pharma.be
ASSOCIATION GÉNÉRALE DE L'INDUSTRIE DU MÉDICAMENT
ALGEMENE VERENIGING VAN DE GENEESMIDDELENINDUSTRIE

be MedTech

Secondary use of patient data for scientific purpose

Guideline on the applicability of the General Data Protection Regulation (GDPR) and the Belgian Personal Data Protection Law

01.10.2025

pharma.be vzw | asbl
Algemene Vereniging van de Geneesmiddelenindustrie (A.V.G.I.) | Association générale de l'industrie du médicament (A.G.I.M.)
Kantersteen 47, Brussel 1170 Bruxelles | tel 02 661 91 11 | info@pharma.be | www.pharma.be
BTW – TVA BE 0407.622.902 | Ondernemingsnummer – Numéro d'entreprise 0407.622.902 | RPR Brussel
beMedTech vzw| asbl
Romeinsesteenweg 468, 1853 Strombeek-Bever | info@bemedtech.be | www.bemedtech.be | tel 02 /257 05 90

Secondary use of patient data for scientific purpose

Guideline on the applicability of the General Data Protection Regulation (GDPR) and the Belgian Personal Data Protection Law

Table of contents

Context

(Bio)pharmaceutical and medtech industries share the commitment to advance healthcare and improve the quality of life of patients. At the core of their missions lies a profound dedication to research, innovation, and collaboration with the ultimate goal to improve healthcare outcomes. Research and development are the cornerstone of these industries, which results in a continuous cycle of discovery and innovation. Through strategic partnerships with academia, healthcare providers, healthcare organizations, government agencies, and patient groups, these industries invest resources to push the boundaries of medical science. This does not only result in the development of new treatments and technologies but also contributes to the advancement of medical knowledge and the evolution of healthcare delivery models.

Real World Data (RWD) is an umbrella term for data regarding the effects of health interventions (e.g. safety, effectiveness, resource use, etc.) that are not collected in the context of highly-controlled Randomized Clinical Trials (Makady *et al*., 2017). RWD can either be primary research data (i.e. collection of new data which reflects how interventions are used in routine clinical practice) or secondary research data (i.e. further use of data from already existing data sources such as databases).
In a real-world health data ecosystem, **all partners contribute** to well-informed value decisions, based on an **optimal access to RWD** and **acceptance of Real World Evidence** (RWE) in order to create a better health for patients. It is exactly these three conditions of a health data ecosystem that also triggers the major challenges.

In (bio)pharmaceutical and medtech research, the potential of health data is relevant throughout the whole lifecycle of a medicine or medical technology. This applies to a drug discovery phase and its clinical/mechanical development, the cost-effectiveness of the medicine or technology in real-world practice, the monitoring of patient safety and a better understanding of the expression of a condition within a population group (such as the amount of patients suffering from a disease given the prevalence of certain genetic characteristics within the total population). The data needed to answer these research questions include for example clinical (such as patient demographics, medical history, lab results, treatment outcomes, surgical outcomes,…) and economic outcomes, administrative data (such as claims data, Minimal Hospital Data (MZG) data from FPS Public Health, operation room time,…), patient-reported outcomes (PRO) and health-related quality of life (HRQoL).

These data are to be found in RWD sources available for instance (but not only) in the hospital such as, among others, patient registries, electronic medical records, claims databases and other hospital data.

Primary data actively collected in clinical studies are difficult, slow, and expensive to obtain. Furthermore, medical technologies are often hard to be evaluated with randomized clinical trials as it is hard to blind and randomize technologies due to strong ethical and practical issues in the choice of the ‘comparator’. The secondary use for research purposes of patient data that already exist, as they were captured for their primary purpose in routine healthcare, may be a beneficial alternative.

On March 5, 2025, the European Health Data Space (EHDS) was officially published, marking a major step forward for healthcare and biopharmaceutical innovation in Europe. EHDS establishes a legal framework for secure, standardized exchange of health data across Member States, enabling better access to RWD for research and policy-making.

For the biopharmaceutical industry, EHDS opens new opportunities for real-world evidence generation, streamlined clinical trials, and accelerated development of innovative treatments. It supports data-driven decision-making, personalized medicine, and improved public health strategies—while maintaining high standards for privacy and security.

While Belgium's national implementation of EHDS is still pending, this guideline aims to clarify how the General Data Protection Regulation (GDPR) applies to the secondary use of health data in the interim.

Content and objective of the guideline

The present guideline focuses on the applicability of the General Data Protection Regulation (GDPR) and the Belgian Personal Data Protection Law and its most relevant aspects to pharma and medtech companies' secondary use of patient data for scientific research purposes that were already collected by health care providers (HCPs) and health care organizations (HCOs) for routine care and treatment purposes (primary use of the data). Please note that other legislations than the GDPR have to be considered, such as the Sunshine Act, but this is out of the scope of the guideline.

The pharma.be members were in need for such a guideline due to different interpretations of the GDPR and the complexity of different possible scenarios in practice. Therefore, this guideline aims at facilitating the harmonisation of managing RWD projects under the current GDPR and relevant Belgian Personal Data Protection laws. These guidelines are equally supported by beMedTech's members.

This guideline does not cover primary data collection projects, such as RWD projects where patients are providing directly their health data in the frame of surveys, apps or wearables.

It aims at providing a methodology for members of pharma.be and beMedTech to assess the application of the Belgian Data Protection law and mainly the GDPR to a secondary use of personal data-project (retrospective studies/analysis of data that were collected for another purpose) and focuses on the following aspects of the GDPR:

- The anonymisation process of personal data, which is a central question to determine the applicability of the GDPR
- The role/qualification of each involved party
- The purpose limitation principle
- The legal basis for the processing of the personal data
- The transparency obligations
- The contractual agreements that need to be in place for the processing of personal data
- The need for additional safeguards for the data protection

This methodology is also illustrated by different concrete use cases. This guidance is non-binding and is to be considered only as an internal guide for members of pharma.be and beMedTech. It reflects the interpretation of the dedicated pharma.be and beMedTech working group, and it is not intended and should not be considered as legal advice. The guidance has not been discussed with the competent national authorities. This guidance may be updated from time to time to accommodate the changing privacy and legal landscape. The list of use cases is given as an illustration and is not exhaustive.

Methodology to assess the applicability of the GDPR to projects of secondary use of data

Step 1: Applicability of the GDPR: Are the patient data necessary to meet your research request already anonymized or not?

- **Why is anonymization key to determine GDPR applicability?** GDPR applies in case of "processing" of personal data.
- Personal data include identified, identifiable but also pseudonymised data.
- GDPR does not apply to "anonymous" (= not identifiable) data.
- The process of anonymization of personal data is considered a "processing" activity regulated by the GDPR.
- In most RWE projects, pharma companies are only asking for an anonymized/statistical report. The question of **timing of the anonymization** of the data is however central in all RWE projects to understand whether GDPR applies to the project or not. Indeed, companies must have a discussion with the HCP/HCO on **whether the patient data are already existing and available in an anonymized format or not at the moment the pharma company is asking for their secondary use. In other words, will anonymization still need to be performed to meet their research request or not.** An interpretation of the concept of anonymisation as described in the "Common Position" of CHAB/RUZB[1] may facilitate this discussion.
- **If your research project can be performed without having to process any personal (identified, identifiable or pseudonymized) patient data because anonymous/anonymized data are already available and are sufficient to provide you with the requested report, personal data shall not be used and GDPR will not apply to your project. You can then stop this analysis after Step 1. Please however review this applicability if there is any change to your project.**

How can you know that the data necessary for your research request are already existing in an anonymized format? Ask and discuss with the HCP/HCO/third party. Which type of data are already existing and available for your research request? Which type of data do they have to process for you? Understanding their data handling processes and anonymization techniques will also help you to assess the level of privacy protection.

Note: Do not confuse the initial data that have to be anonymized to provide you with the report and the report itself[2]. The question asked here is related to the initial data to be used to provide you with the report. The report itself will in most cases be anonymized or even aggregated but it might have required to work on personal (identifiable or pseudonymized) data. If your research request requires the HCO/HCP to provide you with a report where data are not anonymized, these data should at

[1] https://www.univ-hospitals.be/common-position-establishing-a-framework-for-secondary-use-of-real-world-data-routinely-collected-in-hospitals/

[2] Recital 72 of the EHDS allows a situation where the data holder may be considered an independent controller: "*Moreover, a health data applicant should be able to request a response to a health data request in an anonymised statistical format. In such cases, the health data user will only process non-personal data, and the health data access body will remain sole controller for any personal data necessary to provide the response to the health data request*".

least be pseudonymized AND a justification of why it is not possible to work with anonymized data should be kept at disposal[3].

When are data considered "anonymized"?

It will often be very difficult to achieve anonymization.

- Recital 26 of the GDPR:
  - To determine whether a natural person is identifiable, **account should be taken of all the means reasonably likely to be used**, such as singling out, either by the controller or by another person **to identify the natural person directly or indirectly**. To ascertain whether means[4] are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.
- CHAB/RUZB definition of anonymous/anonymized data (https://www.univ-hospitals.be/common-position-establishing-a-framework-for-secondary-use-of-real-world-data-routinely-collected-in-hospitals/):
  - Data can be considered as anonymous or anonymized, only when it is not possible to "single-out" individuals with the data provided and when the applied mechanisms to anonymise are irreversible.
  - Anonymization of health data may be difficult to achieve due to, inter alia, unicity of health-related data, the need to at all times keep source data and the (legal) requirements to ensure traceability. Therefore, you may need to rely on pseudonymized data instead.
  - In the context of RWE, personal data are often aggregated. Aggregated data can be considered anonymized, provided that a "small cell risk assessment" has been considered making sure that even if the group of concerned patients is very small, data remain anonymous.
- One should pay attention to the situation of rare diseases or for specific medical devices with a low rate of availability/implementation where there are so few patients that a risk of re-identification may exist even if the data has been anonymised.

Note: anonymous data is not identifiable data from the start, while anonymized data is data initially identifiable but for which a process has been put in place to make it not identifiable anymore.

[3] Article 132 of the Belgian Act of 30 July 2018 foresees the cascade of anonymous, pseudonymous or non-pseudonymous data.
[4] The CJEU further interpreted the criterion "means reasonably likely to identify the natural person" in its Breyer decision (Case C-582/14) : "that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".

Proposed criteria to determine whether data are anonymous/anonymized/de-identified

1. Is the natural person identifiable?

- **a Guidance Regarding Methods for De-identification of Protected Health Information** in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule[5]

2. Are there objective factors preventing re-identification?

- The WP29 in its Opinion 05/2014 on Anonymization Techniques, explains that there is **risk of re-identification** by:
  - Singling out (isolate data belonging to an individual)
  - Linkability (linking records concerning the same person between separate files or databases)
  - Inference (deduce a value or attribute belonging to a person)

Step 2: Determination of the parties' role(s)

If Step 1 has confirmed that GDPR applies to your project, defining the roles of the parties is crucial in order to understand the responsibilities and obligations of each party, and what type of contractual arrangements are needed.

The actual situation and division of the capacities will always depend on how the study is conceived, who has a decisive role in this study and what is included in the study protocol/the study agreement.

- If the RWD are **processed to meet a legal obligation**, the roles are probably defined by law. Be aware that it is not because data are asked by a public authority (e.g. RIZIV/INAMI) that the data are required by law.
- **The company** asking for a further processing of the data (secondary use) will be considered a **data controller** if it specifies the purpose and the means of the data processing (independently or jointly with the hospital).
- **The HCP/HCO having collected the data for their primary use (care) will be with respect to the further processing, either:**
  - Independent controller → No influence or involvement in the Secondary use of the data.
  - Joint controller: if the HCO/HCP has decisive influence on purpose and important means of the Secondary use project.
  - Processor: if HCO/HCP merely processes the data on behalf of the Company (e.g., specific instructions to draft a report using RWD).

If any, an **Authorized Third party** will usually be data processor.

[5] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

For more information, please refer to the EDPB[6] guidelines 07/2020 that describes the concepts of controller and processor in the GDPR.

Note: In addition, the hospital could also be an independent controller when further processing the data for its own purposes in addition to the processing for the pharma or medtech company.

Step 3: Purpose limitation

Personal patient data must always be collected for specified, explicit and legitimate purposes (by the controller/HCP/HCO):

1. The Primary purpose is the care of the patients for example.
2. The Secondary purpose is the further purpose for which the data will be used (e.g. scientific research).

The Secondary purpose must be compatible with the Primary purpose for which the data have initially been collected and processed (Article 5(1)(b) of the GDPR). The information that patients have received at the moment their data is collected is important to understand for what Primary purpose(s) their data has or will be used.

Are the primary and secondary purposes for processing compatible?

Two possibilities:

1. The purpose of the secondary use is "scientific research": Further use for scientific research is assumed to be compatible with the initial purpose (Article 5.1(b) and Recital 50 GDPR) provided that the safeguards in terms of data minimisation of Art. 89(1) are in place (cfr. Infra i.e. data should be anonymized where possible and, if not possible, at least pseudonymized).
    - See also the notion of "scientific research" below.
2. The secondary purpose is not for research purposes (e.g. for commercial purpose) and hence, is not assumed to be compatible with the primary purpose:
    - Does the secondary purpose processing rely on explicit and specific patient consent or a legal obligation? => OK
    - If no patient consent or legal obligation, a "compatibility test" (art. 6.4 GDPR) must be performed. In principle, this assessment is carried out by the controller before accepting the transferring, making available or otherwise processing the data for the secondary purposes.

[6] https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_hu

What is considered "scientific research" under (article 89) of the GDPR?

- The scope of the notion of scientific research has not been clarified by the European authorities yet. However, the following texts can be used to interpret this notion:

  - Recital 159 GDPR: Broad interpretation of "scientific research":
    "Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. ***For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.*** *In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area.* ***Scientific research purposes should also include studies conducted in the public interest in the area of public health.*** *To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures."*

- Article 53, 1 (e) European Health Data Space (EHDS) lists purposes for which electronic health data can be processed for secondary use[7]:
  "(e) scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators, including:
  (i) development and innovation activities for products or services ;
  (ii) training, testing and evaluation of algorithms, including in medical devices, in vitro diagnostic medical devices, AI systems and digital health applications."

- Article 29 Working Party Guidelines on consent under Regulation 2016/679 of 10 April 2018, p.2
  "the notion of scientific research may not be stretched beyond its common meaning and understand that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice."

- NB: The EDPB is working on a definition of "scientific research". This Guidance might be amended as appropriate in the future to comply with this upcoming definition.

Step 4: Legal basis and processing of sensitive data

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

The GDPR requires that each processing of personal data must have a ”legal basis”. Article 6 GDPR sets out what these potential legal bases are, namely: consent; contract; legal obligation; vital interests; public task; or legitimate interests.

In addition, the processing of “sensitive” personal data (e.g. health related data) is prohibited, except for limited circumstances. Such processing requires both a legal basis under Article 6 GDPR, as well as meeting one of the conditions of Article 9 which allow such data to be processed.

To determine the legal basis, we differentiate between the initial processing of the patient data by the hospital in the context of the provision of care (the primary purpose) and the subsequent processing of patient data by the hospital and/or the pharma or medtech company for scientific research (the secondary purpose).

The initial processing activity must be based on one of the six legal bases listed in Article 6 GDPR. Because it concerns health data, the processing must also be based on a legal basis from Article 9.2 GDPR.

According to the EDPB[8], when it concerns research based on patient data collected in the context of health care which is later used for scientific research purposes, it concerns further secondary processing for a different purpose.

While the GDPR mandates a legal basis for each processing activity and purpose (article 6.1 GDPR), it does not necessarily require a pharma or medtech company to establish its own separate legal basis when it acts as a (joint) data controller. This is because article 6.4 GDPR permits the legal basis for further processing to be derived from the initial processing performed by the hospital.

However, some legal authors argue that a separate legal basis is required for secondary research. An alternative option of the pharma or medtech company is to choose to establish its own legal basis for scientific research instead of relying on the initial legal basis used by the hospital. In that case, the legal basis can either be the consent or the legitimate interest. Because the consent as legal basis is not the most appropriate one (limited to a more restricted population and hence data set, can be withdrawn,...), legitimate interest would then usually be considered as a the most appropriate legal basis.

Step 4.1: Is the Secondary purpose compatible with the Primary Purpose of collection/processing of the data?

- **Yes:** in that case, recital 50 of the GDPR indicates that “no legal basis separate from that which allowed the collection of the personal data is required”[9].

[8] EDPB, Guidelines 03/2020 on the process of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21 April 2020, 6

[9] NB : Some legal authors still argue that a separate legal basis is required for secondary research. . Usually the legitimate interest (art. 6, 1, f GDPR is then used).

- **No:** a new legal basis is required:
  - Consent:
    - Consent might not be considered as an appropriate legal basis for this type of projects because of (i) the difficulty to meet the requirements for valid consent (i.e. a freely given, specific[10], informed, and unambiguous indication of the data subject's wishes (Art. 4 (11) GDPR)), (ii) the risk of unwanted bias (e.g. research group may not be representative if you only work with people who have given consent) (iii) the risk that the patient withdraws her/his consent and the difficulties to manage this withdrawal.
    - However, consent could be relevant when no alternative exception is available to the general prohibition to not process health-related data (Article 9 GDPR). In these cases, the patient's explicit and specific consent should prevail (e.g. request to further process RWD for purely commercial objectives that cannot qualify as research, nor on obligation of public interest).
  - Public interest described in a law[11]
  - Contract to which the data subject (patient here) is a party[8]
  - Legitimate interest: When relying on "legitimate interest" as a legal basis, the controller must document how it balances these interests against the rights and freedoms of the data subject (article 6 (1)f GDPR and cfr. CJEU in Rigas case, C-13/16, 4 May 2017)

Step 4.2: Even if the purposes are compatible, is it allowed in this case to process health-related data (see article 9 GDPR about "Sensitive data")

Article 9 GDPR foresees some exceptions to the prohibition to process sensitive data, including health data (subject to all other GDPR conditions of course). The following 3 conditions might be relevant here:

1. Explicit and specific consent of the data subject (patient here)
2. Data manifestly made public by the data subject
3. Data processed for Scientific Research provided that a law foresees this possibility, and that the safeguards of Art. 89(1) are respected (data minimization by use of anonymous/anonymized data only and if not possible, at least pseudonymization) cfr. Infra, In other words, the GDPR allows the processing of personal health data for research purposes if data minimisation principles are strictly applied and if a law foresees this possibility. Unlike many other EU countries, Belgium has fortunately adopted such law and more particularly articles 194 and more of the data protection law of 30 July 2018.

   These articles foresee a.o. an obligation to have a contract between the Primary and the Secondary users of the personal data.

[10] E.g. Although Recital 33 GDPR mentions the possibility of using "broad consent" (i.e. data subjects have the opportunity to give their consent to certain areas of for scientific research), strictly speaking, this consent cannot be considered specific nor informed. The EDPB says: when research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. In addition, adequate safeguards should be in place to enhance the transparency of the processing during the research project and to ensure that the requirements on specificity of consent are met as best and as soon as reasonably possible (https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf)

[11] Not usually relevant for commercial companies

Be aware that even if you are allowed to process personal data related to the health of a data subject, you still have to respect all the other obligations foreseen in the GDPR, including transparency (and hence information) to this data subject.

Step 5: Transparency

Article 12 of the GDPR imposes to the Controller(s) to provide concise, transparent, intelligible and easily accessible information to the data subject, using plain and clear language. The information must be provided in writing or by other appropriate means.

In addition, article 14 of the GDPR foresees some conditions when the personal data have not been obtained from the data subject directly, which is mostly the case in the frame of Secondary use of patient data. However, this article 14 also foresees some limitations and nuances to the information obligation.

Step 5.1: Does an exception to the obligation to provide information apply?

The exceptions are, amongst others, the following:

1. Data subject is already sufficiently informed:
   - Check with the HCO/HCP whether the patient has already been provided the necessary information on the secondary use (e.g. digital solutions exist whereby patients have direct access to their health record and have a personalised overview of any secondary use of data). Make sure you can document the fact that patients have already been informed.

2. Providing information is impossible or requires disproportionate effort:
   - "Impossibility" arises only when the controller can demonstrate the factors preventing it from providing the information to the data subjects
   - A balancing test should be performed between:
     - Cost / impact of investment and efforts
     - Effects of absence of information on data subjects' rights
   - Examples of justification of impossibility to provide individual information: huge number of patients involved where there is no available contact information, age of data, etc.

3. Providing information would entail undesirable ethical risk:
   - This exception would arise for instance when transparency obligation would cause patients to be informed about their medical condition, despite having expressed a right not to know. This exception is not foreseen in the GDPR but in article 7 §3 of the law of 22 August 2002 relating to patients' rights.

Step 5.2: if information to data subject is required, consider the following best practices

- According to the CHAB/RUZB, transparency is achieved by combining different stages and levels of information (e.g. combination of posters in the waiting room, information on the website of the hospital, information on the digital health record of the patient etc.)
- Coordination with the HCO/HCP will be needed to ensure compliant transparency
- If information is provided on an electronic platform, patients should be aware on how to access the info.
- Consider the specific situation of minors.

Step 6: Provision of the patient data by the Primary user to the Secondary user

In the very specific case of projects where one single third party is pseudonymizing the patient data from several HCOs/HCPs and analyzing/combining/processing these data all together to provide an even more meaningful and representative report to a controller (e.g. the pharma company), in terms of patient population, this third party could potentially represent the different HCOs/HCPs in the Agreement in order to avoid for the controller to sign an Agreement with each involved HCO/HCP. This would of course require the appropriate legal mandate from the concerned HCP/HCO towards this third party.

Step 7: Additional measures and data protection by design foreseen by the GDPR

When personal data are processed for the purpose of "Scientific research", a specific regimen applies (e.g. the compatibility of purposes is presumed, company is allowed to process health-related data), provided that additional measures are in place.

There is no exhaustive list of additional safeguards, but, the processing of the data should be organised in a way that the rights of the data subjects are protected in any way ("data protection by design").

Step 7.1: What additional measures are in place to ensure data protection "by design"?

1. Data used and provided in the report are preferably anonymized and, if not possible, pseudonymized (cfr. supra); the impossibility to use anonymized data must be documented and kept on file.
   Data minimisation: Researchers should strive to minimize the amount of personal data held. De-identify or pseudonymise data by removing identifying details as early in the process as is feasible (Art. 5 (1),(c) GDPR).
2. A Register of Processing Activities must be held including, for each type of processing, when relevant, the specific motivation why pseudonymised data is (not) used.
3. Data Protection Impact Assessment (DPIA) in case of sensitive data:
   a. A DPIA is mandatory when the nature of the processing potentially entails a high risk for the rights and freedoms of data subjects.
   b. Several criteria to indicate that processing is likely to create a high risk to rights and freedoms.

4. Deliberation of the Information Security Committee if it concerns a data transfer between 2 separate controllers.
5. Applicable ethics framework (incl. Declaration of Taipei).
6. Involve DPO if there's likely to be a large scale processing of health related data.

Further use of health data: some practical use cases

Different scenarios are possible:

I. **Data Transfer** between the HCO/hospital and a pharma or medtech company: company asks to pseudonymize or anonymize patient personal data, receives the pseudonymised/anonymised raw dataset and performs the analysis.
II. **Data Access** by pharma or medtech company (no transfer of any copies of the data): the company gets access to the personal data on the Controller's systems (no transfer) and performs the analysis itself as well.
III. **Data Report** asked by pharma or medtech company: company asks Controller to extract some personal data from its existing database(s) or from patients records and generate an anonymized (or exceptionally, pseudonymized) report answering the company's specific request. The Controller can sometimes use a Third Party to perform the extraction, pseudonymization/anonymization and report drafting tasks.
IV. 'Standard' anonymised data purchase report ("**off the shelf**"): pharma or medtech company asks a report on or a copy of data that are already existing in an anonymized format at the moment the company asks for a report.

Please also note, even if not mentioned explicitly, a third party can be involved in every scenario.

Use case 1: Hospital data provided to a pharma company via a third party acting upon request of the pharma company

In use case 1, a 3rd party has built a data warehouse upon request of a hospital; this data warehouse is containing data initially collected from the patients of the hospital in order to improve their care (= the primary processing). The collected data are systematically pseudonymised and the hospital only holds the key for the de-pseudonymisation.

Next to this activity for the hospital, the 3rd party offers services to pharmaceutical companies related to these data (= a secondary processing of the data). Pharmaceutical companies can ask scientific questions based on a protocol. After the approval by the hospital for the processing of the data to respond to this request, the 3rd party will process (pseudonymise) the data needed to answer to the scientific question and provide a report containing only aggregated data. The company only get anonymized/aggregated data in this proposed example.

1. Does the GDPR apply to that relationship?

To respond to this question, one should consider whether, in this specific example of use case, the data are already anonymized or whether the anonymization of the data is still to be performed to respond to the request of the pharma company.

If the data (existing under a pseudonymised format in de warehouse) are anonymised (= processed) upon request of the company => the GDPR applies.

> **Note**: specific attention should be paid in case of rare disease when considering anonymisation.

2. What are the roles of the parties for the primary and secondary processing?

	If hospital has limited influence on the protocol (i.e. does not collaborate with the company on the drafting of the protocol (purpose, methodology, design of the study, data to be collected, inclusion/exclusion criteria…)	If protocol is jointly written and decided by hospital and company
Hospital	Primary (separate) controller for the collection and storage (in the data warehouse) of patient data for the purpose of patient care	Controller for the collection and storage in the data warehouse of patient data for the purpose of patient care Joint controller with the pharma company for the secondary use of data to answer to the scientific questions based on the jointly drafted protocol
3d Party processing the data upon request of the Company	Processor for the company process the data in accordance with the protocol drafted by the Company.	Processor for the joint-controllers to process the data in accordance with the protocol drafted by them.
Company	Secondary (separate) controller for the secondary use of data to answer the scientific questions based on the solely drafted protocol	Secondary joint controller for the secondary use of data to answer the scientific questions based on the jointly drafted protocol.

3. Which agreement between the parties should be in place?

a. An **agreement** for the secondary use of the data between the hospital (controller) and the pharma company (controller) (cfr supra)
b. A **data processing agreement** between the 3d party (processor) and the pharma company (controller) (according to art. 28 GDPR) (cfr supra)

> **Note**: it is possible for the 3rd party to get a mandate from the pharma Company to represent it in its Secondary use agreement with the Hospital. In this case, there will be only one tri-partite agreement signed between the Hospital (as Controller) and the third Party (as Processor and as representative of the Secondary Controller=Company).

Use case 2: a pharma company requests data to Sciensano to respond to a scientific question, healthdata.be being the third party

The database(s) of healthdata.be is built based on data collected from the patients by general practitioners for the primary care (primary processing). All the data are pseudonymized and can be made available upon request from a pharma company to respond to a scientific question (secondary processing). Sciensano will perform an analysis of the data to respond to this request. This analysis can be part of their general legal mandate or could be outside of this legal mandate, and hence specifically performed upon request of the pharma company.

1. **Does the GDPR apply to that relationship?**

   To respond to this question, one should consider whether the data are already anonymized or whether the anonymization of the data is done to respond to the request of the pharma company. All the data in the database of healthdata.be are pseudonymised. Upon request, the pharma companies may have access to the pseudonymised data, or data anonymized for them.

   If the data are anonymised (= processed) upon request of the company => the GDPR applies. If the company has access to pseudonymised data, the GDPR applies.

2. **What are the roles of the parties for the primary and secondary processing?**

	Accessing an existing register	Building a new data collection (analysis outside of the legal mandate of Sciensano)
(healthdata.be sciensano)	Controller	Processor
Company	Controller	Controller

3. **Which agreement between the parties should be in place?**

   In the situation where a new data collection should be built and the analysis is performed outside of the legal mandate of Sciensano, a **data processing agreement between processor (Sciensano) and the controller (pharma company)** (according to art. 28 GDPR).

   In the situation where data of an existing register are used and the analysis of the data is performed within the legal mandate of Sciensano, the relationship is a controller-controller relationship for the secondary processing. No agreement is required according to article 28 of the GDPR (as this may not be a controller-processor scenario). However, it is strongly advised to have an agreement in place to define the term and conditions for this processing and the obligations of each one (controller-controller).

Use case 3: retrospective studies from hospitals

In the case of retrospective studies on hospital health data conducted by a pharma company, several situations are possible.

- In a first case, fully anonymised data are provided by the hospital institution upon request of a pharma company:
  - These fully anonymised data can be off-the-shelf data, meaning that they were already existing in an anonymized format in an already existing set of anonymised data. Another possibility would be that the anonymized report meeting the needs of the pharma company is already existing at the moment the pharma company expressed its request.
  - Or existing (non-anonymized) data can be anonymised by the hospital to respond to the request of the pharma company.
- In a second case, pseudonymised data are provided by the hospital institution upon request of the pharma company.

1. Does the GDPR apply to that relationship?

To respond to this question, one should consider whether the data are already anonymised or whether the anonymisation of the data is done to respond to the request of the pharma company.

- In the first case, when the **fully anonymised data provided by the hospital is part of an already existing set of anonymised data** (off-the-shelf data), there is no processing of the data generated by the request of the pharma company, and hence the **GDPR does not apply to the company**.
- When the **data are anonymised by the hospital**, and hence processed, to be provided to the pharma company and respond to its request, the **GDPR applies**.
- In the second case, when **pseudonymised data** are provided to the pharma company by the hospital, the **GDPR applies to the company**.

2. What are the roles of the parties for the primary and secondary processing?

	Data anonymised upon request of the company or data pseudonimised upon request of the company and provided to the company	
	The hospital does not collaborate with company on the drafting of the protocol of the retrospective study (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, etc.)	The hospital has a decisive influence over the protocol of the retrospective study
Hospital	Processor of the company for the secondary use	Joint controller with the company for the secondary use of data to answer the scientific questions based on the jointly drafted protocol Processor of the company for the secondary use
Company	Separate controller for the secondary use of patient data to answer the scientific questions based on the solely drafted protocol	Joint controller for the secondary use of data to answer the scientific questions based on the jointly drafted protocol.

3. Which agreement between the parties should be in place?

There should be an **agreement for the secondary use of data, including data processing agreement (cfr supra) between the hospital and the pharma company)** according to art. 194 of the Belgian law on data protection.

Use case 4: Farmanet

In this use case, there is no processing of personal data, the pharma company has access only to data related to the sales medicines. Hence the GDPR does not apply.

Glossary

- **Real World Data**[12] as routinely collected data relating to a patient's health status or the delivery of health care from a variety of sources other than traditional clinical trials.

- **Real World Evidence**[9] as the information derived from the analysis of RWD.

- **Controller**: The data controller determines the purposes for which and the means by which personal data is processed. There is a:

  - **Primary controller**: the institution/organisation/individual who originally processed the data for their primary purpose. E.g. The healthcare professional, the hospital/HCO, the general practitioner processing the data for primary care purpose

  - **Secondary controller**: the institution/organisation/person who is asking the processing of these data for other further purposes and is determining means and purposes for this further processing (= the secondary use). E.g. the pharmaceutical company, or the controller himself (hospital/HCO). A research purpose is not always present during the primary data collection, but can be decided on a later by the collecting institution

  - **Two controllers** can act jointly, and hence are joint controllers when together with one or more organisations it jointly determines 'why' and 'how' personal data should be processed. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules

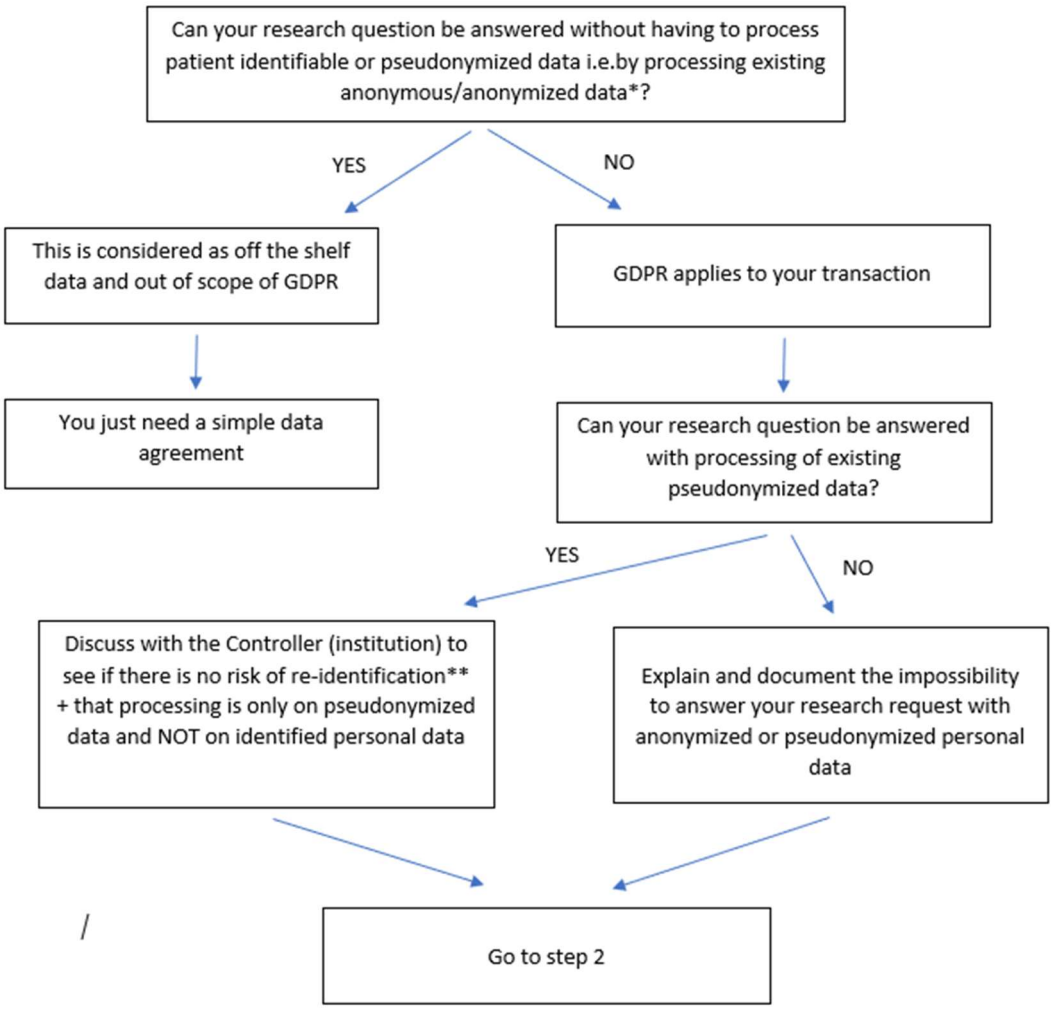
- **Processor**: The data processor processes personal data only on behalf of the controller. The data processor is usually a third-party external to the company

- **Information Security Committee**: By the law of September 5, 2018, the Information Security Committee was established. It consists of two chambers: the Social Security and Health Chamber, located at the KSZ and the eHealth Platform, and the Federal Government Chamber, located at the FPS BOSA. It has specific missions in the field of information security - including the granting of deliberations for certain types of communications of personal data.

[12] A.Cave1, X.Kurz1 and P. Arlett (Pharmacovigilance and Epidemiology Department, European Medicines Agency), 2019, Real-World Data for Regulatory Decision Making: Challenges and Possible Solutions for Europe, https://doi.org/10.1002/cpt.1426

Flow charts

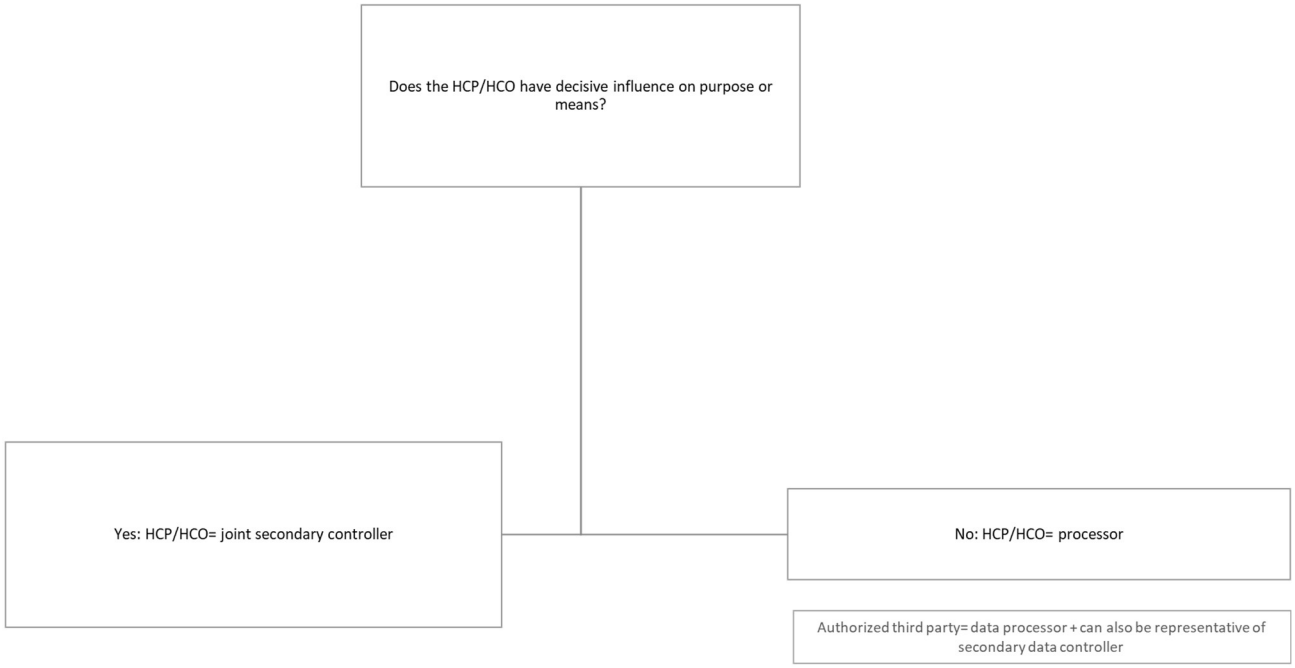
Step 1: Anonymisation



** Data can be considered as anonymous or anonymized, only when it is not possible to "single-out" individuals with the data provided and when the applied mechanisms to anonymise are irreversible.*

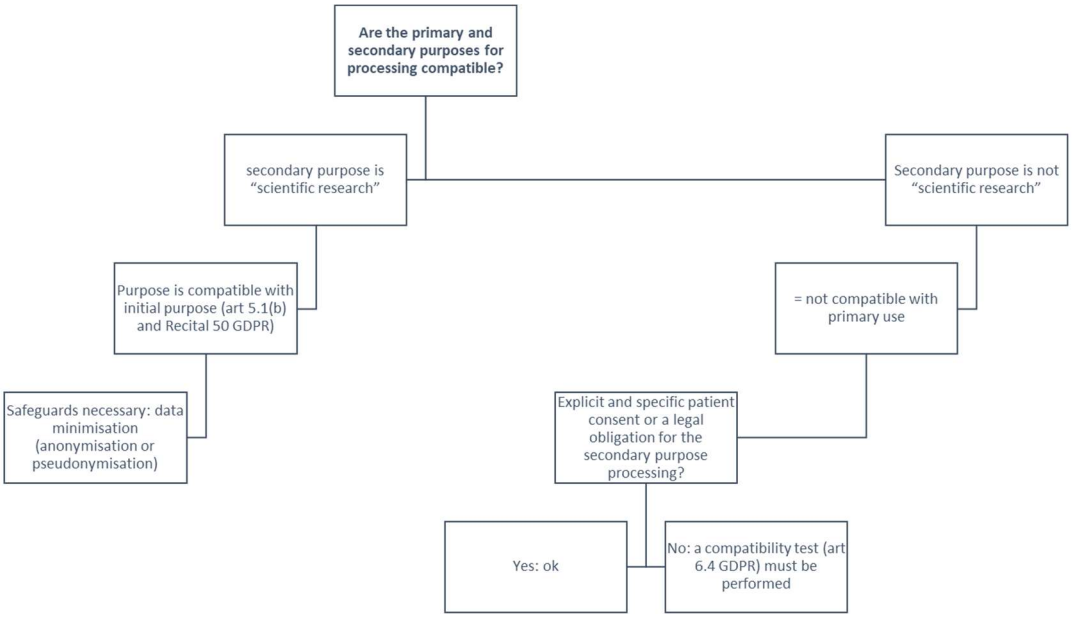
*** For rare diseases for example, the risk of re-identification may exist even if the data has been anonymised as there are only a few patients. Take this into account when assessing whether the available data is really anonymous or, if combined with others or in a specific environment, there is a reasonable risk of re-identification*

Step 2: Determination of the parties' roles

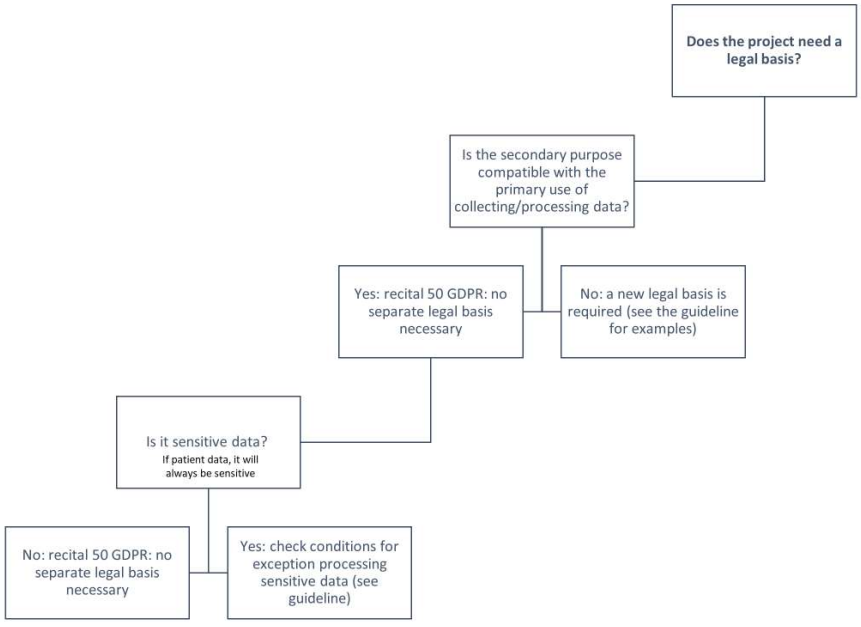


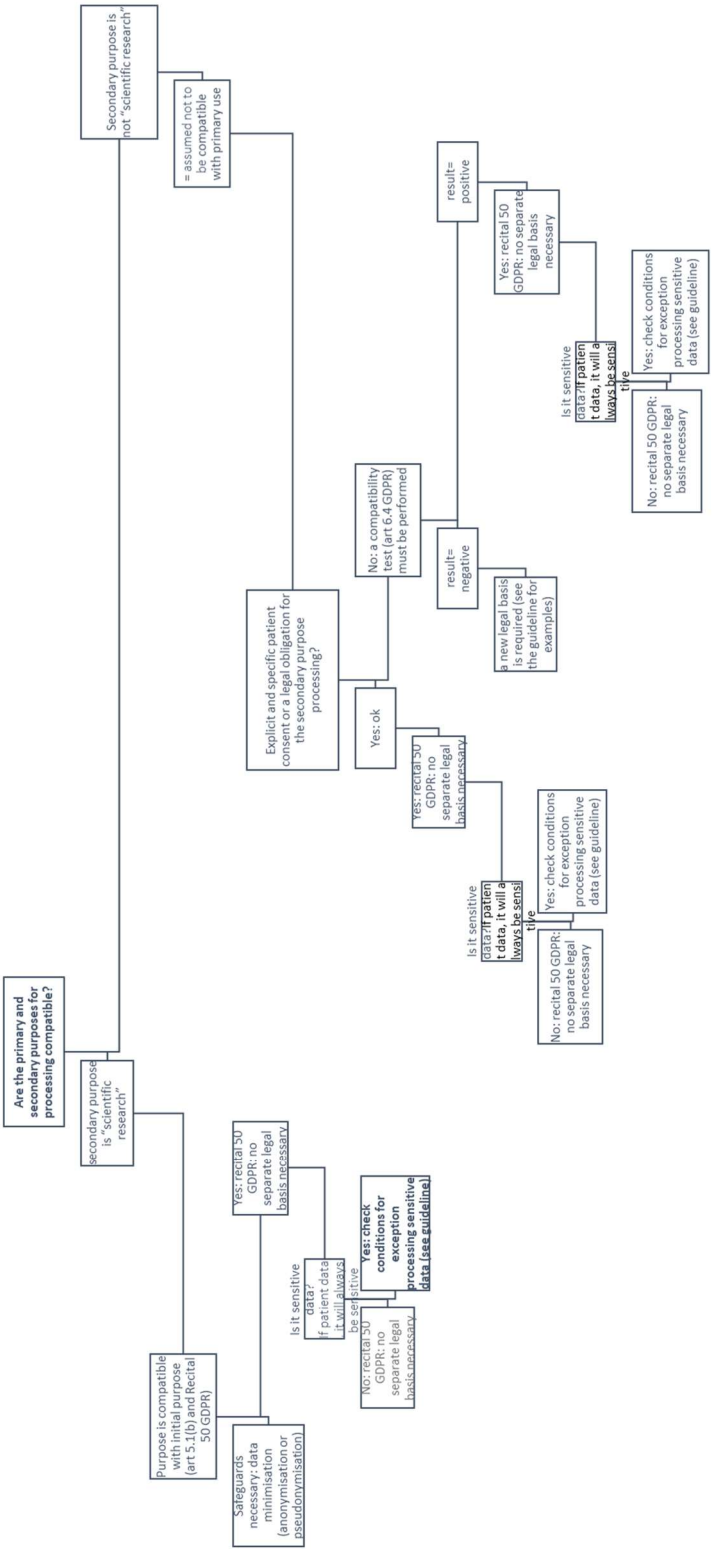
Go to steps 3 and 4

Step 3 and 4: Purpose limitation, legal basis and processing of sensitive data



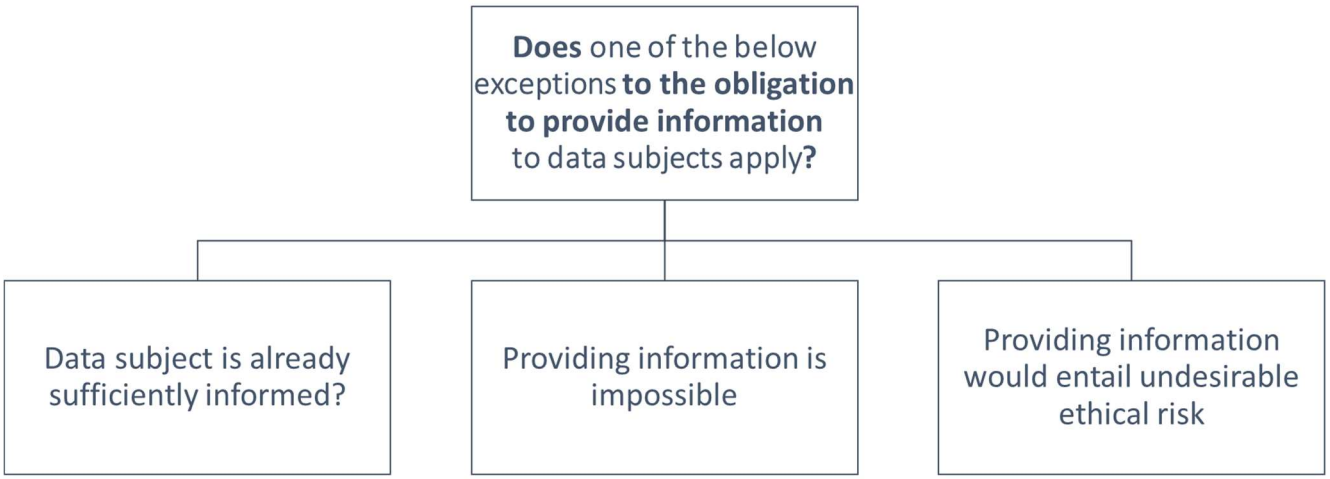
Step 4: legal basis and processing of sensitive data




Are the primary and secondary purposes for processing compatible?
secondary purpose is "scientific research"
Purpose is compatible with initial purpose (art 5.1(b) and Recital 50 GDPR)
Safeguards necessary: data minimisation (anonymisation or pseudonymisation)
Yes: recital 50 GDPR: no separate legal basis necessary
Is it sensitive data? If patient data it will always be sensitive
Yes: check conditions for exception processing sensitive data (see guideline)
No: recital 50 GDPR: no separate legal basis necessary
Secondary purpose is not "scientific research"
= assumed not to be compatible with primary use
Explicit and specific patient consent or a legal obligation for the secondary purpose processing?
Yes: ok
Yes: recital 50 GDPR: no separate legal basis necessary
Is it sensitive data? If patient data it will always be sensitive
Yes: check conditions for exception processing sensitive data (see guideline)
No: recital 50 GDPR: no separate legal basis necessary
No: a compatibility test (art 6.4 GDPR) must be performed
result= negative
a new legal basis is required (see the guideline for examples)
result= positive
Yes: recital 50 GDPR: no separate legal basis necessary
Is it sensitive data? If patient data it will always be sensitive
Yes: check conditions for exception processing sensitive data (see guideline)
No: recital 50 GDPR: no separate legal basis necessary

Go to step 5

Step 5: Transparency



See guideline for best practices of information to data subject