

**Mémoire Au-delà de la survie : que reste-t-il d'un séjour en soins intensifs ?
Étude de la relation entre la durée du séjour en soins intensifs et l'intensité du
syndrome post-soins intensifs dans une cohorte monocentrique.**

Auteur : NEIS GILSON, Sarah

Promoteur(s) : ROUSSEAU, Anne-Françoise; LAMBERMONT, Bernard

Faculté : Faculté de Médecine

Diplôme : Master en sciences infirmières, à finalité spécialisée en pratiques avancées

Année académique : 2025-2026

URI/URL : <http://hdl.handle.net/2268.2/27192>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

Data transfer and processing agreement

BETWEEN

Centre Hospitalier Universitaire de Liège (CHU de Liège), located at Avenue de l'Hôpital 1, 4000 Liège, Belgium, Public establishment with legal personality created by Royal Decree of 31 mars 1987, company number 0232.988.060.

represented by its Managing Director (CEO), Mr Marc DE PAOLI, appointed to the position of Managing Director by decision of the Board of Directors on 17 January 2022

hereinafter referred to as the "**CHU DE LIEGE**",

And in presence of Prof. **Lambermont Bernard**, Head of Department

AND

Université de Liège, Département de Santé des sciences de la santé Publique located at Place du 20 Août, 7, 4000 Liège, Belgium company number 0325.777.171

represented by **Pr Donneau Anne Françoise**
And in presence of **Rousseau Anne Françoise**

hereinafter referred to as "**ULiège**"

The CHU DE LIEGE and ULiège are hereinafter individually referred to as "**Party**" and collectively referred to as the "**Parties**".

WHEREAS, ULiège wishes to encourage its Master's students to carry out final year projects involving researches that require the analysis of data from CHU DE LIEGE databases. Particularly, in the frame of this agreement, ULiège supervises the student.. **Neis-Gilson Sarah** in the completion of his/her final year project work entitled "**Study of the relationship between the length of stay in intensive care and the intensity of post-intensive care syndrome**"[2026-272]

WHEREAS, All defined terms within the Agreement shall have the same meaning when used in this Data Processing Agreement, unless explicitly defined otherwise in this Data Processing Agreement.

NOW, THEREFORE, in consideration of the premises and of the following mutual promises, covenants and conditions and any sums to be paid, the Parties hereto agree as follows:

Article 1: OBJECT

The data transferred and processed are defined in Schedule 1 to this Agreement (hereinafter referred to as "Data" or "Information").

Article 2: CONFIDENTIALITY

For the purposes of this Agreement, the following is and shall be considered throughout and during a period of ten (10) years after the term or termination of this Agreement as confidential information (hereinafter referred to as "Confidential information" whether marked as "confidential" or not,

- all information received by ULiège from the CHU DE LIEGE, including but not limited to proprietary information, trade secret, data, Know-How (hereafter "CHU DE LIEGE's CONFIDENTIAL INFORMATION");
- all information received by the CHU DE LEIGE from ULiège, including but not limited to proprietary information, trade secret, data, KnowHow (hereafter "ULiège's CONFIDENTIAL INFORMATION");

Confidential information notably includes but is not limited to, every communication of information, data or materials between the Parties in any form whatsoever, including oral, written and machine readable.

Confidential information does not include information that:

- at the time of disclosure thereof is or thereafter becomes part of the public domain through no breach, fault or omission of the receiving Party or of their respective employees, agents, Subcontractors or participants;
- at the time of disclosure thereof by the disclosing Party, is already in the receiving Party's lawful possession as evidenced by the receiving Party's competent written records and not subject to prior confidentiality obligations;
- the receiving Party receives from a third party who has the right to disclose the same and who did not obtain such information in violation of the disclosing Party's rights;
- is independently developed by the receiving Party without the use of Confidential information as evidenced by the receiving Party's written records and is not subject to confidentiality obligations;
- the receiving Party is required to disclose by applicable law, by a court or by a governmental authority, provided that the receiving Party (i) promptly notifies the disclosing Party of such requirement prior to disclosure –to the extent reasonably and legally permissible - in order to allow them the opportunity to oppose the requirement or seek an appropriate protective order; (ii) discloses only that Confidential information required to comply with the legal requirement and (iii) continues to maintain the confidentiality of this Confidential information with respect to all other third parties.

The burden of proving the applicability of any of these exceptions resides with the receiving Party.

The receiving Party shall hold such Confidential information of the disclosing Party in strict confidence and shall only disclose such Confidential information on a need-to-know basis to their agents, employees, Subcontractors or personnel who are directly involved in the performance of services for the Study.

The receiving Party shall further use the Confidential information of the disclosing Party only for the purpose of fulfilling their respective obligations under this Agreement.

Data transfer and processing agreement

The receiving Party shall not disclose to any third party any of the Confidential information without specific prior, express written authorisation from the disclosing Party with respect to such disclosure.

The receiving Party shall notify the disclosing Party immediately upon discovery of any unauthorized disclosure or use of the Confidential information and will collaborate with the disclosing Party in every reasonable way to assist the disclosing Party regaining the possession of the Confidential information and prevent its further unauthorized use or disclosure.

The Confidential information is and shall remain the exclusive property of the disclosing Party. The disclosure of Confidential information does not grant any expressed or implied rights or license to the receiving Party to any Intellectual Property Rights possessed by the disclosing Party.

At the end of the Study and within thirty (30) Days following the written request of the disclosing Party, all Confidential information, whether in documentary, permanent or machine-readable form, including any copies and translations of all or any part thereof shall be returned to the disclosing Party or destroyed if instructed by disclosing Party, save that each Party may retain one copy of such Confidential information solely for record-keeping purposes pursuant to applicable laws or regulations and/or to guarantee compliance with the confidentiality obligations under this Article 0. If requested by the disclosing Party, such destruction shall be promptly confirmed in writing by the receiving Party.

Article 3: OWNERSHIP AND USE OF DATA

The Data shall be the sole property of the Disclosing Party.

Subject to the confidentiality provisions of this Agreement, the Disclosing Party hereby grants to the Receiving Party a non-exclusive, non-transferable and non-assignable right to use the Data solely for non-commercial research purposes, educational purposes, patient care purposes.

The Receiving Party agrees that the Data: (a) is to be used only for the purposes of the Research, (b) will not be transferred to any third party. Receiving Party shall not duplicate, transfer, distribute or supply to any other person or entity the Information, whether with or without consideration, for any purpose or use and shall not carry out the Research with any third party or entity without prior written approval of Disclosing Party.

The data to be transferred to Receiving Party will not contain directly identifying personal data. Under no circumstances will the identity of the patient or any means to derive such identity be provided to Receiving Party. Receiving Party shall not carry out any procedures with the Data (linking, comparison, processing) through which the identity of the patient could be derived. Parties agree to process personnel data in accordance with the GDPR and Schedule 2. Receiving Party shall safeguard the Data received with a degree of care which is no less than Disclosing Party uses to protect such Data and shall have in place appropriate technical and organizational measures hereto but always in compliance applicable privacy laws and regulations. Any accidental or unauthorised access to the Data or loss of Data must be reported to Disclosing Party immediately.

It is recognized and understood that all Intellectual Property Rights existing as of the Effective Date and know how owned or controlled by a Party are that Party's separate property and are not affected by this Agreement, and no Party hereunder shall have any claims to or rights in such Background IP of the other Party.

Article 4: PUBLICATION

For the duration of this agreement and the subsequent five-year period mentioned above, no communications or publications of a scientific nature directly related to the Results obtained during the Research, could not be made without the prior written consent of both Parties. A Party shall be deemed to have given this agreement within 30 days of the request for publication and/or communication submitted by the other Party. Should the Parties decide to file a patent application, they shall withhold publication for an additional period of three months.

The Parties also agree not to use the name of a Party in any publication or marketing materials without the prior and written consent of this Party. Nothing contained herein prevents Disclosing Party to publish any documents relating to the Information.

Article 5: RESPONSIBILITIES

Disclosing Party has collected Information in a competent and professional manner. Disclosing Party does however not provide hereby any guarantee regarding the obtainment of specific results regarding Information. Receiving Party shall bear all risks and assume all liability resulting from the use, storage or disposal of Information. Disclosing Party shall not be liable towards Receiving Party and third parties for any loss, claim or demand made by Receiving Party or made against Receiving Party by any third party due to or arising from the use of the Information by the Receiving Party.

Article 6: FINANCE

Each party bears its own costs.

Article 7: TERM

This Agreement is a limited term agreement which will enter into force at the date of the last signature by the Parties of this Agreement ('**Effective Date**') and will remain in force for a duration of 1 year. Any clauses that will be expected or intended by its nature to survive the expiration of this Agreement, shall survive the expiration of this Agreement.

Upon expiration of this Agreement, the right to use the Data and Confidential Information will automatically end and ULiège will return or destroy all Confidential Information received from Disclosing Party. Upon request from Disclosing Party, Receiving Party shall confirm in writing the complete deletion of such Confidential Information.

Either Party may terminate this Agreement upon written notice if the other Party materially breaches any provision of this Agreement, which breach continues and is not remedied within twenty (20) calendar days after the date of receipt of such notice.

Either Party may terminate this Agreement at any time for an objectively justified reason upon thirty (30) days prior written notice to the other Party.

Article 8: Entire Agreement and obligations towards third parties

This Agreement, together with its SCHEDULES 1 and 2 represents the entire agreement between the Parties in relation to the subject matter of this Agreement, and supersedes, replaces and extinguishes all prior negotiations, representations, undertakings, arrangements, draft agreements, agreements, including confidentiality agreements, written or oral, in relation to such subject matter.

Data transfer and processing agreement

Article 9: MODIFICATION AND WAIVER

No modification of this Agreement shall be deemed effective unless in writing and signed by each of the Parties hereto, and no waiver of any right set forth herein shall be deemed effective unless in writing and signed by the Party against whom enforcement of the waiver is sought.

Article 10: GOVERNING LAW

This Agreement and all terms used therein shall be construed and interpreted in accordance with the laws of Belgium, excluding its conflicts of law provisions.

Article 11: SETTLEMENT OF DISPUTES

In the event of any disputes, controversies or claims arising from or in connection with this Agreement or the breach thereof, the Parties shall try to settle this issue amicably between themselves. Should the Parties so fail, the courts in Liège (Belgium) shall have exclusive jurisdiction to finally settle the dispute, controversy or claim.

Article 12: COUNTERPARTS

The Agreement is executed in 2 original copies and each Party acknowledges having received an original.

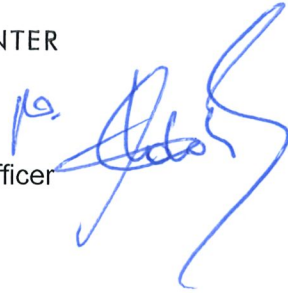
[intentionally left blank]

IN WITNESS WHEREOF, the undersigned by their duly authorised representatives have executed this Agreement on the date of last signature.

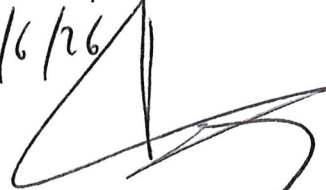
Centre Hospitalier Universitaire de Liège (CHU de Liège):

VOLDERS Anja
Director
CLINICAL TRIAL CENTER
CHU de Liège

Name: De Paoli Marc
Title: Chief Executive Officer
Date: 30 JUN 2026



Name: Lambermont Bernard
Title: Head of Department
Date: 24/6/26



ULiège:

Pr. AFr. Donneau

Pr. AFr. Donneau (24 juin 2026 19:40:34 GMT+2)

Name: Donneau Anne-Françoise
Title: Présidente du département
des sciences de la santé publique
24/06/2026

AF Rousseau

AF Rousseau (24 juin 2026 22:43:14 EDT)

Name: Rousseau Anne-Françoise
Title: Chargée de cours
Date:
24/06/2026

Schedule 1: Description of the Data

Description of the Data

The data to be transferred consist of anonymized clinical and questionnaire data collected within the Post-Intensive Care Clinic (CPSI) of the CHU de Liège, as part of a systematic postICU screening program.

This study is a retrospective observational analysis conducted in the context of a Master's thesis in Nursing Sciences.

Nature and origin of the data The

data originate from:

- a structured post-ICU follow-up program implemented at the CHU de Liège since June 2024
- a clinical database (CPSI database), fed through anonymized extraction of patient records via the hospital information system (SIME)
- standardized questionnaires sent to patients approximately one month after ICU discharge

Categories of data collected

The dataset includes the following variables:

1. Sociodemographic data

- Age
- Sex
- Socio-economic status (e.g. BIM status if available)

2. Clinical data related to ICU stay

- Length of stay in ICU
- Reason for ICU admission
- Medical history (if available)
- Exposure to mechanical ventilation
- Occurrence of delirium (if available)
- Severity indicators (e.g. APACHE II if available)

3. Post-ICU outcome data (primary outcome)

- HABC-M-HV-F questionnaire scores (total score and subdomains):
 - Cognitive

- Functional ○ Psychological ○
- Quality of life

4. Patient-reported experience data

- IPREA questionnaire responses (binary variables reflecting perceived discomfort during ICU stay): ○ Pain ○ Noise ○ Light ○ Restraints ○ Thirst ○ Isolation ○ Other discomforts

Data format and identifiability • The data are **pseudonymized before analysis**

- No directly identifiable personal data (name, address, etc.) are transferred
- Patients are identified only through coded identifiers
- The key linking identifiers to patients remains exclusively within CHU de Liège

Purpose of data processing

The data are processed exclusively for:

- academic research purposes
- the completion of a Master's thesis
- the evaluation of the relationship between ICU length of stay and the intensity of postintensive care syndrome (PICS)

No commercial use will be made of the data.

Data access and security

- Data are stored on secure CHU de Liège servers
- Access is restricted to authorized members of the research team
- Data processing complies with GDPR requirements

Schedule 2: SCOPE OF THE DATA PROCESSING AGREEMENT

- 1.1 The **CHU DE LIEGE** acts as a Processor as defined under article 4, 8) of the GDPR ("Processor") for ULiège who acts as controller as defined under article 4, 7) of the GDPR ("Controller"), when the **CHU DE LIEGE** processes Personal Data for ULiège as set out in Annex 1.

2 PROCESSING OF PERSONAL DATA

- 2.1 **Instructions:** The Processor is instructed to process the Personal Data for the term of this Data Processing Agreement and only for the purposes of providing the data processing tasks set out in Annex 1. The Processor may not process or use Personal Data for any purpose other than a Data Subject's medical records or other than provided in the Agreement or instructions, including with regard to transfers of Personal Data to a third country or an international organization, unless the Processor is required to do so according to Union or Member State law. In that case, the Processor shall inform the Controller in writing of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

- 2.2 The Processor shall at all times maintain a record of processing of Personal Data in accordance with Applicable Laws and if the Processor considers an instruction from the Controller to be in violation of the Applicable Laws, the Processor shall promptly inform the Controller in writing about this.

3 THE PROCESSOR'S OBLIGATIONS

- 3.1 The Processor must ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The Processor shall take full responsibility in the event there is a breach of said confidentiality obligation.
- 3.2 The Processor shall implement appropriate technical and organizational measures to prevent that the Personal Data processed is:
- (i) accidentally or unlawfully destroyed, lost or altered, (ii) disclosed or made available without authorization, or
 - (iii) otherwise processed in violation of Applicable Laws.
- 3.3 The Processor must also comply with the special data security requirements of Annex 1.
- 3.4 The appropriate technical and organizational security measures must be determined with due regard for:
- (i) the current state of the art,
 - (ii) the cost of their implementation, and
 - (iii) the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Data transfer and processing agreement

- 3.5 The Processor shall upon request provide the Controller with sufficient information to enable the Controller to ensure that the Processor's obligations under this Data Processing Agreement are complied with, including ensuring that the appropriate technical and organizational security measures have been implemented.
- 3.6 The relationship of the Parties and the nature of the Study outlined in the Agreement are such that the Controller has no access to the identity of the Study Participants. Therefore, the Controller needs to rely on the Processor in order to be able, by means of appropriate technical and organizational measures, to fulfil the obligation imposed to the Controller under Applicable Laws. The Processor shall therefore respond to requests from data subjects in accordance with Article 3.11. of the Agreement pursuant to Applicable Laws (such as, the right of access, the right to rectification, the right to erasure, the right to restrict the processing, the right to data portability and the right to object).
- 3.7 The Controller is entitled to appoint at its own cost an independent expert, who shall have access to the Processor's data processing facilities and receive the necessary information for the sole purpose of auditing whether the Processor has complied with its obligations. The Processor may reasonably and in a justified manner object to the appointment of this proposed expert. The expert shall upon the Processor's request sign a non-disclosure agreement provided by the Processor, and treat all information obtained or received from the Processor confidentially, and may only pass on, the findings as described under clause 3.9(ii) below to the Controller.
- 3.8 The Processor must give authorities who by Union or Member State law have a right to enter the Controller's or the Controller's processors' facilities, or representatives of the authorities, access to the Processor's physical facilities against proper proof of identity and mandate, during normal business hours and upon reasonable prior written notice.
- 3.9 The Processor must without undue delay, and where feasible within 72 hours, notify the Controller in writing about:
- (i) any request for disclosure of Personal Data processed under the Agreement by authorities, unless expressly prohibited under Union or Member State law,
 - (ii) any finding of (a) breach of security that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by the Processor under the Agreement ("**Data Breach**"), or (b) other failure to comply with the Processor's obligations under Clause 3, or
 - (iii) any request for access to the Personal Data (with the exception of medical records of the Study Participants for which the Processor is considered Controller) received directly from the data subjects or from third parties.
- 3.10 Such a notification from the Processor to the Controller with regard to a Data Breach will contain at least the following information:

Data transfer and processing agreement

- (i) The nature of the Personal Data Breach, stating the categories and (by approximation) the number of data subjects concerned, and stating the categories and (by approximation) the number of the Personal Data registers affected (datasets);
- (ii) The likely consequences of the Personal Data Breach;
- (iii) A proposal for measures to be taken to address the Personal Data Breach, including (where appropriate) measures to mitigate any possible adverse effects of such breach.

The Processor shall document (and shall keep such documentation available for the Controller) any Personal Data Breaches, including the facts related to the Personal Data Breach, its effects and the corrective measures taken. After consulting with the Controller, the Processor shall take any measures needed to limit the (possible) adverse effects of Personal Data Breaches (unless such consultation cannot be awaited due to the nature of the Personal Data Breach).

- 3.11 The Processor must promptly and reasonably execute all actions required to handle (a) responses to any breach of security as described in 3.9(ii) above and (b) any requests from data subjects under Chapter III of the GDPR, including requests for access, rectification, restriction of processing or erasure. The Processor must also reasonably implement the appropriate technical and organizational measures to enable the Controller to fulfil the Controller's obligation to respond to such requests. Any reasonable documented costs and expenses pre-approved in writing by the Controller related to the above will be reimbursed by the Controller to the extent such costs and expenses are not related to any requirements according to Applicable Laws imposed on the Processor or due to any breach of this Schedule F or the Agreement by Processor.
- 3.12 The Processor must reasonably assist the Controller with meeting the other obligations that may be incumbent on the Controller according to Union or Member State law where the assistance of the Processor is implied, and where the assistance of the Processor is necessary for the Controller to comply with its obligations. This includes, but is not limited to, at the request to provide the Controller with all necessary information about an incident under Clause 3.9(ii), and all necessary information for an impact assessment in accordance with Article 35 and Article 36 of the GDPR. Any reasonable documented costs and expenses pre-approved in writing by the Controller related to the above will be reimbursed by the Controller to the extent such expenses are not related to any requirements according to Applicable Laws imposed on the Processor or due to breach of this SCHEDULE or the Agreement by the Processor.

4 SUBPROCESSORS

- 4.1 The Processor may only engage a subprocessor, with prior specific or general written consent from the Controller. At the time of this Data Processing Agreement, the Processor uses the subprocessor listed in Annex 2. The Processor undertakes to inform the Controller of any intended changes concerning the addition or replacement of a subprocessor by providing a reasonable prior written notice to the Controller.

Data transfer and processing agreement

The Controller may reasonably and in a justified manner object to the use of a subprocessor. The Processor must inform the Controller in writing of the discontinued use of a subprocessor.

- 4.2 Prior to the engagement of a subprocessor, the Processor shall conclude a written agreement with the subprocessor, in which at least the same data protection obligations as set out in this Data Processing Agreement shall be imposed on the subprocessor, including obligations to implement appropriate technical and organizational measures and to ensure that the transfer of Personal Data is done in such a manner that the processing will meet the requirements of the Applicable Laws.
- 4.3 The Controller has the right to receive a copy of the relevant provisions of Processor's agreement with the subprocessor related to data protection obligations. The Processor shall remain fully liable to the Controller for the performance of the subprocessor's obligations under this Data Processing Agreement. The fact that the Controller has given consent to the Processor's use of a subprocessor is without prejudice for the Processor's duty to comply with this Data Processing Agreement.

5 CONFIDENTIALITY

- 5.1 The Processor shall keep Personal Data confidential.
- 5.2 The Processor shall not disclose Personal Data to third parties or take copies of Personal Data unless strictly necessary for the performance of the Processor's obligations towards the Controller according to this Data Processing Agreement, and on condition that whoever Personal Data is disclosed to is under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
- 5.3 The Processor shall ensure that all employees and any persons that it involves in the conduct of the Study comply with this Data Processing Agreement.
- 5.4 The Processor shall limit the access to Personal Data to all employees and any persons that it involves in the conduct of the Study for whom access to said Personal Data is necessary to fulfil the Processor's obligations towards the Controller.
- 5.5 The obligations of the Processor under Clause 5 shall continue until such time as provided by Applicable Laws and regardless of whether the cooperation of the Parties has been terminated.

6 TERM AND TERMINATION OF THE DATA PROCESSING AGREEMENT

- 6.1 Regardless of the expiry or termination, for whatever reason, of the Agreement, this Data Processing Agreement remains in force and applicable as long as the Processor processes Personal Data for the Controller under the Agreement.
- 6.2 In case of termination of the Agreement, the Processor must provide the necessary transition services to the Controller. The Processor is obliged to reasonably assist Controller at Controller's expense.

The Processor shall have appropriate procedures in place for the archiving of the Personal Data after the end of the Study in accordance with Applicable Law and at the end of the legally mandated archiving period ensure the destruction of the Personal Data and promptly inform Controller of the same.

- 6.3 If the Processor is required based on Union or Member State law to retain all or part of the Personal Data for a longer period than is possible based on the period mentioned in the Data Processing Agreement, the Processor shall immediately communicate this to the Controller, stating the basis, term and scope of such obligation. Once compliance with the obligation is no longer impeded by Union or Member State law, the Processor shall as yet erase the Personal Data in accordance with the provisions in the Data Processing Agreement.

Annexes:

Annex 1: Instructions

Annex 2: Subprocessors

Annex 3: EU Standard Contractual Clauses

Annex 1 – Instructions

This Annex 1 constitutes the Controller's instruction to the Processor in connection with the Processor's Personal Data processing for the Controller, and is an integrated part of the Data Processing Agreement.

Contact details of the Controller (including its Data Protection Officer, if applicable):

Monsieur Pierre-François PIRLET, Délégué à la protection des données dpo@uliege.be

Contact details of the Processor (including its Data Protection Officer, if applicable):

Mrs Ghislaine DUMONT dpo@chuliege.be
CHU de Liège Data Protection Officer

The processing of Personal Data

STUDY TITLE

Study of the relationship between the length of stay in intensive care and the intensity of Post-Intensive Care Syndrome (PICS)

a) Purpose and nature of the processing operations

This retrospective observational study is conducted in the context of a Master's thesis in Nursing Sciences at the University of Liège.

The purpose of the study is to evaluate the relationship between the length of stay in the Intensive Care Unit (ICU) and the intensity of Post-Intensive Care Syndrome (PICS) one month after ICU discharge.

Questionnaire data are routinely collected as part of the standard Post-Intensive Care Follow-up Program (CPSI) implemented at the CHU de Liège and are not collected specifically for this research project.

The processing operations that the Processor will execute within the above framework include:

- collection of questionnaire data routinely gathered within the Post-Intensive Care Follow-up Clinic (CPSI);
- extraction of demographic, clinical and hospitalization data from the CHU de Liège hospital information system (SIME);
- linkage of questionnaire and clinical data through an internal pseudonymized identifier;
- preparation and provision of a pseudonymized dataset for research purposes ;

b) Categories of data subjects

Adult patients previously hospitalized in the Intensive Care Unit of the CHU de Liège and included in the routine Post-Intensive Care Follow-up Program (CPSI).

c) Categories of Personal Data

- Age
- Sex
- Socio-economic status (BIM status when available)
- Internal pseudonymized identifier

No directly identifying personal data (name, surname, address, national registration number, telephone number or e-mail address) will be transferred for research analysis purposes.

d) Special categories of Personal Data

Health-related personal data including:

- Length of ICU stay
- Reason for ICU admission
- Medical history when available
- Mechanical ventilation exposure
- Delirium occurrence when available
- Severity indicators when available
- HABC-M-HV-F questionnaire scores (global score and subdomains)
- IPREA questionnaire responses regarding perceived discomfort during ICU stay
- Medical history
- Information related to ICU hospitalization
- Information related to treatments received during hospitalization
- Functional outcomes
- Cognitive outcomes
- Psychological outcomes
- Patient-reported quality of life
- Patient-reported experience data collected through the IPREA questionnaire
- Clinical information extracted from the hospital information system

No genetic data, biometric data or biological samples are collected within the framework of this study.

e) Address, city and country of all locations where the processing will be performed by the Processor on behalf of the Controller

Centre Hospitalier Universitaire de Liège (CHU de Liège)
Intensive Care Department – Post-Intensive Care Follow-up Clinic (CPSI)
Avenue de l'Hôpital 1
4000 Liège
Belgium

f) Specific security requirements

The following requirements reflect the minimum data processing requirements expected of the Processor. It is a condition that other agreed documents, legislation or industry standards laying down requirements of the processing of Personal Data in connection with Study/ mandatory safety monitoring are complied with as well.

1. The Personal Data may only be used for the Study and/or mandatory safety monitoring.
2. The collection, registration and other processing of Personal Data must be legally authorized under Applicable Laws, or applicable policies issued of the supervisory authorities.
3. Any person who takes part in the processing of Personal Data must be familiar with these requirements.
4. Premises used for the storage and other processing of Personal Data must be arranged in such a way as to prevent unauthorized access.

Data transfer and processing agreement

5. Appropriate security measures must be implemented to protect Personal Data against accidental or unlawful destruction, loss or impairment. Furthermore, it must be ensured that no incorrect or misleading Personal Data is processed. Incorrect or misleading data, or data processed in contravention of the above Applicable Laws, policy of the supervisory authority or these requirements, shall be rectified or erased.
6. Personal Data may not be stored in a way that makes it possible to identify the data subjects for longer than is necessary for the achievement of the Study and/or mandatory safety monitoring.
7. The publication of results from clinical studies must take place in such a way that it is impossible to identify individual persons.
8. It is a condition that other legislation laying down requirements of the processing of Personal Data in connection with Study and/or mandatory safety monitoring is complied with.

Electronic data

9. Identification data must be encrypted or replaced by a code number or similar. Alternatively, all data stored can be encrypted. Encryption keys, code keys, etc. must be stored securely and separately from the Personal Data. This also applies to Personal Data that is stored on portable devices such as laptop PCs, tablets, etc.
10. Data may only be accessed by using a unique user name and a confidential password. The password must be renewed at least once a year and when otherwise necessary in order to ensure the secure processing of the data.
11. On the transfer of Personal Data via the internet or other external networks, the necessary security measures must be taken to ensure that the Personal Data does not come to the knowledge of any unauthorized persons. This includes that encryption is required if sensitive Personal Data is transferred via the internet (or other open networks), and security of authenticity (identities of transmitter and recipient) and integrity (the authenticity of the transmitted Personal Data) must be appropriately ensured by the use of suitable security measures. On using internal networks, it must be ensured that no unauthorized persons can gain access to the data.
12. Removable storage media, safety copies of Personal Data, etc. must be stored securely and under lock and key, so that unauthorized access is prevented.

Manual ("paper") data

13. Manual material, including print-outs, error and control lists, etc. with Personal Data, must be stored securely under lock and key, and in such a way as to prevent unauthorized access.

Biobank and biological material

14. Samples with biological material and biological material in biobanks must be stored securely under lock and key so as to prevent unauthorized access, and in such a way as to ensure that the material is not lost, impaired, or accidentally or illegally destroyed.
15. Biological material collected for the purpose of the Study and marked with a civil registration number or name must be stored subject to special safety requirements.
16. Internal guidelines must be laid down within the Processor's organization regarding the project for the storage of biological material.

Information to be given to the Study Participant / Data Subject

17. Where the Personal Data is obtained from the Study Participant/ data subject (via interviews, questionnaires, clinical or para-clinical examination, treatment, observation, etc.), more detailed information concerning the clinical Study/testing/safety monitoring shall be distributed/forwarded to the data subject in accordance with Article 13 of the GDPR. The Study Participant must, via the privacy notice or via the informed consent form (as applicable) as drafted by the Controller and as approved by the relevant ethics committee and /or relevant authorities, be informed of the name of the Controller and of the name of the Processor with clear indication that the Processor shall act as the first point of contact with the Study Participant in connection to the processing of the Personal Data and/or with the exercise of rights granted to data subjects under the GDPR, the purpose of the trial/testing/safety monitoring, the fact that it is voluntary to participate in the trial/testing, the identity of any recipients of Personal Data, and the purpose of the disclosure of Personal Data, as well as any further information which is necessary for the Study Participant / data subject to be able to safeguard his/her interests. The data subject has been informed about the right of access to the Personal data that is processed concerning the person in question.

Disclosure

18. Disclosure/issue of Personal Data to other parties may take place to the extent that this is legally authorized under Applicable Laws.

On the conclusion of the project

19. At the latest on the conclusion of the Study/testing/safety monitoring the Personal Data (including biological material) shall be erased, made anonymous, or destroyed, unless Union or Member State law requires continued storage of the Personal Data. In accordance with Belgian Law as defined in the Agreement the Processor stores the medical records for at least 30 years, starting from the last Study Participant contact. It must not subsequently be possible to identify individuals participating in the clinical Study/testing/safety monitoring. The deletion of Personal Data must be properly documented.
20. Alternatively, the Personal Data may be transferred for further storage in archives according to the Controller's instructions. Any costs related to such transfer and further storage of Personal Data shall be borne by the Controller.
21. Erasure of Personal Data from electronic media shall take place in such a manner that it is impossible to recover the Personal Data and such erasure must be properly documented.

Annex 2 – Subprocessors

The Data Controller agrees that the Data Processor – subject to compliance with Clause 4 of the Data Processing Agreement – engages the parties listed below as subprocessors.

None.



Data transfer and processing agreement

Annex 3 - EU Commission's Standard Contractual Clauses for the transfer of Personal Data to third countries

Non applicable.

DTA TFE Sarah Neis-Gilson (JUR31792)

Rapport d'audit final

2026-06-25

Créé le :	2026-06-24
De :	Secrétariat SAJ (secretariatsaj@uliege.be)
État :	Signé
ID de transaction :	CBJCHBCAABAAfa-sFgaCIK8-TEzEz0Q2rU71qz8tGG7F

Historique de "DTA TFE Sarah Neis-Gilson (JUR31792)"

-  Document créé par Secrétariat SAJ (secretariatsaj@uliege.be)
2026-06-24 - 13:56:26 GMT
-  Document envoyé par e-mail à afdonneau@uliege.be pour signature
2026-06-24 - 14:01:25 GMT
-  Document envoyé par e-mail à afrousseau@uliege.be pour signature
2026-06-24 - 14:01:26 GMT
-  E-mail consulté par afdonneau@uliege.be
2026-06-24 - 17:40:13 GMT
-  Le signataire afdonneau@uliege.be a saisi ce nom lors de la signature en tant que Pr. AFr. Donneau
2026-06-24 - 17:40:32 GMT
-  Document signé électroniquement par Pr. AFr. Donneau (afdonneau@uliege.be)
Date de signature : 2026-06-24 - 17:40:34 GMT - Source de l'heure : serveur - Apparence de signature sélectionnée : TYPE
-  E-mail consulté par afrousseau@uliege.be
2026-06-25 - 02:42:37 GMT
-  Le signataire afrousseau@uliege.be a saisi ce nom lors de la signature en tant que AF Rousseau
2026-06-25 - 02:43:12 GMT
-  Document signé électroniquement par AF Rousseau (afrousseau@uliege.be)
Date de signature : 2026-06-25 - 02:43:14 GMT - Source de l'heure : serveur - Apparence de signature sélectionnée : TYPE
-  Accord terminé
2026-06-25 - 02:43:14 GMT

