Monitoring low-value care in medical patients from Swiss university hospitals using a Findable, Accessible, Interoperable, Reusable (FAIR) national data stream and patient and public involvement : LUCID study protocol

Guffi, Tommaso; Ehrsam, Julien; Débieux, Marie; Rossel, Jean-Benoît; Crevier, Marie-Josée; Reny, Jean-Luc; Stirnemann, Jérôme; Meier, Christoph A.; Aujesky, Drahomir; Bassetti, Stefano; Aubert, Carole Elodie; Méan, Marie

Collaborators: Lovis, Christian

LUCID REGISTRY

Low-Value Care in Medical Hospitalized Patients: a National Data Stream on Quality of Care in Swiss University Hospitals

Registry Description / General Framework

The Scope of this document is to describe the general framework of the **LUCID national registry**, by referring to essential documents needed for the registry establishment and maintenances.

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

LUCID
Low Value Care in Medical Hospitalized patients

TABLE OF CONTENTS

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

Glossary

LUCID	Low value care in medical hospitalized patient, a national data stream
CDW	Clinical Data Warehouse
DTUA	Data Transfer and Use Agreement
DTPA	Data Transfer and Processing Agreement
EB	Executive board
EC	Ethical committee
EHR	Electronic health records system
CHOP	Swiss classification of surgical interventions
LVC	Low value care
NDS	National Data Stream
SETT	Secure Encryption and Transfer Tool
SPHN	Swiss Personalized Health Network
UH	University Hospitals

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

1. INTRODUCTION

According to the Organization for Economic Co-operation and Development and evidence from different countries, low value care (LVC), defined as healthcare services providing little or no benefit to patients, is estimated to represent 20% of healthcare costs. LVC is common but varies between countries and according to services provided [1-3]. In Switzerland, LVC would amount to 16 billions CHF, according to Swiss Federal Statistical Office data. Therefore, recommendations for treatments / tests to be avoided, with an emphasis on futile treatments and tests where risks and costs may outweigh benefits, cover a broad spectrum of common diagnostic and therapeutic measures, mainly in the inpatient sector [1, 3-9] [5].

As both the number of patients and the cost of acute care are expected to increase in the future, LUCID registry aims to help avoiding healthcare waste, while satisfying inpatients expectations, which is key for the Swiss health system.

2. LUCID REGISTRY OBJECTIVES AND POPULATION

2.1. LUCID Registry Objectives

To date, the feasibility of a national quality improvement initiative based on a monitoring of LVC in hospitalized patients is limited by the lack of 1) a federated database in Switzerland and 2) detailed clinical information necessary to detect the provision of LVC in hospitalized patients. Thus, LVC frequencies and consequences of LVC in Swiss hospitals remain unknown.

The overarching goal of the registry is to promote sharing and access to existing routine clinical data of adult hospitalized patients within the five main national university hospital **to foster monitoring and research in the field of quality of care of medical hospitalized patients**. Changes and amendments to the Registry will be executed according to the consortium agreement.

LUCID registry provides a national picture of hospital quality of care based on existing clinical data. It enables researchers and clinicians to target areas needing quality improvement actions and to design future tailored interventions for improving the quality of medical inpatient care.

A major benefit of LUCID registry is its ability to monitor LVC, instead of indicators of performance, at low operational cost, using existing clinical routine data. Improving the quality of hospital care at low costs and resources satisfies healthcare administrators, patients, and care providers.

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

In summary, **the main objectives** of LUCID registry are:

1) To investigate the prevalence and trends of LVC
2) To assess the consequences and costs of LVC
3) To explore, using innovative approaches based on artificial intelligence / machine Learning and privacy-enhancing technologies, solutions to improve the quality of hospital care and reduce the waste of medical resources
4) To inform patients, healthcare providers, healthcare administrators and the public about the overall quality of the care.

In order to achieve those objectives, different studies (quality or research projects) will be conducted following executive board (and Ethical Commission, when applicable) approval as described in the consortium agreement (**Annex I: Consortium Agreement**).

2.2. LUCID Registry Population

LUCID registry is filled by existing routine clinical data of all adult hospitalized patients with or without general consent accepted, meeting the following criteria:

- Inclusion criteria: age ≥18 year old, hospitalized in one of the participating university hospitals (Geneva, Lausanne, Bern, Zürich, Basel), after 01.01.2014.
- Exclusion criteria: duration of hospitalization of less than 24 hours; hospitalization in non-medical wards (I.e., psychiatry, gynecology/obstetric, pediatrics, surgical wards).

Depending on the nature of studies, patient consent may be needed (ref. section 5.1 and 5.3).

3. THE REGULATORY FRAMEWORK AND STRUCTURE

A consortium agreement has been established and describes the contractual, and legal basis of the registry **(Annex I**), in order to regulate the general principles of collaboration (governance, allocation of work, rules for publications and intellectual property, financial conditions, etc.) between the consortium members. LUCID Consortium is composed of 17 members (academic physicians, nurse scientists, IT specialists and data scientists) from the five main University hospitals, the University of Fribourg and EPFL (detailed description in **Annex II**). Furthermore, according to the LUCID registry governance, an Executive Board has been setup whose roles and responsibilities are described in the consortium agreement.

It should be noted, that LUCID registry is a national project developed within the SPHN/PHRT framework and based on the request for developing NDS in Switzerland (National Data Streams -

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

SPHN). NDS are multidisciplinary-consortia research infrastructures (platforms) involving a national network of clinical and science/engineering partners. Therefore, the LUCID registry adheres to the SPHN Ethical Framework for Responsible Data Processing, the SPHN Information Security Policy and SPHN de-identification concept.

Following section 4 describes the LUCID registry data management, whereas section 5 depicts details on data management for specific studies using LUCID registry data.

4. LUCID REGISTRY DATA COLLECTION

4.1. IT infrastructure

The LUCID Registry database is hosted on the SENSA BioMedIT node (https://sensa.sib.swiss) operated by UNIL. On BioMedIT, a project-specific environment is called "B-space" (**Fig. 1 and 4**). B-spaces are specialized environments that are segmented into specific study-spaces (quality or research project), and allow project members to collaborate from multiple institutions, but also maintain the security of the data imported in the B-space.

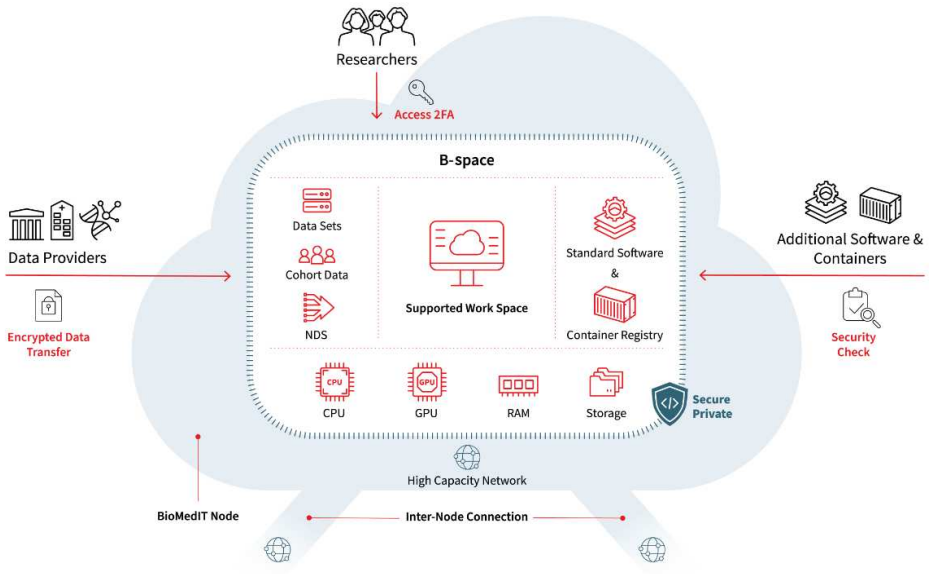

***Figure 1**. B-Space overview (source https://www.biomedit.ch)*

LUCID Registry data are securely transferred from the University Hospitals to the LUCID Registry B-space using end-to-end encryption based on public-key cryptography via the SETT tool provided by BioMedIT (https://sett.readthedocs.io/en/stable/). Data from CHUV and HUG will be sent directly to SENSA (Lausanne BioMedIT node), while data from Inselspital, USB and USZ will be sent to the BioMedIT nodes sciCORE and SIS, respectively, and then transferred through the BioMedIT network to SENSA (**Figure 2**). IT security measures in the BioMedIT nodes are implemented according to the

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

"SPHN/BioMedIT Information Security Policy" approved by hospitals' Chief Information Security Officers. Data security mainly relies on the allocation of project-specific IT resources within an access-controlled, private, and virtual environment offering network isolation, data isolation, and computational resources isolation (**Figure 2**). BioMedIT strictly controls the access to the Internet, which is limited to trusted and explicitly whitelisted web resources.

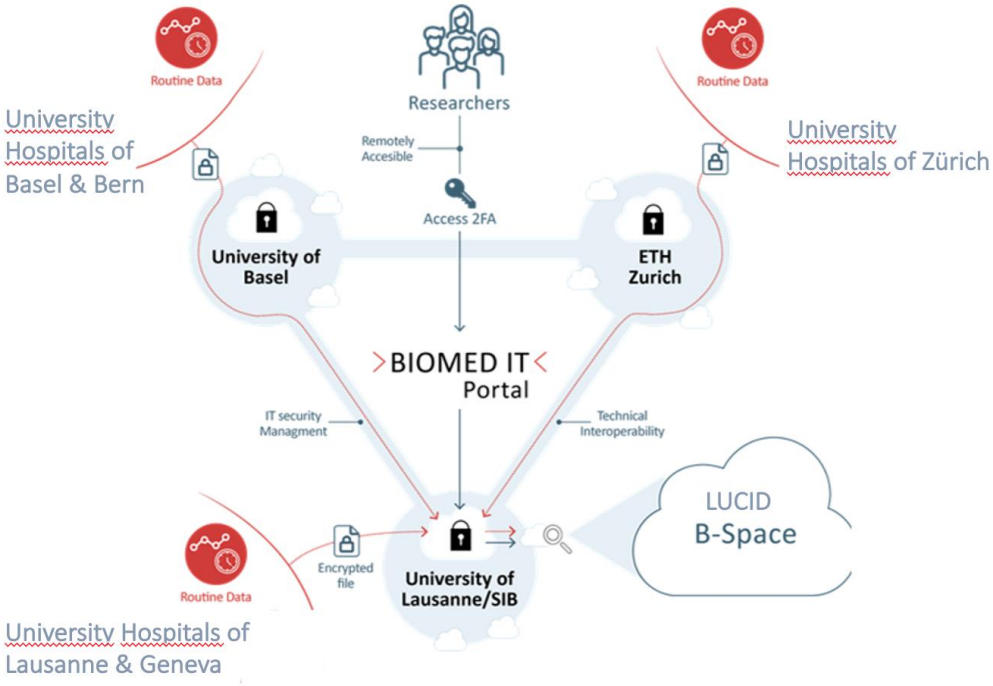

***Figure 2**. High-level data flow from University Hospitals to SENSA (UNIL) BioMedIT node.*

In addition to B-spaces, the LUCID infrastructure leverages:

- **A meta-data/dataset catalog (under development by BioMedIT)**: The catalog stores meta-data about variables available in the registry (e.g., type, format, provenance, mapping to standards) and about archived project datasets that have been curated and are available for re-use (e.g., size of the dataset, related publications, project PI, conditions of re-use).
- **A cohort explorer**: The cohort explorer enables researchers to run feasibility queries, which consists in obtaining patient counts for user-specified inclusion/exclusion criteria, using the i2b2 (https://www.i2b2.org) open-source cohort explorer. Patient privacy in i2b2 is ensured as it natively provides only patient counts that can be further obfuscated by adding Gaussian

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

noise to minimize risk of inference attacks on summary statistics to achieve differential privacy.

Both these tools are accessible to researchers inside and outside the consortium and contributes to the "Findability" and "Accessibility" of LUCID Registry data for further use.

The LUCID Registry adheres to the SPHN Ethical Framework for Responsible Data Processing and the SPHN Information Security Policy for the data hosting infrastructure.

4.2. Variables imported into LUCID registry

The registry contains variables described in the **Annex IV**. These data are collected during hospital clinical routine.

Type of collected variables:

- Administrative data, including costs and insurance data
- Drug administered/prescribed during the hospital stay
- Diagnostic (using ICD-10 codes) observed during the hospital stay
- Lab results obtained during the hospital stay, including bacterial resistance to antibiotics
- Clinical parameters (blood pressure, temperature, SO_2, height and weight, clinical scores, ...) collected during hospital stay
- Clinical interventions such as medical devices (e.g. urinary or blood catheter, ECG); any radiological investigations; any surgical intervention (using CHOP codes) performed during hospital stay
- Clinical outcome such as death

Between 2014 and 2022, a mean of 50'000 patients per site is expected to be included in the registry. Afterwards, additional patients will be included in the LUCID registry, with a total of approximately 50'000 additional patients per year.

4.3. Data re-identification risk assessment

A registry data re-identification risk assessment and the related data de-identification policy is provided as an appendix to this LUCID registry description/general framework (**Annex III**). The risk assessment and de-identification policy are based on the SPHN de-identification concept and will be periodically updated to consider the evolution of the registry and the advancements of the technology.

The SPHN de-identification concept and related risk-assessment template has been developed by the SPHN "DeID Task Force" and aims to enable data providers to perform the evaluation of the re-

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

identification risk associated with the transfer of their data for research purposes. The template, which is organized in an Excel file (**Annex III**), collects information on the project's specific setup and foreseen de-identification strategy through a set of multiple-choice questions. Based on heuristics, practical methods and expert determination, each combination of question-answer is assigned a risk level. The weighted sum of the risk levels across all questions determines the re-identification risk profile associated with the project's dataset and the envisioned use case. The assessment of the risk of re-identification is multi-dimensional as it considers an intersection of domains (technical, organizational and contractual). The risk of re-identification tied to the data itself considers direct and indirect identifiers that are present in the dataset. This risk is evaluated also considering the de-identification rules that will be applied to the identifiers prior to the data transfer. The contextual measures, such as legal agreements and IT security mechanisms that regulate and limit the access to the data once out of the hospital's IT infrastructure, also contribute to further reduce the risk.

Applying this risk score to LUCID dataset (**Annex IIIa**) we obtained a low-risk score of 0.5 (green zone <0.51) and a set of related de-identification rules to be applied to the data before transfer to the secure registry B-Space:

- Direct identifiers: "Direct identifiers are replaced by pseudonyms"
- Date of birth: "Only the year of the original birthdate is kept"
- Professions: "Profession will be suppressed"
- Locations: "Only regions are kept"

To ensure that the risk of disclosure of personal private information in the data that each University Hospitals (UH) provides to the registry is minimized, each UH will de-identify its data before it is transferred to the registry. De-identification is performed according to the above-mentioned rules defined by the "LUCID data de-identification policy" provided as an appendix to this document (**Annex IIIa**). In summary, direct identifiers (such as patient identifiers) is replaced by registry-specific pseudonyms at each data provider. The re-identification key will be securely stored in the respective hospital and never disclosed to the users of the registry (i.e., registry data manager, authorized persons or researchers). Thanks to the re-identification key, patient re-identification is possible, should the need arise or for legal reasons.

4.4. Interoperability

Each institution must ensure that the transcription of the source data into LUCID registry follows applicable quality and regulatory standards, and ensure data integrity, quality, privacy and security. Therefore, the data import must by performed by dedicated and qualified staff and the institution should have a proper infrastructure in place. The LUCID registry has at least one expert dedicated to data management activities and reference person for any concerns (LUCID data manager).

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

As mentioned above, to ensure that the risk of disclosure of personal private information is very low, each University Hospitals (UH) must apply the rules defined the "LUCID data de-identification policy" provided as an appendix to this document (**Annex IIIa**).

To connect and communicate efficiently in a coordinating way, syntactic and semantic interoperability has been set up and each institution must be compliant with the Work Instruction LUCID guidelines (**Annex V**) in order to properly import the variables in the LUCID registry. For example, all medical data are encoded by appropriate interoperability standards, defined by SPHN, such as ICD-10, ATC, GTIN, SNOMED-CT, HPO, etc. The compliance of the data to these standards is checked by applying SHACL rules at the hospital IT level.

Moreover, at each site, quality tests are performed on the LUCID data by an IT dedicated team to detect outliers, inconsistencies for a given patient, and discrepancies between different sources of data (refer to Work Instruction LUCID guidelines, **Annex Va**).

Similarly, in the LUCID registry B-space, the LUCID data manager also performs quality controls, such as interoperability compliance, data completeness (refer to work instruction LUCID B-space guidelines, **Annex Vb**).

4.5. LUCID registry Access and Conditions

Only the LUCID data manager and the consortium members authorized by the LUCID Project Leader have access to the LUCID Registry B-space.

Authorized persons accessing LUCID data must complete the mandatory course "SPHN/BioMedIT Data Privacy and IT Security Training" provided by the BioMedIT node hosting the LUCID data before they are granted access to the data[1]. This course explains the legal and regulatory context of personalized health research and what should be done in practice to protect the patients' privacy when performing biomedical research on human data. A certificate is released upon the successful completion of the course. Additionally, authorized persons are asked to follow the course "Responsible Health Data Usage" also available on the BioMedIT platform Web site to learn the key points of the SPHN Ethical framework for responsible usage of health data in biomedical research.

4.6. LUCID registry archiving

Storage capability, security policies, and backup procedures of SENSA are available at the following link: https://sensa.sib.swiss. At the registry closure, all the datasets will be archived for at least 10 years on a CHUV secured server.

[1] https://www.biomedit.ch/home/outreach-training/training.html

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

5. STUDIES ASSOCIATED TO LUCID REGISTRY

5.1. General framework for studies using data from LUCID registry

The Executive Board oversees the evaluation and decision regarding internal (conducted by at least two parties of the consortium) and external studies (conducted in collaboration with third parties), except for 4 studies already founded (SPHN/PHRT Joint Call for Proposals on National Data Stream (NDS), recipients of SPHN/PHRT funding agreed in February 2022) as mentioned in the consortium agreement (**Annex I**).

LUCID executive board verifies that foreseen studies using data of the registry meet the purposes and missions of LUCID registry, that the risk of re-identification is low and that studies are led by "bona-fide" researchers as detailed in the consortium agreement. Acceptance of a given study (quality or research project) and related data access, including the necessity of patient consent, is further conditioned by EC approval when applicable (**Figure 3**).

To be granted access to the LUCID Registry's data, for the purpose of either an internal or external collaboration study, researchers or data requesters shall meet a certain number of conditions described in detail in the LUCID Consortium Agreement (**Annex I**).

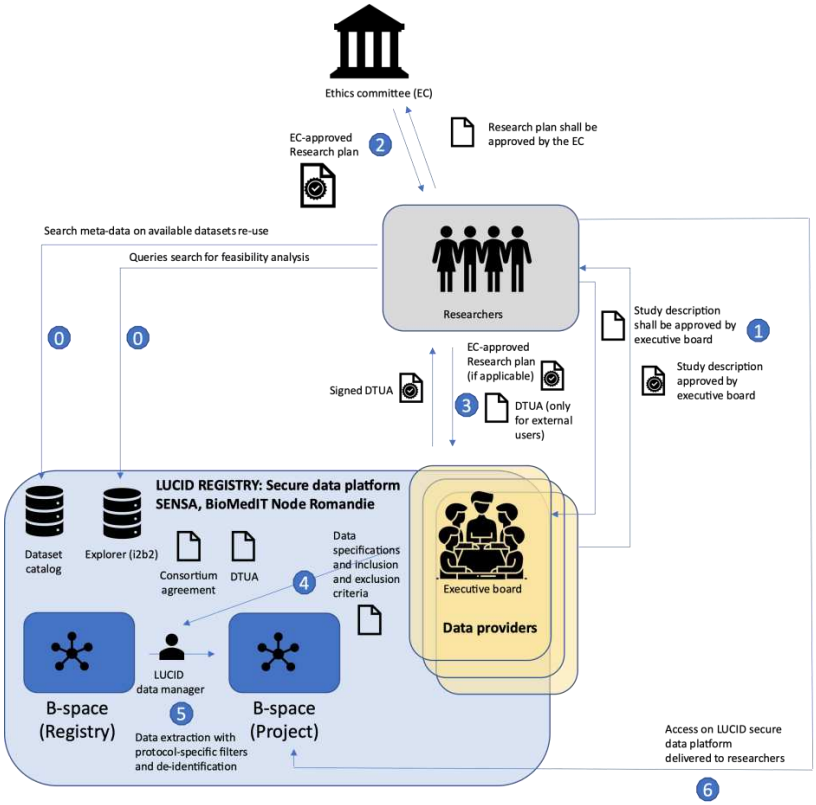

Figure 1. *Process for further use LUCID registry data by third parties.*

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

The main steps for the data access procedure are depicted in **Figure 3** and described below:

- **Step 1:** The data requester submits a study description to the LUCID Registry Executive Board (EB) for validation. In addition, a re-identification risk assessment specific to the study dataset is performed by the LUCID data manager, in close collaboration with the study specific project leader to evaluate if further de-identification of LUCID registry data is needed for the specific study.
- **Step 2:** Following EB approval, the study protocol is reviewed and approved by the Ethics Committee (EC), when applicable, before requesters are allowed to access the data. Some quality studies may require a waiver from the Ethics Committee.
- **Step 3:** The requester complies with the rules of the Registry detailed in the current document and the Consortium Agreement (CA) and signs a Data Transfer and Use Agreement with the EB, represented by the project leader (**Annex I**).
- **Step 4**: Following EB and ethical committee (if applicable) approval, the study-specific project leader communicates the data specifications along with the research protocol to the LUCID Data Manager.
- **Step 5:** The LUCID Data manager pushes the data from the LUCID Registry B-space to the "Project" B-space or other platform (see section 5.2).
- **Step 6:** The data requester is granted access to the requested dataset on a "Project" B-space and can access it after a 2-factor authentication via Switch eduID.

5.2. IT infrastructure for studies associated to LUCID registry

5.2.1. BioMedIT infrastructure

On BioMedIT, a project-specific environment is called "B-space" (**Figure 4**). B-spaces are specialized environments that are specific to a single study (quality or research project), and allow project members to collaborate from multiple institutions, but also maintain the security of the data imported for the project. While data, applications and methods can be reused within the BioMedIT platform (if applicable), each use should be within the environment of a specific approved project.

For each study using LUCID registry data, the use of BioMedIT B-space is recommended in the first place. Another platform can also be used as long as the risk assessment (**Annex IIIb**) is performed and the resulting risk falls in the "low risk" category (see section 5.2.1).

- **"Project" B-space**: this B-space hosts project-specific datasets extracted from the "LUCID Registry" B-space. For each study, the LUCID Data Manager is responsible for extracting the

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

requested data for the project transforming it to the desired format (e.g., RDF, csv, json) and pushing it to a project-dedicated folder on this B-space. For each project, only authorized researchers can access this B-space on their project-dedicated folder. Segmentation of data for different projects is ensured by UNIX access control lists.

Authorized researchers or data requesters accessing LUCID data on the "Project B-space" have to complete the mandatory course "SPHN/BioMedIT Data Privacy and IT Security Training" provided by the BioMedIT node hosting the LUCID data before they are granted access to the data[2]. This course explains the legal and regulatory context of personalized health research and what should be done in practice to protect the patients' privacy when performing biomedical research on human data. Additionally, researchers are asked to follow the course "Responsible Health Data Usage" also available on the BioMedIT platform Web site to learn the key points of the SPHN Ethical framework for responsible usage of health data in biomedical research.

Once done, authorized researchers or data requesters connect on on BioMedIT to their own project secure "Project B-space" workspace for which they have been authorized explicitly (see, **Figure 3**). The connection to the "Project B-space" is made possible via a virtual desktop or a virtual terminal environment after a 2-factors authentication step enabled by the Switch eduID infrastructure. Legal agreements set up for the project (**Annex I**) provide contractual and technical measures preventing data to be shared and/or combined without appropriate authorization. Transfer, access, and processing operations are logged. In addition, physical access to the BioMedIT node's server room is tightly controlled.

5.2.2. Other platform(s)

Other IT platforms, different than BioMedIT, can be used to host and project data extracted from the LUCID Registry, as long as a formal risk assessment is performed and researchers / data requesters have received the EB authorization. The risk assessment must follow the SPHN de-identification concept (**Annex IIIb**) which takes into account technical, organizational and contractual measures for protecting privacy and security of patient data. The resulting risk should fall in the "low risk" category.

5.3. Patient consent in studies associated to LUCID registry

All five participating University Hospitals have deployed a general consent for routine data and biological material reuse in the field of clinical research. For each study (quality or research) the need

[2] https://www.biomedit.ch/home/outreach-training/training.html

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

and the type of patient consent (i.e. general consent or study specific consent or EC waiver of consent need) will be defined in the study protocol together with term of withdrawal of consent.
The general consent status will be reassessed in the LUCID registry every 3 months by each hospital, while refreshing data imported in the LUCID registry. This is part of the work instruction LUCID guidelines (**Annex Va**) provided to each UH.

5.4. Study-specific data re-identification risk assessment and variables export from LUCID registry

For every new study, additional de-identification rule, such as generalization of certain fields or date shifting, is applied to indirect identifiers, according to the study-specific risk assessment evaluation (**Annex IIIb**). As specified in the LUCID data de-identification policy (section 4.3) the goal is to decrease the residual re-identification risk into the "low" category while preserving as much as possible the utility of the data for downstream analyses.

To ensure that when transferred outside of the secure LUCID registry BiomedIT infrastructure, the result of statistical queries and analyses (for e.g., in public dashboards, scientific publications, open datasets catalogs), including trained machine learning models, considered aggregate-level information, or the release of microdata, considered individual-level information, do not disclose sensitive private information about LUCID patients, we apply techniques from statistical disclosure control[3]. Particular attention is paid to privacy risks stemming from the release of machine learning models.

To quantitatively assess the risks of a potential disclosure of private information from statistical and machine learning algorithms, we will use tools such as the "Privacy Meter"[4]. Privacy Meter uses state-of-the-art inference techniques to audit a wide range of machine learning algorithms for classification, regression, computer vision, and natural language processing. It generates extensive reports about the aggregate and individual privacy risks for data records in the training set, at multiple levels of access to the model. If the privacy risks that are associated with a potential release of the results of a statistical or machine learning analysis are deemed too high for a given data sharing scenario, EB will ensure that researchers or data requesters will mitigated by applying protective technical measures such differential privacy.

[3] https://en.wikipedia.org/wiki/Statistical_disclosure_control
[4] https://github.com/privacytrustlab/ml_privacy_meter

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

5.5. Specific study protocol, analysis and reports

The Executive Board oversees the evaluation and decision regarding internal and external studies based on a dedicated outlines template (**Annex VI**). If accepted, internal (conducted by at least two parties of the consortium) and external studies (conducted in collaboration with third parties) must describe in detail in a study protocol, the planned analyses / presentation of the results. For each study, a protocol will define the people who will contribute to it *a priori* and who will be the "authors" and those who will just be listed as "o*n behalf of the LUCID consortium* ".

5.6. Specific study archiving

Each study protocol must describe in detail the archiving terms and duration. Moreover, study-specific data hosting needs shall be regulated by a separate agreement.

6. OVERVIEW OF LUCID DATA FLOW

The data flow is summarized in the figure below.

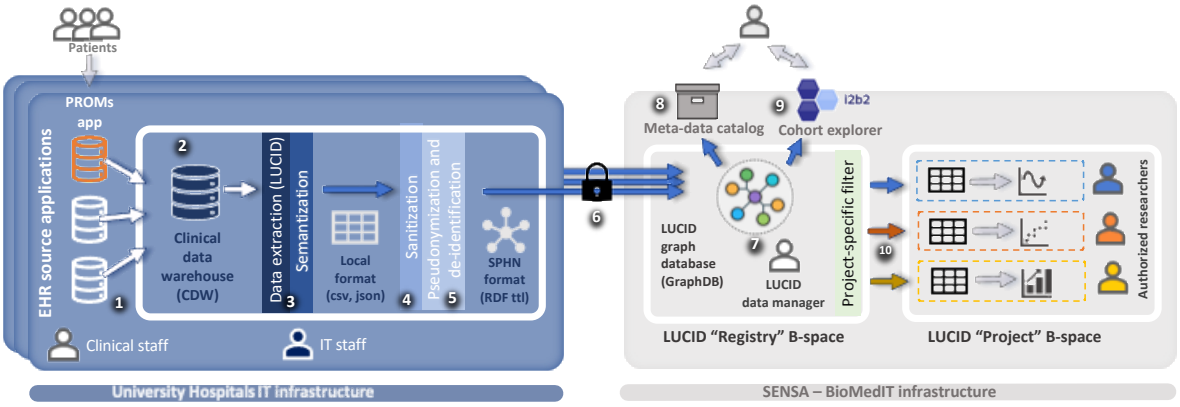

Figure 4*. LUCID data flow main steps from hospital to BiomedIT infrastructure.*

1. Clinical hospital data are routinely collected in EHR source applications by healthcare personnel.
2. At each hospital, data from source applications is automatically pulled into the central clinical data warehouse.
3. LUCID data is extracted from the clinical datawarehouse by trained IT staff according to the registry inclusion/exclusion criteria and mapped to SPHN syntactic and semantic interoperability standards (**Annex Va**).
4. At each UH, data sanity checks for consistency and completeness are executed to remove outliers, duplicates, and inconsistent records.

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

5. LUCID data is de-identified following the "LUCID data de-identification policy" (**Annex IIIb**).
6. Standardized, sanitized and de-identified data are converted to the RDF format and sent to the Registry B-Space by using the SETT encryption tool provided by BioMedIT.
7. Data from all participating hospitals are decrypted by the LUCID data manager and consolidated into a graph (RDF) database that provides more flexibility and better data explorability with respect to conventional relational databases. Graph databases are recommended by SPHN (**Annex Vb**).
8. The meta-data of sanitized datasets are annotated and stored on the BioMedIT meta-data/dataset catalog.
9. A copy of the research dataset will be stored on i2b2 for future feasibility analyses (to plan future studies).
10. Project-specific datasets will be extracted from the registry and pushed to the "Project" B-space (or another platform) and analyzed by authorized researchers.
11. Authorized researchers for each project are granted access to their project data for analyses within the B-space secure environment
12. Each study protocol must describe in detail the archiving terms and duration.

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

LUCID
Low Value Care in Medical Hospitalized patients

7. REFERENCES

1. Ganguli, I., et al., *Low-Value Care at the Actionable Level of Individual Health Systems.* JAMA Intern Med, 2021. **181**(11): p. 1490-1500.
2. Mafi, J.N., et al., *Trends in Low-Value Health Service Use and Spending in the US Medicare Fee-for-Service Program, 2014-2018.* JAMA Netw Open, 2021. **4**(2): p. e2037328.
3. Rosenberg, A., et al., *Early Trends Among Seven Recommendations From the Choosing Wisely Campaign.* JAMA Intern Med, 2015. **175**(12): p. 1913-20.
4. Levinson, W., et al., *'Choosing Wisely': a growing international campaign.* BMJ Qual Saf, 2015. **24**(2): p. 167-74.
5. *Smarter Medicine*. Available from: https://www.smartermedicine.ch/fr/page-daccueil.html.
6. *Choosing Wisely Initiative*. July 2021; Available from: https://www.choosingwisely.org/clinician-lists/american-society-clinical-pathology-routine-preop-testing-for-low-risk-surgeries-without-indication/

   https://www.choosingwisely.org.au/recommendations/tsanz6.
7. *Choosing Wisely Canada*. July 2021; Available from: https://choosingwiselycanada.org/recommendations/.
8. Blum, M.R., et al., *Optimizing Therapy to Prevent Avoidable Hospital Admissions in Multimorbid Older Adults (OPERAM): cluster randomised controlled trial.* BMJ, 2021. **374**: p. n1585.
9. Aubert, C.a.c., *Proton pump inhibitors in older multimorbid patients: what are longitudinal patterns of prescribing and deprescribing, and what are the potential adverse effects?* under review (unpublished), 2022.

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

8. LIST OF ANNEXES

I. LUCID Consortium agreement, DTUA and DTPA (Regulations)

II. Consortium members

III. Risk assessment evaluation for data exported to LUCID registry

IV. Dataset using SPHN ontology

V. Work Instruction LUCID guidelines: Va. For hospital; Vb. For LUCID B-spaces (work in progress)

VI. Template for study submission to Executive Board (available at: www.lucid.nds.ch)

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

ANNEX I: see consortium agreement (separate document)

ANNEX II: Consortium members

1. **PD Dr. med. Marie Méan** (Senior physician in internal medicine, **Lausanne University Hospital** (CHUV) and Privat Docent, University of Lausanne): **Registry Director**.
2. **Dr. Guillaume Obozinski, PhD** (Deputy Chief Data Scientist at the Swiss Data Science Center, **EPFL & ETH Zürich**): **Registry co-director**.

Co-applicants from the clinical side:

3. Prof. D. Aujesky, MSc (Chief physician of the Department of General Internal Medicine, Inselspital, Bern University Hospital)
4. PD Dr. med. J. Stirnemann (Senior physician in internal medicine at Geneva University Hospital (HUG)
5. Prof. S. Bassetti (Chief physician of the Department of General Internal Medicine, Basel University Hospital)
6. Prof C. Meier (Chief physician of the Department of General Internal Medicine, Inselspital, Zürich University Hospital)
7. PD Dr. med C. Baumgartner, MAS, (Senior physician in the Department of General Internal Medicine, Inselspital, Bern University Hospital)
8. PD Dr. med F. Vallellian, (Senior physician in the Department of General Internal Medicine, Zürich University Hospital)
9. Dr. med. Florian Rüter (Head of Quality Management at University Hospital Basel)

Co-applicants from IT/Data Science side:

10. Prof. Christian Lovis (Chairman, Medical Information Sciences, University Hospitals of Geneva)
11. Dr. Jean-Louis Raisaro, PhD (Data Science Lead at CHUV Data Science Division, Lausanne University Hospital)
12. Dr. med. Bram Stieltjes, PhD (Vice Chair of Research in Radiology, Head of Research and Analytics, ICT, University Hospital Basel)
13. Prof. A Leichtle (Professor of computational and laboratory medicine, Inselspital and University of Bern)
14. Dr. Oksana Riba Grognuz (Head of Open Research Data Engagement & Services at the Swiss Data Science Center, EPFL & ETH Zürich)
15. Prof. Manuela Eicher, BScN, MScM, PhD (Director of IUFRS, University of Lausanne Head of the Patient Lab in Oncology affiliated to the Swiss Cancer Center Leman, member of the Federal Quality Commission)
16. Prof Arnaud Chiolero, MD PhD, epidemiologist and public health physician, Full Professor at the University of Fribourg, Director of the Population Health Laboratory (https://projects.unifr.ch/pophealthlab/).
17. Jérémie Despraz (Senior Data Scientist at CHUV IT Department, Lausanne University Hospital).

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

Table: Field of expertise of the consortium and synergies

	Medical Inpatient Care	Quality of Care / LVC	Data semantic	Health data science	ETH Domain
M. Méan	✓	✓			
G. Obozinski				✓	✓
D. Aujesky	✓	✓			
C. Meier	✓	✓			
J. Stirnemann	✓	✓			
S. Bassetti	✓	✓			
C. Lovis	✓		✓	✓	
J.L. Raisaro			✓	✓	
B. Stieltjes			✓	✓	
O. Riba Grognuz				✓	✓
A. Leichtle				✓	
C. Baumgartner	✓	✓			
F. Rueter		✓			
F. Vallelian	✓				
M. Eicher		✓			
A.Chiolero		✓		✓	
J. Despraz				✓	

At the time of the initiation of LUCID Registry:

- **Data manager:** Cyril Matthey-Doret, engineer, EPFL
- **Project Manager:** Tommaso Guffi, physician, CHUV

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662

LUCID
Low Value Care in Medical Hospitalized patients

ANNEX III. Risk assessment evaluation for data exported to LUCID registry

- **Annex IIIa: Risk assessment evaluation for data exported from hospitals to LUCID registry**

  Available upon request (separate document)

- **Annex IIIb: Risk assessment evaluation for data exported from LUCID Registry to project B spaces (work in progress)**
  Available upon request (separate document)

ANNEX IV: Dataset using SPHN ontology

Available upon request (separate document)

ANNEX V: Work Instruction LUCID guidelines

(work in progress for hospitals and BioMed IT/B spaces)

ANNEX VI: Template for study submission to Executive Board

Available at: www.lucid.nds.ch

Guffi T, *et al. BMJ Open* 2024; 14:e089662. doi: 10.1136/bmjopen-2024-089662