Mission creep / data misuse

Introduction

Data misuse, also known as mission creep, in the context of this research pathway entry - goes to the core of (mis)using a patient's personal health data, beyond the purpose(s) for which it was collected. Whilst it may sometimes be closely related to function creep, a very well-known phenomenon in the field of science and technology studies (describing an instance where systems or technologies expand beyond their initial scope of deployment) - mission creep or data misuse is more focused on the legitimacy and purposes for which patient data is collected, used, stored, and processed.

The findings of a Special EuroBarometer on Data Protection demonstrated that citizens were often worried about how they could control their own data. Hence, European Union (EU) law establishes the relevant legislation to ensure the proper use and protection of patients' rights to privacy when their relevant health data is collected and processed. This is in addition to the Charter of Fundamental Rights of the European Union. Addressing patients' concerns regarding privacy, data sharing and accessing their own health data, is necessary in a healthcare context (including care given through eHealth or mHealth), or in a cross-border healthcare context, and research (clinical trials, clinical investigations, epidemiological research, patient registries, etc).

In the context of patients' genetic data, this may also fall under the category of "sensitive data" which may be given additional protection under EU law. Hence, this engages the core principles for which EU law legislation was enacted, in

order to ensure that data misuse or mission creep does not happen.

For the purposes of this entry, the key relevant EU legislation is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR); and the Proposal for the Regulation of a European Health Data Space (EHDS).

Stakeholders

Data controllers: any natural (human person) or legal persons (non-human person) that determines which data will be processed, for which purpose and using which means. (Article 4(7) GDPR)

Data processors: any natural or legal person that processes personal data on behalf of the controller. Data processors do not always exist, as the controller itself may be responsible for all these tasks. (Article 4(8) GDPR)

Data subjects: any persons whose data is being collected and whose data is about. In the context of healthcare and health research, patients and research participants are data subjects because their personal health or genetic data are being processed for healthcare or research purposes.

Data Protection Authorities: The European Data Protection Board (EDPB), an independent European body established by the GDPR, and contributes to consistent application of data protection rules throughout the EU.

The European Commission and the European Free Trade Association (EFTA) Surveillance Authority also participate in

activites and meetings of the EDPB without voting rights.

Member States' (MS) Digital Health Authorities, pursuant to the European Health Data Space (also known as "Supervisory authority" in accordance with the Art. 51 GDPR), are also appointed to participate in cross-border digital infrastructure to support patients' sharing their data across borders (Art.22 EHDS Proposal for a Regulation).

The role and participation of the European Union Agency for Fundamental Rights is also envisaged with regards specifically for persons with disabilities. Where persons with disabilities are patients in the context of healthcare, the agency helps to ensure the safeguarding of their data, privacy and matters, including in relation to new technologies.

Patient organisations: These may include independent European organisations, such as the European Patients' Forum, European Hospital and Healthcare Federation, European Public Health Association, etc. that are non-profit organisations working in healthcare areas to champion patients' rights in various ways and forms.

With the establishment of the EHDS, it is also pertinent to note new categories of stakeholders that will be defined at the legislative level, especially within the healthcare context, as follows:

Data recipient: any natural or legal person that receives data from another controller in the context of the primary use of electronic health data. (Article 2(2)(k) EHDS Proposal for a Regulation)

Data holder: any natural or legal person operating in the healthcare domain (as a healthcare provider, researcher, developer of AI medical tools, entity or institution in charge of monitoring the activity of another player), that has the electronic health data under its control, to be transmitted to data recipients for primary uses of those data, or data users of

the referred data. (Article 2(2)(y) EHDS Proposal for a Regulation)

Data user: any natural or legal person who has lawful access to electronic health data for secondary use. (Article 2(2)(z) EHDS Proposal for a Regulation)

Health data access bodies: administrative authorities to be created in the Member States to perform the tasks listed in Article 27 of the EHDS Proposal for a Regulation, namely, to issue the data permit that will allow data users to have access to electronic health data for secondary purposes, arguably in a transparent, simplified, and secure way. When that happens, the health data access bodies and the data users will be both data controllers (joint controllers).

Definitions

The term **"mission creep"** has its origins in military operations. In Science and Technology Studies, the term used is "gradual function expansion" or "function creep", to indicate that a system or technologies expand beyond their original purposes, or acquire new uses for which it was not originally intended. In the context of patient involvement and patient data, "mission creep" has been used to also denote **"data misuse"**, since, in the scope of healthcare and medicine, patients' data are collected and used in a particular way, for limited purposes, and (ideally) with the patients' informed consent.

In the Charter of Fundamental Rights of the European Union, Article 8 specifically provides for the Protection of Personal Data, where "Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

Relationally to the GDPR, neither the terms “mission creep” nor “data misuse” appear -although the wordings used in the GDPR, and its incumbent provisions, makes clear that this is what is intended to be captured. (Recital 88 is the only provision in the GDPR which uses the word “misuse”). Nevertheless, the purpose of the GDPR is to regulate the “processing of personal data and rules relating to the free movement of personal data” (Article 1(1) GDPR). Specific rights are given to, or obligations are imposed on “data subjects” (Chapter 3, Arts. 12 - 23), “Controller and Processor”, “Data Protection Officer” and “third party” (Chapter 4, Arts. 24 - 43), “third countries or international organisations” (Chapter 5, Arts. 44 - 50), and “independent supervisory authorities” (Chapter 6, Arts. 51 - 59).

Data Subjects - Data subjects under the GDPR have a variety of rights regarding their personal data pursuant to Arts. 15 - 21. And whilst “mission creep” or “data misuse” is not specifically mentioned, the confines under which the personal data is processed appears to be controlled vis-a-vis the “purposes of the processing”, “the legal basis for the processing”, and “the legitimate interests pursued by the controller or third party”. (Art. 13(1) GDPR)

Controller and Processor, **Data Protection Officer** and **third party** - Controllers are tasked to “determine the purposes and means of the processing of personal data”. Processors process the personal data, as do third parties, and the Data Protection Officer is tasked with data protection. (Chapter 4, GDPR). Again, there is no mention of “mission creep” or “data misuse” but the obligation can be drawn from the definition of personal data breach as well.

“Personal data breach” (Art. 4 GDPR) is defined as a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. A personal data breach, when it happens, is a common indication that there has been data misuse or mission creep in some form or other.

Third countries or international organisations - Art. 44 GDPR broadly deals with transfers to third countries or international organisations, and the same obligations of data protection also apply to these entities in third countries or international organisations.

Challenges

With transparency, accountability, and audit being the operative principles of the GDPR, the challenges that are presented for patient involvement and patient data in the healthcare dimension, especially in ensuring that mission creep, or data misuse does not happen - are as follows :

1. Explicit informed consent and justification – because of the sensitive nature of personal information, patients need to be fully informed and explicitly consent to disclosure of their personal information. Healthcare and medical professionals must obtain explicit informed consent from the patient for each occasion which the data might be used. This can affect smooth operations, flexibility and efficiency.

2. Supply chain compliance – compliance is essential in every stage of the life cycle of healthcare supply chain. If compliance is unsatisfactory, or cannot be proved, this can disrupt the healthcare supply chain and cause increased costs and burdens.

3. Risks of unauthorised disclosure – where patient data needs to be shared with others, the risk of unauthorised disclosure can arise, and the patient's privacy could be affected if specific data can be viewed. This risk, for example, is also something that needs to be guarded against with wider patient data sharing pursuant to the European Health Data Space.

4. Security issues – with wider patient data sharing, security risks can also increase if systems that protect the data are

not updated (for example).

5. Conformity pressures – where all healthcare institutions are concerned with the processing of patient data, institutions where there is staff shortage (as an example), or whom are unable to appoint a qualified Data Protection Officer, are at risk of non-compliance due to conformity pressures.

Opportunities and incentives

The GDPR contains extensive provisions regarding the processing of personal data, under which patient data is also captured. The various stakeholders involved in data processing have specific ogligations imposed upon them under the GDPR, particularly obligations to obtain informed consent from patients. It is expected that, because of these extensive provisions, personal data breaches, mission creep, or data misuse, would result in the event these specific provisions are not complied with.

In addition to the GDPR, the EHDS, which is the latest initiative of the EDPB and European Data Protection Supervisor (EDPS), encourages data sharing in a common space, involving safe and secure exchange, use and reuse of health data. The EHDS expands the use of electronic health data to deliver health care to the individual from whom those data were collected (primary use) and to improve research, innovation, policy making, patient safety, personalised medicine, official statistics or regulatory activities (secondary use). Nevertheless, there is limited consideration of data misuse or mission creep in the EHDS.

Interactions with regulators

Interactions with regulators are specifically captured in the provisions of both the GDPR and the EHDS. Besides the

overarching role of the EDPB, Chapter 6 GDPR captures the role of the independent supervisory authority, which is one or more public authorities in each Member State tasked with monitoring the effective application of the GDPR. These independent supervisory authority are the first national point of contact for data controllers or data processors, etc (Art. 57 GDPR). Amongst others, the tasks of the independent supervisor authority is to "handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80 and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary" (Art. 57(1)(f) GDPR). This is likely the closest iteration of what mission creep or data misuse might entail, where interactions with regulators then become necessary.

Under the EHDS, in addition to the overall role of the EDPB and EDPS, interactions with regulators would involve connections with the individual Member States' Digital Health Authority (Art. 22 EHDS Proposal for a Regulation). There is some overlap in the role of the latter, with the role of the independent Supervisory Authorities under the GDPR (Art. 51). The specific details of tasks, responsibilities, and powers of the Member States Digital Health Authorities and the Supervisory Authorities can be found in, respectively, in Arts. 22 to 26 of the EHDS Proposal for a Regulation; and Arts. 51 to 58 of the GDPR. Their organisation as distinct authorities or as a unique national authority will depend on each Member State.

Practical steps

Principles of the GDPR – Article 5

There are six key principles in the GDPR to be followed by all data controllers in respect of data processing. This applies to patient data as well. The five principles for data processing are below, and must be strictly followed by data controllers to

avoid data misuse or mission creep, and “purpose limitation” is especially relevant.

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (“purpose limitation”);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate

technical or organisational measures (“integrity and confidentiality”).

Definitions of patient data – Article 4(13) and 4(15) ; and circumstances where patient data can be processed or shared – Article 9

Complying with the GDPR’s specification on circumstances when patient data can be processed is necessary to ensure there is no data misuse or mission creep. In the GDPR, patient data may be regarded as sensitive data . This encompasses “data concerning health” in Article 4(15) (defined as “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”) ; as well as “genetic data” in Article 4(13) (defined as “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question”). It is forbidden to process (including to share) this patient data except in limited circumstances.

The limited circumstances in which patient data may be processed or shared is under Article 9 GDPR (paragraphs 1 and 2), as follows :

- Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.
- Paragraph 1 shall not apply if one of the following applies:

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Critical knowledge of patients' rights under the GDPR

A critical knowledge of the rights given to patients under the GDPR is essential, so as to ensure at all times that patients are fully informed about not only their rights in healthcare, but their available rights to the protection of their own data under the GDPR. When so requested by patients accordingly, the data controller must comply with the patients' request. The main rights of patients under the GDPR are as follows (European Patients Forum, n.d.):

Patients' Rights	**Article No.**	**Summary of the Article**
Conditions for Consent	7	Patients shall have the right to provide their consent, or withdraw such consent to their data being processed, at any time whatsoever. In the event that consent is sought from patients for data processing, it shall only be for the lawful processing purposes specifically

Patients' Rights	Article No.	Summary of the Article
		stipulated in Article 6 para (1). (Note: withdrawal of a patient's consent shall not affect any lawful processing that has taken place based on earlier consent, prior to the withdrawal).
To be informed / transparency	13 and 14	Data controllers have an obligation to provide information to patients, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. At the time of collecting the health data, the data controller must provide the following information: 1. identity of the contact person or controller, 2. the purpose for which the data is processed, 3. the period for which the data will be stored, 4. if the data is intended to be transferred in another country, 5. if the data will be processed other than for the original purpose, 6. the patient's rights as a data subject.
Access to own	15	One of the fundamental rights in data protection is the patient's right to access their own

Patients' Rights	Article No.	Summary of the Article
personal data		personal data. Upon request, all data controllers must provide this information to the patient.
Rectification	16	A patient may ask for the rectification of inaccurate personal data and/or for incomplete data to be duly completed.
Erasure (right to be forgotten)	17	A patient has the right to have their data erased, especially where their consent has been withdrawn and the data controller no longer has any legitimate purposes for processing the data.
Data portability / transfer to another data controller	20	Where patients have consented to providing their health data, they may request for a copy to be received for purposes of transferring it to another data controller. Patients may also request that such data be transferred directly on their behalf and data controllers must do so.
Objection to data processing	21	Under Article 21(1), even if a patient has provided their consent to data processing, a patient still retains the right to object, on grounds relating to their personal situation, at ANY time of processing of personal data concerning them that are based on Article 6(1) para (e) or

Patients' Rights	Article No.	Summary of the Article
		(f), including profiling based on these articles. [Note: the right to object is independent of the definition of what amounts to lawful processing under Article 6(1)]. The patient's right to object also extends to: • If the processing happens in the context of direct marketing, including profiling of the patient for direct marketing purposes (Article 21(2)). • If the processing happens for scientific/historical/statistical research pursuant to Article 89(1) – unless the processing is necessary for the performance of a task carried out for reasons of public interest (Article 21(6)).
Not to be subject to automated individual decision-making, including profiling	22	A patient has the right not to be subject to a decision based solely on automated processing, including profiling, whereby such decision produces legal effects concerning them, or significantly affects them unless: • It is necessary for entering into/performance of a

Patients' Rights	Article No.	Summary of the Article
		contract between the patient and a data controller, • Authorised by Union/Member States law to which the controller is subject and which has safeguards for data subject's rights, freedoms, and legitimate interests, • Is based on the patient's explicit consent.
Breach	34	If there is a security breach and patients' personal data is unduly disclosed, accessed, or destroyed, the data controller must inform the patient about the breach if it is a threat to patients' rights or freedoms. Data controllers must also inform the national supervisory authorities of such breach and take specific measures to protect the data.

European Union Legislation

Charter of Fundamental Rights of the European Union (2012/C 326/02), OJ C 326, 26.10.2012, p. 391-407, CELEX number: 12012P/TXT

- Original text (available in the 24 official languages of the EU)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 **on the protection of natural**

persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1-88, CELEX number: 32016R0679

- Original text (available in the 24 official languages of the EU)
- Current version with last amendments (available in the 24 official languages of the EU)
- Document summary (available in the 24 official languages of the EU)

Proposal for a Regulation of the European Parliament and of the Council **on the European Health Data Space**, 3 May 2022, COM/2022/197 final, CELEX number: 52022PC0197

- Original text (available in the 24 official languages of the EU)

European Union Guidance

- EDPB Document on response to the request from the European Commission for clarification on the consistent application of the GDPR, focusing on health research, European Data Protection Board (EDPB), 2 February 2021
- Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725)
- EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI)
- Guidelines 01/2022 on data subject rights - Right of access

Relevant literature

- Purpose Limitation By Design as A Counter to Function Creep and System Insecurity in Police AI
  - Scientific abstract

- The new EU Regulation on the protection of personal data: what does it mean for patients?
- Stop the Creep of Biometric Surveillance Technology
- Research Handbook on EU Data Protection Law
  - Scientific abstract

- Transparency of Machine-Learning in Healthcare: The GDPR & European Health Law
- Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate
- The EU General Data Protection Regulation (GDPR): A Practical Guide
  - Scientific abstract

- Purpose and Function Creep by Design: Transforming the Face of Surveillance through the Internet of Things
  - Scientific abstract

- The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation

Acknowledgements

Published: 19/06/2023

Author:

Pin Lean Lau, Assistant Professor in Bio-Law, Brunel Law School, Brunel University London

Reviewed by **Aurélie Mahalatchimy**, EuroGCT WP4 Convenor, UMR 7318 DICE CERIC, Aix-Marseille University, CNRS, Aix-en-Provence- France

Data sharing / Open data

Research Pathways

Research and Innovation

Therapy Classification

Manufacturing

Commercialisation

Actors and Networks

Public Involvement and Data

- Data protection
- Data collection, processing, controlling
- Data sharing / Open data
- Mission creep / data misuse

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 965241.