Sources	Human; Systems/Tools
Description	Software malfunctions, outdated firmware, device failures, network component failures, inadequate maintenance, hardware/software tampering		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Use of Unauthorised Software/Hardware	Category	Technical threats
Impact Areas	Availability; Confidentiality; Integrity	Risk Sources	Human; Systems/Tools

Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Existence of a register of IT resources used for personal data processing	Applied	Applied
Organisational Security Measures	Access to resources based on authorisation profiles determined by user role and job duties	Applied	Applied
Technical Security Measures	Exclusive use of authorised storage and sharing solutions, with automatic blocking of unauthorised solutions	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Denial of Service (DoS) and Distributed Denial of Service (DDoS)	Category	Technical threats
Impact Areas	Availability	Risk Sources	Systems/Tools
Description	Attacks aimed at making a resource (such as a website) unavailable to legitimate users by overloading it with requests until its resources are exhausted		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Zero-day Exploits	Category	Technical threats
Impact Areas	Availability; Confidentiality	Risk Sources	Systems/Tools

Description	Targeted attacks with the aim of stealing data, spying on users, distributing malware or causing damage to systems and networks. They are so called because developers have "zero days" to resolve the problem before it can be exploited by attackers.		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Technical Security Measures	Assignment and management of access privileges according to the principle of least privilege (Role Profiling)	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Credential Stuffing Attacks	Category	Technical threats
Impact Areas	Availability; Confidentiality	Risk Sources	Systems/Tools
Description	A form of cyber attack in which attackers use lists of previously breached usernames and passwords (obtained from data breaches of other websites or services) to attempt access to various websites and online applications, exploiting the common tendency of users to reuse the same credentials across multiple sites and services.		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Clear definition of procedures for revoking user rights and responsibilities in the event of internal reorganisations or changes of employment	Applied	Applied
Organisational Security Measures	Existence of staff training procedures on data protection	Applied	Applied

Organisational Security Measures	Existence of periodic controls on issued user accounts	Applied	Applied
Organisational Security Measures	Access to resources based on authorisation profiles	Applied	Applied
Technical Security Measures	Assignment and management of access privileges (principle of least privilege)	Applied	Applied
Technical Security Measures	Existence of rules on the correct use and management of access passwords	Applied	Applied
Technical Security Measures	System access with strong authentication	Applied	Applied
Technical Security Measures	Assignment of personal encryption keys to each user	Applied	Applied
Technical Security Measures	Implementation of an audit log and privacy-preserving system	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Sniffing	Category	Technical threats
Impact Areas	Confidentiality	Risk Sources	Systems/Tools
Description	An interception technique used to capture data travelling across a network. Attackers, using specialised software or hardware called sniffers, can monitor and analyse network traffic to extract sensitive information without the sender or recipient being aware.		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		1	Unlikely
INITIAL RISK LEVEL		1	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Technical Security Measures	Assignment and management of access privileges (principle of least privilege)	Applied	Applied
Technical Security Measures	System access with strong authentication	Applied	Applied
Technical Security Measures	Use of secure network protocols (SSL/TLS)	Applied	Applied
Technical Security Measures	Implementation of an audit log and privacy-preserving system	Applied	Applied

Element	Final Numeric Value	Final Level
Impact	1	Minor
Probability	1	Unlikely
RESIDUAL RISK LEVEL	1	Low

Threat	Identity Theft Attacks	Category	Technical threats
Impact Areas	Confidentiality	Risk Sources	Systems/Tools
Description	Commonly known as identity theft, these are a form of cybercrime in which a malicious individual takes possession of and illegally uses another person's personal information for personal gain.		

Element	Initial Numeric Value	Initial Level
Impact	1	Minor
Probability	1	Unlikely
INITIAL RISK LEVEL	1	Low

Security Measures

Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Clear definition of procedures for revoking user rights and responsibilities	Applied	Applied
ENISA Security Measures	Application of privacy-supporting techniques at the database level	Applied	Applied
Organisational Security Measures	Existence of staff training procedures on data protection	Applied	Applied
Organisational Security Measures	Access to resources based on authorisation profiles	Applied	Applied
Technical Security Measures	Existence of rules on the correct use and management of access passwords	Applied	Applied
Technical Security Measures	System access with strong authentication	Applied	Applied
Technical Security Measures	Pseudonymisation of data	Applied	Applied
Technical Security Measures	Assignment of personal encryption keys to each user	Applied	Applied
Technical Security Measures	Encryption of the database	Applied	Applied

Element	Final Numeric Value	Final Level
Impact	1	Minor
Probability	1	Unlikely
RESIDUAL RISK LEVEL	1	Low

Threat	Compromise of REDCap Access Credentials	Category	Research threats – REDCap application
Impact Areas	Confidentiality	Risk Sources	Human
Description	Unauthorised acquisition of usernames and passwords for access to the REDCap platform by unauthorised individuals		
Element		Initial Numeric Value	Initial Level
Impact		2	Moderate
Probability		2	Low Probability
INITIAL RISK LEVEL		4	Medium
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Organisational Security Measures	Existence of a formal procedure for the issuance and deletion of credentials	Applied	Applied
Organisational Security Measures	Existence of periodic controls on issued user accounts	Applied	Applied
Technical Security Measures	Assignment and management of access privileges (principle of least privilege)	Applied	Applied
Technical Security Measures	Existence of rules on the correct use and management of access passwords	Applied	Applied
Technical Security Measures	System access with strong authentication (MFA)	Applied	Applied
Technical Security Measures	Session timeout after N minutes of inactivity	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Abuse of Administrative Privileges	Category	Research threats – REDCap application
Impact Areas	Confidentiality	Risk Sources	Human
Description	Improper use of administrator privileges to access unauthorised data or modify security configurations		
Element		Initial Numeric Value	Initial Level
Impact		3	Severe

Probability		2	Low Probability
INITIAL RISK LEVEL		6	High
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Organisational Security Measures	Existence of staff training procedures on data protection, including security profiles	Applied	Applied
Technical Security Measures	Implementation of an audit log and privacy-preserving system to record activities performed by users and the system	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Corruption of Data in the REDCap Database	Category	Research threats – REDCap application
Impact Areas	Integrity	Risk Sources	Human
Description	Unauthorised alteration of health data contained in the REDCap database compromising the integrity of the research		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		2	Low Probability
INITIAL RISK LEVEL		2	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Application of privacy-supporting techniques at the database level	Applied	Applied
ENISA Security Measures	Definition of documented backup and data recovery procedures	Applied	Applied
Technical Security Measures	Input validation at application level (SQL Injection prevention)	Applied	Applied
Technical Security Measures	Encryption of the database	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely

RESIDUAL RISK LEVEL	1	Low
----------------------------	----------	------------

Threat	Malware Attacks on the REDCap Platform	Category	Research threats – REDCap application
Impact Areas	Availability; Integrity	Risk Sources	Human
Description	Attacks aimed at rendering the REDCap platform inaccessible or maliciously encrypting the data		

Element	Initial Numeric Value	Initial Level
Impact	2	Moderate
Probability	2	Low Probability
INITIAL RISK LEVEL	4	Medium

Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Definition of documented backup and data recovery procedures	Applied	Applied
Organisational Security Measures	Existence of staff training procedures on data protection	Applied	Applied
Technical Security Measures	Use of secure network protocols (SSL/TLS)	Applied	Applied
Element	Final Numeric Value	Final Level	
Impact	1	Minor	
Probability	1	Unlikely	
RESIDUAL RISK LEVEL	1	Low	

Threat	REDCap Database Data Breach	Category	Research threats – REDCap application
Impact Areas	Confidentiality	Risk Sources	Human
Description	Unauthorised exfiltration of pseudonymised health data from the REDCap database		

Element	Initial Numeric Value	Initial Level
Impact	2	Moderate
Probability	2	Low Probability
INITIAL RISK LEVEL	4	Medium

Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation

ENISA Security Measures	Definition of documented backup and data recovery procedures	Applied	Applied
Organisational Security Measures	Existence of staff training procedures on data protection	Applied	Applied
Technical Security Measures	Pseudonymisation of data	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Breach of Pseudonymisation	Category	Research threats – REDCap application
Impact Areas	Confidentiality	Risk Sources	Human
Description	Compromise of the automatic coding system allowing re-identification of data subjects		
Element		Initial Numeric Value	Initial Level
Impact		3	Severe
Probability		2	Low Probability
INITIAL RISK LEVEL		6	High
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Organisational Security Measures	Existence of staff training procedures on data protection	Applied	Applied
Technical Security Measures	Assignment and management of access privileges (principle of least privilege)	Applied	Applied
Technical Security Measures	Pseudonymisation of data	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Data Interception During Transmission	Category	Research threats – REDCap application
Impact Areas	Confidentiality	Risk Sources	Context; Systems/Tools

Description	Unauthorised interception of data during communication between the REDCap client and server		
Element		Initial Numeric Value	Initial Level
Impact		2	Moderate
Probability		2	Low Probability
INITIAL RISK LEVEL		4	Medium
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Technical Security Measures	Protected transmission channels: use of protected transmission channels in line with the state of the art, ensuring, after verification, the digital identity of the server providing the service and the client workstation, using digital certificates issued in compliance with the law by a certification authority	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Unauthorised Access to Excel Files Containing Decoding Keys	Category	Research threats – Excel files with decoding keys
Impact Areas	Confidentiality	Risk Sources	Human; Context
Description	Unauthorised access to Excel files containing the associations between pseudonymised codes and real identities		
Element		Initial Numeric Value	Initial Level
Impact		3	Severe
Probability		2	Low Probability
INITIAL RISK LEVEL		6	High
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
Logical Security Measures	Access to individual productivity tools via strong authentication credentials	Applied	Applied
Organisational Security Measures	Access to resources based on authorisation profiles determined by user role and job duties	Applied	Applied

Organisational Security Measures	Issuance of appropriate instructions regarding personal data processing to all persons involved in the procedure	Applied	Applied
Technical Security Measures	Assignment and management of access privileges (principle of least privilege)	Applied	Applied
Technical Security Measures	Existence of rules on the correct use and management of access passwords	Applied	Applied
Technical Security Measures	Assignment of personal encryption keys to each user	Applied	Applied
Technical Security Measures	Encryption of the database	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor
Probability		1	Unlikely
RESIDUAL RISK LEVEL		1	Low

Threat	Corruption/Alteration of Decoding Keys	Category	Research threats – Excel files with decoding keys
Impact Areas	Integrity	Risk Sources	Human
Description	Unauthorised or accidental modification of Excel files compromising the ability to re-identify data subjects		
Element		Initial Numeric Value	Initial Level
Impact		1	Minor
Probability		2	Low Probability
INITIAL RISK LEVEL		2	Low
Security Measures			
Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Definition of documented backup and data recovery procedures	Applied	Applied
Technical Security Measures	Creation of at least weekly backup copies	Applied	Applied
Technical Security Measures	Guarantee of immutability of backup copies	Applied	Applied
Technical Security Measures	Digital signature of the database with hash	Applied	Applied
Element		Final Numeric Value	Final Level
Impact		1	Minor

Probability	1	Unlikely
RESIDUAL RISK LEVEL	1	Low

Threat	Loss of Excel Files Containing Decoding Keys	Category	Research threats – Excel files with decoding keys
Impact Areas	Confidentiality	Risk Sources	Human
Description	Loss of files containing decoding keys making re-identification of data subjects impossible		

Element	Initial Numeric Value	Initial Level
Impact	1	Minor
Probability	2	Low Probability
INITIAL RISK LEVEL	2	Low

Security Measures

Category	Measure	Impact Mitigation	Probability Mitigation
ENISA Security Measures	Definition of documented backup and data recovery procedures	Applied	Applied
Organisational Security Measures	Issuance of appropriate instructions regarding personal data processing to all persons involved in the procedure	Applied	Applied
Technical Security Measures	Assignment and management of access privileges (principle of least privilege)	Applied	Applied
Technical Security Measures	Creation of at least weekly backup copies	Applied	Applied

Element	Final Numeric Value	Final Level
Impact	1	Minor
Probability	1	Unlikely
RESIDUAL RISK LEVEL	1	Low

Risk Assessment Summary

Threat	Initial Risk	Residual Risk
Malware (viruses, trojans, ransomware)	2	1
Phishing and social engineering	1	1
Man-in-the-Middle (MITM) Attacks	1	1
Web Application Vulnerabilities	1	1
IoT and Cloud Device Attacks	2	1

Supply Chain Disruption and/or Data Corruption	1	1
System Failures	1	1
Use of Unauthorised Software/Hardware	1	1
Denial of Service (DoS) and Distributed Denial of Service (DDoS)	1	1
Zero-day Exploits	1	1
Credential Stuffing Attacks	1	1
Sniffing	1	1
Identity Theft Attacks	1	1
Compromise of REDCap Access Credentials	4	1
Abuse of Administrative Privileges	6	1
Corruption of Data in the REDCap Database	2	1
Malware Attacks on the REDCap Platform	4	1
REDCap Database Data Breach	4	1
Breach of Pseudonymisation	6	1
Data Interception During Transmission	4	1
Unauthorised Access to Excel Files Containing Decoding Keys	6	1
Corruption/Alteration of Decoding Keys	2	1
Loss of Excel Files Containing Decoding Keys	2	1

Overall Risk Level by Impact Area

Impact Area	Risk Level
Availability	Low
Confidentiality	Low
Integrity	Low

Overall Residual Risk Level
LOW

8. Stakeholder Involvement

Question	Response
Were the opinions of data subjects or their representatives collected?	No Considering that the risk assessment is low, thanks to the technical and organisational measures adopted by the Data Controller, it was not considered necessary to involve the contactable data subjects.

Was the Data Protection Officer consulted?	No Considering that the risk assessment is low, thanks to the technical and organisational measures adopted by the Data Controller, and referring to the provisions of Art. 39(1)(c) GDPR, it was not considered necessary to consult the company's Data Protection Officer.
---	--

9. Notes

No additional notes.