ISW

In Silico World: Lowering barriers to ubiquitous adoption of In Silico Trials

Grant Agreement No. 101016503

D9.2 **In-depth analysis of legal and ethical requirements**

Deliverable information	
WP number and title	WP9 Legal and Ethical Framework
Lead beneficiary	KU Leuven Centre for IT & IP Law (KUL-CTP)
Dissemination level	Public
Due date	30 April 2023
Actual date of delivery	27 April 2023
Author	KU Leuven Centre for IT & IP Law (KUL-CTP)
Contributors	University of Bologna (UNIBO)

The following document reflects only the author's view. The Agency is not responsible for any use that may be made of the information it contains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101016503

Quality assurance

To ensure the quality and correctness of this deliverable, we implied an internal review and validation process. The deliverable was drafted by the work package leader KUL-CTP. All partners contributed to and reviewed the overall draft. Finally, the semi-final version was submitted to internal reviewers, for a final review and validation.

Version	Date	Status	Author	
0.1	19/10/2022	Table of Contents	E. Biasin (KUL-CTP)	Input ToC
0.2	27/03/2023	First User Story	E. Biasin (KUL-CTP)	Submission of the deliverable first draft as first user story for D9.2
0.3	06/04/2023	KUL-CTP Internal Review	E. Biasin (KUL-CTP)	Submission of the finalised version of the deliverable for internal review
0.4	14/04/2023	KUL-CTP Review	Dr. Ana Maria Correa Harcus (KUL-CTP)	Feedback from internal review
0.5	17/04/2023	Second User Story	E. Biasin (KUL-CTP)	Submission of the deliverable in its finalized version for the partners' review
0.6	22/04/2023	Partner's Review	John Wilkinson (Advisory Board)	Deliverable review (#1)
0.7	24/04/2023	Partner's Review	Benjamin Csippa (BME)	Deliverable review (#2)
0.6	25/04/2023	UNIBO Feedback	Prof. dr. Marco Viceconti (UNIBO)	Feedback and input to sections 4.2.2 - 4.3.3
1.0	27/04/2023	Final Version	UNIBO	Submission to the EC Portal

Table of contents

Executive Summary

The present Deliverable, '**D9.2** – **In-depth analysis of legal and ethical requirements',** part of Work Package 9 'Ethical and Legal Framework' (WP9) of the In Silico World project assesses the **core pieces of legislation and ethical principles** identified in Deliverable 'D9.1 – Legal and Ethical Inventory'. The report analyses the following areas of legislation – and identifies some key issues – **relevant for the In Silico World project** and, thus, for ***in silico* trials**:

- **Privacy and Data Protection:** Data protection is a long-established legislation in the European Union (EU), which has evolved throughout the last decades, and the GDPR is the fundamental EU law to consider for *in silico* trials. Hence, the report introduces the principles of data processing, the notion of personal data and health data and the legal bases for data processing. *In silico* trials may highlight some of the common challenges for the healthcare sector in data protection. These include the legal bases and the further processing of health data. *In silico* trials may also raise interpretative questions. These include doctrinal discussions about the nature of synthetic data in their relationship with anonymization and pseudonymisation, and the concept of data ownership.

- **Data Governance:** The legal landscape concerning health data sharing is changing due to a series of new EU legislative initiatives. These initiatives encompass the Data Governance Act, the European Health Data Space (EHDS) proposal, and the Data Act proposal. The Data Governance Act sets rules for re-using certain categories of personal data and introduces the concept of data altruism in healthcare. The EHDS proposal regulates, *inter alia,* the primary and secondary use of health data. The Data Act proposal proposes business-to-consumer, business-to-business and business-to-government data sharing rules. These three pieces of legislation are expected to apply simultaneously, once all approved. Nevertheless, some challenges may arise in the future, which may concern the appropriate legal basis for data sharing and data altruism, and the interaction of these with the GDPR and national legislation.

- **Clinical Trials, Medicinal Products and Medical Devices:** Clinical trials, medicinal products and medical device legislation are relevant to the very essence of *in silico* trials. For clinical trials and medicinal products, Regulation 726/2004 provides the legal basis for the EMA to deal with novel methodologies for drug development. The Medical Device Regulation (MDR) and In Vitro Medical Device Regulation (IVDR) are the applicable laws for medical device legislation and explicitly mention modelling and simulation. However, while these laws do not prohibit *in silico* trials, they do not extensively address them either. There exist challenges and barriers that need to be addressed both on a regulatory and legislative perspective. On the regulatory side, guidance and standardisation efforts are needed in general (to tackle, for example, Artificial Intelligence (AI)) and in particular (on the verification and validation of *in silico* models). On the legislative side, there is common agreement that the current pharmaceutical legal framework lacks behind digital innovation processes. The EU Pharmaceutical Strategy promises the reform of the existing pharmaceutical framework. It is desirable that the reform will address more comprehensively innovative aspects for the medicinal product's lifecycle, including *in silico* trials.

- **Artificial Intelligence:** The legal framework of AI is in the process of being established in the EU. The AI Act proposal, expected to be approved in 2023, will introduce new requirements for providers, users and all the actors involved in AI systems. These include, *inter alia,* adopting a risk management system, a quality management system, documentation duties, ensuring transparency, human oversight, accuracy, robustness, and cybersecurity. The AI Act will be relevant for medical devices and in vitro diagnostic medical devices, as – according to the latest available version of the proposal – they

are explicitly included in the scope of the regulation. The regulation sparked several discussions that this report cannot summarise comprehensively. Therefore, the report chooses a new item currently negotiated in the latest proposal's version may be of crucial relevance for medicine and healthcare: the potential non-application of AI rules in the context of scientific research. The preliminary conclusion is that these rules, as currently formulated, may generate legal uncertainties in the future.

The report concludes with a section on the 'Ethics Principles'. The section is based on the **Biomedical Ethics principles** that were illustrated in D9.1, i.e. **autonomy, justice, beneficence, and non-maleficence**. The report offers some examples (patients' self-determination for autonomy; incidental findings for beneficence; safety and security risks for non-maleficence; patients' representativeness for justice) to show how these principles could guide stakeholders to ensure the protection and advancement of human values in the context of *in silico* trials.

1. Introduction

1.1. Objectives

This deliverable is based on the formerly Deliverable 'D9.1 – Ethical and legal inventory of in silico trials' and has a twofold objective.[1] First, it offers an **in-depth analysis** of core **legal aspects** deemed **crucial for the uptake of *in silico* trials in the EU**. Second, the deliverable analyses the previously identified fundamental ethical principles and suggests their relevance in the realm of *in silico* trials through practical application examples.[2]

1.2. Document outline

To achieve the above objectives, the deliverable is divided into six main sections, following the main categorisations identified in D9.1. Section 2, '**Privacy and Data Protection**', analyses with more detail the existing data protection legislation in light of the most recurrent issues in *in silico* trials and medical research in general. Notably, it contextualises the meaning of personal and health data, which are analysed against the arising questions about synthetic data. Section 3, '**Data Governance'**, provides a descriptive overview of the Data Governance Act[3], which introduced the concept of data altruism for sharing health data. It studies the recently proposed European Health Data Space (EHDS),[4] which will be crucial in the future for the healthcare sector as it disciplines the primary and secondary use of health data. A third part of the section is dedicated to the Data Act proposal[5], which concerns business-to-consumer, business-to-business, business-to-government data sharing. Section 4 '**Clinical Trials, Medicinal Products and Medical Devices,**' condensates the main references of law that may be relevant to in *silico* trials for medicinal products and medical devices, ending with some initial remarks about the possible avenues for *in silico* trials in that regard. The report then illustrates the most recent developments and open discussions concerning the AI Act proposal[6] and artificial intelligence regulation in Section 5, '**Artificial Intelligence**'. Finally, section 6, '**Ethics Principles**', builds from the biomedical ethics principles mentioned in D9.1 and further explores them as a possible way of guidance for *in silico* trials.

[1] See Elisabetta Biasin, 'In Silico World D9.1 Legal and Ethical Inventory' <https://zenodo.org/record/7104079> accessed 10 January 2023.

[2] ibid, section 7 'Ethics principles'.

[3] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1.

[4] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' COM(2022) 197 final (European Health Data Space proposal).

[5] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM(2022) 68 final.

[6] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM(2021) 206 final.

2. Privacy and Data Protection

2.1.Selected aspects of data protection for in silico trials

2.1.1. Subject matter and material scope of the GDPR

Regulation 2016/679 (also known and General Data Protection Regulation or GDPR)[7] is a directly applicable piece of legislation that lays down rules relating to the **protection of natural persons concerning the processing of personal data** and rules relating to the free movement of personal data.[8] Its objective is to protect the fundamental rights and freedoms of natural persons, particularly their right to the protection of personal data.[9] As seen in ISW D9.1, the GDPR is not the first EU law regulating personal data processing.[10] Many more in the past set rules and principles that evolved throughout the history and became the principles that are known in the GDPR. Before the GDPR, the common piece of legislation in the EU was the Data Protection Directive (DPD), whose aim was to harmonise data protection rules throughout the EU.[11] In 2009, the DPD underwent a review process which culminated in the adoption of the GDPR in 2016.

The GDPR applies to personal data, meaning that non-personal data and pieces of information not falling under the definition of personal data[12] will not be covered by this Regulation's rules. As per Recital 26 GDPR, the principles of data protection should not apply to anonymous information, which is information not relating to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable. Consequently, **anonymised data** fall outside the scope of the GDPR, including those processed for statistical or research purposes.[13] **Pseudonymised** data, on the contrary, are considered by the GDPR as personal data, and therefore it applies to them.[14] Data processing in the context of household activities remains outside the scope of the Regulation.[15]

2.1.2. Personal scope of application of the GDPR

The GDPR foresees rules on its **territorial scope**. Thus, the regulation applies to the processing of personal data of processors and controllers established in the EU (even if then processing takes place elsewhere).[16] If the controller or the processor is not established in the EU, the GDPR applies anyway when the processing activities relate to goods or services offered to data subjects in the EU or to monitoring their behaviour (inasmuch their behaviour takes place within the EU).[17] Territorial scope rules are relevant in healthcare

[7] 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) [2016] OJ L119/1 (GDPR).

[8] GDPR, art 1.

[9] ibid.

[10] Biasin, 'In Silico World D9.1 Legal and Ethical Inventory' (n 1).

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[12] See *infra,* section 2.1.4.

[13] GDPR, rec 26.

[14] In fact, as GDPR rec 26 states: 'personal data which have undergone pseudonymization which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person'.

[15] GDPR, art 2.

[16] GDPR, art 3(1).

[17] GDPR, art 3(2).

settings. For example, a health device manufacturer established in the United States (US) monitors the behaviour of some individuals in the EU. This case might imply the application of the GDPR and its rules – including those on international data transfers and appointment of a representative in the Union.[18]

The personal scope envisaged by the GDPR entails the interaction of different legal or natural persons. The most relevant include **controllers, processors,** and **data subjects.** In data protection, the controller is usually defined as the natural and legal person that determines – alone or jointly with others – *the means* and the *purposes* of the processing.[19] The processor is defined as the natural or legal person data process the person's data on behalf of the controller. The data subject is the individual, the natural person to whom the processed information relates.[20] In healthcare settings, a hospital could be the controller of the patient's personal data for the provision of their services. The patients would constitute the data subjects because the hospital processed their data to provide its healthcare service. For controllers, sometimes is complicated to ascertain whether they should be considered processors or joint controllers. For example, some argued that certain manufacturers or device producers should be considered controllers for health devices.[21] Jurisprudence and data protection guidance have offered new elements to consider throughout these years.[22]

2.1.3. Data processing principles and their relevance to healthcare

The principles of data protection are core aspects for data processing activities, also in the field of in silico trials. When personal data are processed, several aspects and requirements need to be taken into account, which often are linked to the data processing principles. The GDPR includes five principles to regard at when executing the processing of personal data. These are enlisted in Article 5 of the GDPR.

The first principles are **lawfulness, fairness and transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This principle has implications in several requirements of the GDPR. Lawfulness means that the processing of personal data may only take place if based on a lawful ground. Other provisions of the GDPR further declinate the legal bases of processing activities, such as Articles 6 and 9 GDPR. A notable example of legal basis is consent, which in health research is a multi-faceted issue (see *infra,* section 2.1.8). Fairness governs the relationship between the controller and the data subject. It requires the controller to treat data in a manner that the individual would reasonably expect. As a principle, it has several implications, one of which is meant to mitigate the imbalances of power between the controller and the data subject.[23] Transparency is correlated to the information duties that the controller has vis-à-vis the data subjects. It entails an obligation for the controller to take adequate measures to inform data subjects about the processing of their personal data. These include, for example, informing patients of the

[18] See GDPR, Chapter V and art 27 GDPR, respectively.

[19] GDPR, art 4(7). There is EU-level guidance extensively illustrating the notion of controller (and processor). See European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en>.

[20] GDPR, art 4(1).

[21] Alan Dahi and Marcelo Corrales Compagnucci, 'Device Manufacturers as Controllers – Expanding the Concept of "Controllership" in the GDPR' (2022) 47 Computer Law & Security Review 105762.

[22] Charlotte Ducuing and Jessica Schroers, 'The Recent Case Law of the CJEU on (Joint) Controllership: Have We Lost the Purpose of "Purpose"?' (2020) 2020 Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht; Brendan Van Alsenoy, 'Regulating Data Protection: The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing' (2016). Case law include: Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629; Case -25/17 *Tietosuojavaltuutettu intervening parties: Jehovan todistajat — uskonnollinen yhdyskunta*, [2018] ECLI:EU:C:2018:551.

[23] Every principle would deserve a broad illustration on its own and in its interactions. This section summarises some of the many aspects for reasons of space, scope and utility. For a comprehensive analysis on the fairness principle, eg, see Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130.

processing of their personal data when they check-in in a hospital, or when the data concerning them are used in scientific research.

The second principle is **purpose limitation.**[24] Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The principle is particularly relevant when it comes to scientific research. In the case of scientific research, the GDPR specifies that the purpose of further processing of personal data shall not considered to be incompatible with the initial purpose, provided that safeguards and specific conditions are respected.[25]

Data minimisation is the third principle of data processing. It aims to create patient empowerment through obligations for others.[26] The data minimisation principle requires that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[27] In simple terms, it means that the controller should not process 'too much personal data', having regard to the purpose of the processing activities and that data controllers always have to consider alternatives that are less invasive in terms of privacy. In scientific research, the further processing of data is possible if there are appropriate safeguards and technical and organisational measures are in place to ensure respect for the principle of data minimisation.[28]

The principle of **accuracy** requires that data shall be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay, having regard to the purposes for which they are processed.[29] In healthcare, if data used in profiling and automated decision making is inaccurate, the resultant decisions of the profile may be flawed.[30] Moreover, inaccurate data processing might lead to inappropriate predictions or statements about someone's health. Therefore, adjusting inaccuracies of personal data or minimising risks of errors may prevent discriminatory effects on natural persons. Moreover, ensuring the accuracy of personal data may favour the correct performance of health technologies, including those involved in *in silico* trials.[31]

Storage limitation is a principle that requires data to be 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. For scientific research, personal data may be stored for longer periods, insofar specific conditions are applied – i.e. appropriate technical and organisational measures are in place to safeguard the rights and freedoms of the data subject. Usually, implementing the storage limitation principle implies the consideration of data retention policies for the processing of personal data for a given purpose, or adhering to those already identified by the law, if any.

Integrity and confidentiality is the principle mandating the processing of personal data 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

[24] GDPR, art 5(1)(b).

[25] See GDPR, art 89. To be noted that art 89(2-4) leaves room for derogations at the national level. For a comprehensive analysis on the principle of purpose limitation in healthcare, see Griet Verhenneman, 'The Patient's Right to Privacy and Autonomy against a Changing Healthcare Model' (KU Leuven Faculteit Rechtsgeleerdheid 2020).

[26] ibid 173.

[27] GDPR, art 5(1)(c).

[28] GDPR, art 89(1).

[29] GDPR, art 5(1)(e).

[30] WP29, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679'.

[31] Elisabetta Biasin, 'Why Accuracy Needs Further Exploration in Data Protection', *Proceedings of the 1st International Conference on AI for People: Towards Sustainable AI, CAIP 2021, 20-24 November 2021, Bologna, Italy* (EAI 2021) <http://eudl.eu/doi/10.4108/eai.20-11-2021.2314205> accessed 22 January 2023.

measures.[32] Following this principle entails adopting security measures, which may encompass for instance the execution of a Data Protection Impact Assessment (DPIA)[33] before the start of certain data processing activities, setting up procedures for tackling data breaches to limit the risks posed to data subjects.[34] In healthcare, ensuring security of personal data is pivotal to help protecting the patient again certain threats. It may help maintaining the integrity of data and reducing risks for patients over harms of discrimination or stigmatisation for their condition (see also *infra,* section 6.1.1 for its link with the Non-maleficence principle).[35]

Article 5 of the GDPR closes the list of the data processing principles with **accountability**. Accountability is the grounding principle of the GDPR. It requires the controller to adhere and demonstrate compliance to the Regulation and the above principles. Accountability in the context of *in silico* trials may translate, for example, in carrying out the necessary evaluations about consent and ethical procedures for starting clinical research activities entailing the use of personal data.

2.1.4. Data in the scope of application (healthcare focus): personal data

The scope of application of the GDPR is limited to what is considered **personal data**.[36] The GDPR defines personal data as any information relating to an **identified or identifiable natural person**. A natural person may be considered as identifiable if they can be identified, directly or indirectly – by reference to an identifier such as a name, an identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[37] Throughout the years, EU institutions and case law have provided several pointers to further ascertain what can be considered personal data.

In its liminal Opinion 4/2007 on the concept of personal data, the Article 29 Data Protection Working Party (WP29) offered guidance about it.[38] For example, they suggested considering three core aspects of the personal data definition: 1) the element '**any information**'; 2) the element '**relating to**'; 3) the element '**identified or identifiable natural person**'. The first element is very broad, and it includes objective and subjective data. The WP29 exemplifies that data on the results of a patient's medical test contained in their medical records clearly relate to the patient.[39] The third element is often a decisive one. A natural person can be considered as 'identified' when having regard to a group of people, they are distinguished from all other group members. A natural person can be considered 'identifiable' when, even if not identifiable, it is possible to do it in a direct or indirect manner. This may depend on the context of the processing of personal data and all the objective factors surrounding the specific processing of personal data taking place.

---

[32] GDPR, art 5(1)(f).

[33] GDPR, art 35.

[34] GDPR, arts 33-34.

[35] For more remarks about security and cybersecurity in healthcare, see Elisabetta Biasin and Erik Kamenjasevic, 'Cybersecurity of Medical Devices: Regulatory Challenges in the European Union' in Carmel Shachar and others (eds), *The Future of Medical Device Regulation: Innovation and Protection* (Cambridge University Press 2022) <https://www.cambridge.org/core/books/future-of-medical-device-regulation/cybersecurity-of-medical-devices/AC01289C2DB05E44D0D98A9E66666562>.

[36] It may seem a mere theoretical exercise to situate the legal definitions of personal data. In practice, however, these considerations have concrete effects. Most importantly, these imply knowing whether data should be deemed anonymized or pseudonymized – which implies, in essence, whether the GDPR is considered applicable in a given situation.

[37] GDPR, art 4(1).

[38] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data'.

[39] ibid 10.

Examples of the kind of information that may be considered personal data are, for example, a patient's full name, home address, date of birth, admission and discharge dates, clinical trial numbers, patient ID number, photos, videos, physical characteristics, email addresses, audio recordings.

2.1.5. Focus: special categories of personal data and health data

The GDPR considers certain categories of personal data to be more **sensitive** and, thus, worthy of a higher level of protection.[40] Article 9 GDPR identifies the 'special categories or personal data', which are: 'data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.[41]

The healthcare sphere is very personal, and it might entail the processing of several of the above special categories of personal data. The most prominent category within the healthcare domain is **data concerning health** (also called **health-related data**). These are defined in Article 4(15) of the GDPR as related to a natural person's physical or mental health, revealing information about their past, current or future health status. Personal data concerning health include information about the natural person collected in the course of the registration or provision of healthcare services; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; any information on a disease, disability, disease risk, medical history, clinical treatment, physiological or biomedical state of the data subject – independent of its source (e.g. a physician/ health professional, a hospital, a medical device or an in vitro diagnostic test).[42]

EU bodies have, on different occasions, attempted to reconduct some categories of personal data within the broader category of data concerning health. They are present in Council of Europe Recommendations, WP29 and European Data Protection Board (EDPB) opinions, guidelines and working documents, and European Data Protection Supervisor (EDPS) opinions. Also, the European Court of Human Rights (ECtHR) and the European Court of Justice (CJEU) interpreted the concept of health data.[43] In light of existing guidance and case law, the legal doctrine usually distinguishes between **data processed in the medical professional context** ('medical data') and processed outside the medical professional context.[44]

Medical data falls under the first category (data processed in the medical professional context). These are all information concerning a data subject's physical or mental health status that are generated in a professional medical context. It includes all data related to contacts with individuals and their diagnosis or treatment by providers of health services, any information related to diseases, disabilities, and history of an individual. Also, data generated by devices or apps in a professional medical context (irrespective of whether the technologies qualify as medical devices) may be considered medical data.[45]

What does not fall under the medical data falls under the category of **health data processed outside the medical professional context.** This broad category encompasses **data directly concerning the health of the individual.** This category concerns data that have a solid and close link to an individual's health. Examples from EU case law include the case of a woman with a broken leg who works half-time on a medical ground.[46] The

[40] See Article 29 Data Protection Working Party, 'Advice Paper on Special Categories of Data ("sensitive Data")'.

[41] GDPR, art 9(1).

[42] GDPR, rec 35.

[43] Z. v Finland, no. 22009/93, 25 January 1997; I. v Finland, no. 20511/03, 17 July 2008.

[44] From the many conceptualisation efforts in literature, see Verhenneman (n 25) 89.

[45] Article 29 Data Protection Working Party, 'Annex to Letter from the WP29 to the European Commission - Health Data in Apps and Devices' 2.

[46] CJEU, C-101/01, Criminal Proceedings against Bodil Lindqvist, 6 November 2013 (para. 51).

WP29 offered further examples, such as the fact that a person wears glasses or contact lenses, data about a personas intellectual and emotional capacity, information about smoking and drinking habits, data on allergies disclosed to private entities (e.g. airlines) or public bodies (e.g. schools); data on health conditions to be used in an emergency, membership of an individual in a patient support group, or the mere fact that somebody is ill in an employment context. All of these examples are considered as data concerning the health of individual data subjects.[47]

The second sub-category belonging to health data processed outside the medical professional context is **data not per se health-related, but that allows for health-related conclusions after processing.** In its guidance, the WP29 clarified what is often considered a grey area in health and care. In some instances, certain data that at first glance would not seem like data concerning health may nevertheless qualify as health data. Raw personal data, in fact, may change into health data if the dataset is used to **determine a person's health status**.[48] The WP29 exemplifies the following: a single registration of a person's weight, blood pressure, or pulse/heart rate. Without any further information about age or sex, it would likely not allow for the inference about the state of health of that individual. However, if this aspect is measured over time, in combination with age and sex, it may be used to determine aspects of an individual's health, such as health risks of high/low blood pressure etc. In that case, the data should be considered health data. Only if no conclusion can be reasonably drawn about the health status of a data subject, then they would not be regarded as health data (for example, raw data collected through a steps counter that does not combine those data with other data: they would be just raw personal data because one could not infer knowledge about that person's health).[49] Also, when the controller combines non-health data with health data to monitor health and wellbeing, all the collected data shall be qualified as health data. Ultimately, the **purpose of the processing** plays a role in the qualification of health data.[50]

These categorisations, therefore, are necessary and relevant for *in silico* trials. If an *in silico* technology is processing personal data – also in the form of pseudonymized data – to determine a person's health status, then even data that are not per se health related but allow for health-related conclusions after processing, then they should be qualified as health data. As section 2.1.8 ('Legal bases for the processing of personal data') will show, the distinction is not trivial because it implies the application of **different legal bases** for their processing.

2.1.6. Focus: genetic data

Genetic data are health data comprised under the definition of special categories of personal data and are a specific category of health-related data.[51] The GDPR defines **genetic data** as the 'personal data related 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

[47] Article 29 Data Protection Working Party, 'Annex to Letter from the WP29 to the European Commission - Health Data in Apps and Devices' (n 45) 2.

[48] ibid 4.

[49] ibid 3.

[50] See European Data Protection Supervisor, 'Mobile Health' <https://edps.europa.eu/sites/default/files/publication/15-05-21_mhealth_en_0.pdf>. For a critical analysis on the role of purpose with regard to the identification of health data, see Verhenneman (n 25) 98.

[51] Council of Europe, 'Recommendation CM/Rec2019(2). Protection of Health-Related Data' <https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html>.

sample from the natural person in question'.[52] They could include DNA, RNA analysis or personal data resulting from the analysis of another element enabling equivalent information to be obtained.[53]

Both for data concerning health and genetic data, the GDPR establishes that **Member States may maintain or introduce further conditions or limitations** with regard to the processing of genetic data and data concerning health.[54]

2.1.7. Focus: synthetic data

Besides the existing definition of data protection law, some stakeholders in the healthcare sector (and beyond) are increasingly using and thus referring to "synthetic data". Model training for *in silico* technologies often makes use of synthetic data. Synthetic data are a **core element of *in silico trials***.[55] They could also be in simulation studies to inform the clinical trial design as well as offer predictive statements for individuals and populations.[56] They may be relevant in different phases, such as model training, validation, or optimization of the *in silico* technology. Furthermore, studies maintain that using synthetic data to validate simulation and prediction models helps improve prediction accuracy and population representativeness.[57]

The **medical literature** highlighted the uses and benefits of synthetic data. Synthetic data are deemed helpful to accelerate methodological developments in medical research, to develop and validate methods for a particular task before accessing real data.[58] Within a context where it usually takes time to obtain "real" data, literature underlines that synthetic data may help save time.[59] Azizi and others pointed out, it is often difficult for researchers to access high-quality individual-level data for secondary purposes, given data protection requirements.[60]

EU **data protection** stakeholders have praised the positive effects of synthetic data. The OECD defined synthetic data as an approach to confidentiality'.[61] The EDPS itself noted that from the data protection by design approach, this technological aspect might provide an added value for individuals' privacy compared to the disclosure of the original data. However, both in the medical and data protection **literature**, there is an ongoing debate about the meaning of synthetic data and the consequences from a privacy and data protection point of view. More specifically, many considerations are around whether synthetic data constitute personal data.

---

[52] GDPR, art 2(13).

[53] GDPR, rec 34.

[54] GDPR, art 9(4).

[55] Aldren Gonzales, Guruprabha Guruswamy and Scott R Smith, 'Synthetic Data in Health Care: A Narrative Review' (2023) 2 PLOS Digital Health e0000082.

[56] ibid.

[57] Ahmed J Aljaaf and others, 'Partially Synthesised Dataset to Improve Prediction Accuracy' in De-Shuang Huang, Vitoantonio Bevilacqua and Prashan Premaratne (eds), *Intelligent Computing Theories and Application* (Springer International Publishing 2016).

[58] Theodora Kokosi and Katie Harron, 'Synthetic Data in Medical Research' (2022) 1 BMJ Medicine e000167.

[59] This because data access applications can be conducted in parallel or while waiting for data access granting. See ibid 2.

[60] Their study demonstrated that, in clinical studies, synthetic data can serve as a proxy for real data. Zahra Azizi and others, 'Can Synthetic Data Be a Proxy for Real Clinical Trial Data? A Validation Study' (2021) 11 BMJ Open e043497.

[61] See 'Is the Future of Privacy Synthetic? | European Data Protection Supervisor' (14 July 2021) <https://edps.europa.eu/press-publications/press-news/blog/future-privacy-synthetic> accessed 14 March 2023.

If one looks at the GDPR, they will not find a definition or specific rules concerning **synthetic data.**[62] Some mentions are present in a recital of the Data Governance Act. There, the use of synthetic data is mentioned as 'privacy preserving methods that could contribute to a more privacy-friendly processing of data'.[63]

The EDPS recently elaborated on the concept of synthetic data:

> "The concept of synthetic data generation is to take an original data source (dataset) and create new artificial data with similar statistical properties from it. Keeping the statistical properties means that anyone analysing the synthetic data, a data analyst for example, should be able to draw the same statistical conclusions from the analysis of a given dataset of synthetic data as he/she would if given the real (original) data".[64]

Identifying how synthetic data are generated may help understanding what is their nature from a privacy and data protection point of view. As El Emam explains, synthetic health data are generated from a model that is fit to a real data set.[65] Statistical machine learning and deep learning methods are used to fit this model. When the model is fit, it is used to generate new data from that model.[66] The generation is stochastic, a different data set is generated from the model each time.[67]

Some contributions in the literature distinguish three broad categories of synthetic data: fully synthetic, partially synthetic and hybrid.[68] According to Surendra and Mohan, **fully synthetic data** mean that data are completely synthetic and that do not contain original data. For **partially synthetic data,** the method used replaces only values of the selected sensitive attribute with synthetic values. The original values become replaced by synthetic values if there is a high risk of disclosure. **Hybrid synthetic data** are generated by using both original and synthetic data.

Beyond technical characterization, what matters from a data protection point of view is to what extent synthetic data fall within the definition of '**personal data**'. In order to ascertain whether this is the case it is necessary to come back again to the notion of personal data (illustrated *supra*) and the technical considerations that EU level bodies have offered in their guidance on **anonymization and pseudonymization**.[69] Both of the issues are a complex and debated issue in the legal doctrine.[70]

---

[62] Definitions of synthetic data are various: see Gonzales, Guruswamy and Smith (n 55) 3. Also, it is worth to note that study of synthetic data use is not new: see DB Rubin, 'Statistical Disclosure Limitation' (1993) 2 Journal of Official Statistics 461.

[63] DGA, rec 7.

[64] 'Is the Future of Privacy Synthetic? | European Data Protection Supervisor' (n 61).

[65] Khaled El Emam, 'Seven Ways to Evaluate the Utility of Synthetic Data' (2020) 18 IEEE Security & Privacy 56.

[66] ibid.

[67] ibid.

[68] H Surendra and HS Mohan, 'A Review of Synthetic Data Generation Methods For Privacy Preserving Data Publishing' (2017) 6 International Journal of Scientific & Technology Research.

[69] Anonymisation is understood as the process to make information not to 'relate to an identified or identifiable natural person' or 'personal data rendered anonymous in such a manner that the data subjects is not or no longer identifiable' (GDPR, rec 26). Pseudonymisation is defined as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person' (GDPR, art 4(5)).

[70] The core guidance about anonymisation is Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

Concerning the concept of personal data, there is no agreement on the interpretation about the scope of personal data. There exist two opposing views (*objective* vs *relative* criteria).[71] According to the objective criterion, data may be considered as personal when they could be identified by any third party; whereas, according to the relative criterion, data have to be considered as on a case by case basis and following a specific assessment carried out by the controller. In the view of some authors, the ECJ in its case law and WP29 in its guidance seem to favour the objective criterion.[72] In essence, the guidance on anonymisation of personal data sets a high threshold to consider healthcare data as fully anonymous. In most of circumstances, synthetic data generated from original personal data are likely to be considered pseudonymous data.[73]

Therefore, for the purposes of using synthetic data withing *in silico* trials, several data protection aspects need to be considered. The first aspect requires to check the nature of the original data. When the original data is personal data, data protection requirements will have to be considered at least before the execution of synthesis process. Second, while carrying out the synthesis from personal data, one should carefully consider the existing rules and orientations about pseudonymization and anonymisation, and the different privacy enhancing techniques suggested by WP29 in its Opinion 5/2014 on Anonymisation Techniques.

2.1.8. Legal bases for the processing of personal data

As seen above, the principle of lawfulness implies that the processing of personal data shall occur with **a legal basis**. The lawful grounds for the processing of personal data are foreseen by Article 6 of the GDPR. They consist in the following six options:

- **Consent** of the data subject
- Performance of a **contract** with the data subject
- Necessity of compliance with a **legal obligation**
- Protection of the **vital interests** of the data subject or another natural person
- The necessity to perform a **task in the public interest**
- The **legitimate interest** of the controller or of third parties.

The GDPR foresees an additional layer of protection for the special categories of personal data enlisted under **Article 9 GDPR** – which include **data concerning health**.[74] According to the same article, the processing of special categories of personal data is prohibited, unless one of the following exceptions apply:

a) the data subject has given **explicit consent** to the processing of personal data;
b) the processing is necessary for controller to meet **legal obligations** or for the controller and data subject to exercise specific rights in the field of employment law, social security and social protection law;
c) the processing is necessary to protect the **vital interests** of a data subject (or another person), and the data subject is physically or legally incapable of giving consent;

[71] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016].

[72] F Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (2017) 3 European Data Protection Law Review 130. However, it should be clarified that the text of the case does not explicitly recognise the prominence of a criterion over another.

[73] This report condenses the extensive debate in the literature. For an in-depth discussion, see César Augusto Fontanillo López and Abdullah Elbi, 'On Synthetic Data: A Brief Introduction for Data Protection Law Dummies' (2022); Fontanillo López César Augusto and Elbi Abdullah, 'On the Legal Nature of Synthetic Data' (2022). For further references on synthetic data and healthcare, see Katharina Ó Cathaoir and others, 'EUSTANDS4PM Report. Legal and Ethical Review of in Silico Modelling' (2020).

[74] It is widely recognised in the literature that art 6 and art 9 of the GDPR apply conjunctively (and not disjunctively). See Edward S Dove, 'The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era' (2018) 46 Journal of Law, Medicine & Ethics 1013.

d) 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
e) the data are **manifestly made public** by the data subject;
f) the processing is necessary to establish, exercise or defend legal claims;
g) the processing is necessary for reasons of **substantial public interest** on the basis of the Union State law;
h) the processing is necessary for the purposes of **preventive or occupational medicine**;
i) the 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;
j) the processing is necessary for archiving purposes in the public interest, **scientific** or historical **research purposes** or statistical purposes in accordance with Article 89(1) GDPR.

* In addition to the above exceptions, paragraph 4 of Article 9 GDPR establishes that **Member States may maintain or introduce further conditions**, including **limitations**, with regard to the processing of genetic data biometric data or **data concerning health**

The legal doctrine extensively debated about the role of **consent** in scientific research and as the fundamental legal basis for the primary use of health data.[75] In a nutshell, although consent has historically been considered as the core legal basis for research, there are also compelling reasons for which consent may not be the appropriate one in several circumstances.[76] Furthermore, it is essential to clearly distinguish between the concept of consent in data protection law – which has been extensively explored by recent guidance by the EU bodies[77] – from the notion of **informed consent for clinical trials.** Informed consent is governed by the Clinical Trial Regulation (CTR)[78] and shall be meant of the individual free and voluntary expression of willingness to participate in a clinical trial.[79] Therefore, the first is a legal basis for the processing of personal data in health research, the second is a prerequisite for the participation in a clinical trial.[80]

A recent opinion of the European Data Protection Board (EDPB) clarified that **for clinical trials** not all processing operations relating to the use of clinical trial data pursue the same purposes and thus fall within the same legal basis.[81] For the processing of personal data (Article 6 GDPR), the **performance of a task carried out in the public interest** or **legitimate interest** should be considered. The first is deemed as necessary when the conduct of clinical trials falls within the mandate, mission and tasks vested in a public or private body by

[75] See, *ex multis,* Edward S Dove and Jiahong Chen, 'Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis' (2020) 10 International Data Privacy Law 117; Giovanni Comandè and Giulia Schneider, 'Differential Data Protection Regimes in Data-Driven Research: Why the GDPR Is More Research-Friendly Than You Think' (2022) 23 German Law Journal 559.

[76] Dove and Chen (n 75).

[77] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

[78] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC [2014] OK L158/1 (Clinical Trials Regulation or CTR).

[79] CTR, art 2(2)(21).

[80] There seems to be confusion in practice. See Teodora Lalova-Spinks and others, 'Challenges Related to Data Protection in Clinical Research before and during the COVID-19 Pandemic: An Exploratory Study' (2022) 9 Frontiers in Medicine 995689.

[81] European Data Protection Board, 'Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (Art. 70.1.b))' (2019).

national law. The legitimate interest of the controller in the other cases. For the processing of **special categories of personal data** processed for purely research purposes could either be following **reasons of public interest in the area of public health** on the basis of Member States law or **scientific purposes** in accordance with Article 89 GDPR.[82]

2.1.9. The further processing of personal data

If the legal basis for the 'primary' processing of personal data and consent sparked great discussions, the issue of **further processing of personal data** goes even further. The further processing of personal data (also called '**secondary use**' of personal data)[83] is foreseen by the GDPR in Article 5(1)(b), according to which 'further processing for (…) scientific research purposes or statistical purposes shall, in accordance with Article 89(1) [GDPR] not be considered to be incompatible with the initial purposes' of the processing activity. In other words, there is a **presumption of compatibility** for the further processing of personal data for research purposes – if specific circumstances occur.[84] As the EDPB clarified, where data is further processed for scientific purposes, then the further processing shall not be considered *a priori* incompatible with the initial purposes and therefore the controller could be able, in certain situations, to further process the data without the need for a new legal basis.[85]

The legal basis for the further processing of personal data in scientific research is also discussed in doctrine and in practice. Some have considered **consent** to be advantageous for the further processing of personal data, as it would bring transparency and could allow subjects exercising control over their personal data. Others do not deem it appropriate.[86]

Another element of the analysis stems from Recital 33 GDPR on the so-called "**broad consent**". Since 'it is not often possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection', the recital suggests that 'data subjects should be allow to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research'.[87] In addition, the EDPB maintained that 'Recital 33 does not disapply the obligations with regard to the

[82] Art 89 GDPR requires that the '[p]rocessing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner'.

[83] The EHDS proposal (see *infra*, section 3.2 'The European Health Data Space proposal) offers a definition of secondary use of personal data – being its regulation one of the objectives of the proposal itself. To be noted, however, that data protection law discussions intend secondary use of data for 'personal data'; the EHDS, instead, will also concern non-personal data.

[84] As the EDPS put it 'the presumption is not a general authorisation to further process data in all cases for historical, statistical and scientific purposes. Each case must be considered on its own merits and circumstances. See European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research' 22 <https://edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf>.

[85] GDPR, rec 50. See also European Data Protection Board, 'Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (Art. 70.1.b))' (n 81) 8.

[86] Anton Vedder and Daniela Spajić, 'Moral Autonomy of Patients and Legal Barriers to a Possible Duty of Health Related Data Sharing' (2023) 25 Ethics and Information Technology 23.

[87] GDPR, rec 33.

requirements of specific consent' meaning that scientific research project can only include personal data 'on the basis of consent if they have a well-described purpose.[88]

For the reasons above data protection legislation on the further processing of personal data has been criticised by healthcare stakeholders for being 'unclear and confusing'.[89] The matter becomes even more complicated on other two fronts of application. At the EU level, the new EU data laws will need to be in line with the GDPR when it comes to the legal basis of primary and secondary use of health data and data altruism mechanisms.[90] At the national level, the GDPR rules may have implied **fragmentation across the Member States**.[91] There is the expectation that EU bodies will soon release a final guidance on the further processing of data for scientific research. It is to be hoped that the guidance could shield some light In that regard.[92]

2.1.10. Open discussions: data ownership

In addition to the established GDPR roles seen in section 2.1.2 'Personal scope of application of the GDPR', stakeholders in data governance have increasingly referred – sometimes also in academic works – to **data ownership**. The question may appear in health data sharing of *in silico* trials, especially for the sharing of certain datasets. For example, one entity wants to share certain datasets – in this case, we will consider non-personal data – for that other entities could use them for model training, or with the objective of obtaining evidence for *in silico* trials. In that case, some actors may wonder whether they do retain 'the ownership' of the data.

It is important to acknowledge that the GDPR in its wording does not envisage the formulation 'data ownership'. Data ownership is a concept that has been defined in the literature, within a debate about the evolution of data laws. According to some authors, a new European data law is emerging, adding up to data protection law.[93] New pieces of data legislation, such as the Data Act proposal and others imply an increasing interpenetration between economic law of data and personal data protection law.[94]

Therefore, when dealing with practical matters of data sharing, it is necessary to **conceptually separate the notion of data ownership, from the notion of data controllership**.[95] Data controllership is meant, as seen above, as the situation upon which data protection stakeholders may have the capacity to define the purposes and means of personal data processing. Differently, data ownership should be understood 'an economic

[88] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (n 77).

[89] Avicenna CSA, 'In Silico Clinical Trials: How Computer Simulation Will Transform the Biomedical Industry' (2016) 64.

[90] Mahsa Shabani and Sami Yilmaz, 'Lawfulness in Secondary Use of Health Data' [2022] Technology and Regulation 128.

[91] since they leave room for further conditions or limitations under Article 9(4) GDPR. One of the examples worth mentioning is the Italian case and Article 110 bis of the renovated Privacy Code. See Laura Liguori and Claudio Todisco, 'Il riutilizzo dei dati personali a fini di ricerca anche alla luce dei più recenti orientamenti del Garante' (*AboutPharma*, 1 December 2022) <https://www.aboutpharma.com/legal-regulatory/il-riutilizzo-dei-dati-personali-a-fini-di-ricerca-anche-alla-luce-dei-piu-recenti-orientamenti-del-garante/> accessed 5 April 2023.

[92] It is worth to note also that some researchers challenge this opinion, see Comandè and Schneider (n 75). They argue that the GDPR differently promotes research-valuable data flows in consistency with an emerging principle of free movement of personal data.

[93] This shift in legislative approaches at the EU level may be seen, for example, in the Data Governance Act, the Data Act proposal (see *infra,* section 3 'Data Governance). See Charlotte Ducuing, 'An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses' (2022) CiTiP Working Paper.

[94] ibid.

[95] For reasons of space this report cannot delve extensively on these conceptual matters. For further explorations, see the seminal research by Charlotte Ducuing, including ibid; Charlotte Ducuing, 'What Can We Still Learn from Data Ownership?' (ELI Digital Law SIG Seminar, 1 June 2022).

ownership right in data as intangible assets in the form of an exclusive right that enables the right holder to appropriate the economic benefits from the use of data'.[96]

It is not uncommon to hear in non-legal technical language 'the hospital owns the data' or 'the patient owns the data'.[97] From a data protection perspective, these assertions are incorrect. The hospital may be a data controller of the data, and the patient may – to a certain extent – exert control over their personal data, for example by enforcing their rights. However, in data protection law they both do not own the personal data. 'Owning' personal data opens further conceptual connotations concerning 'property'. In that respect, it is also essential to clarify – despite some authors deem it differently – as per the current orientation of EU data protection authorities sees is no property over personal data and that personal data cannot be 'commercialised'.[98] Finally, it is worth to note that data ownership aspects may concern also the discipline of **intellectual property law,** and it could concern access and modification of databases and thus copyright or the 'sui generis' database rights but also trade secrets.[99]

3. Data Governance

3.1. The Data Governance Act

3.1.1. Subject matter and material scope of the DGA

The Data Governance Act was initially put forward by the European Commission in November 2020, as part of its European Strategy for Data.[100] One of the underlying rationales the proposal was that, while the use of **data generated or collected by public sector bodies** at the expense of public budgets should benefit society, [101] certain categories of data – such as commercially confidential data, data subject to statistical confidentiality and data restricted through IP or data protection requirements – often are not made available, not even for research or innovative activities in the public interest.[102]

To face these challenges, the regulation **promotes the availability of data** and build a trustworthy environment to facilitate their use for research and the creation of innovative new services and products. Accordingly, the DGA sets out rules on the **re-use of certain categories of data by public sector bodies** in the EU,[103] the **notification and supervisory framework** for the provision of **data intermediation services**, the

[96] Josef Drexl, 'The (Lack of) Coherence of Data Ownership with the Intellectual Property System' in Niklas Bruun and others (eds), *Transition and Coherence in Intellectual Property Law* (1st edn, Cambridge University Press 2021) <https://www.cambridge.org/core/product/identifier/9781108688529%23CN-bp-16/type/book_part> accessed 4 April 2023.

[97] The example is taken from Kathleen Liddell, David A Simon and Anneke Lucassen, 'Patient Data Ownership: Who Owns Your Health?' (2021) 8 Journal of Law and the Biosciences lsab023.

[98] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (2017).

[99] Studio Legale Stefanelli & Stefanelli, 'Databases: Legal Protection between Italian Copyright and Sui Generis Right - Lexology' (2022) <https://www.lexology.com/library/detail.aspx?g=e4cb0182-b3b8-429c-9ac0-51325d8eca36> accessed 4 April 2023.

[100] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data' COM (2020) 66 final (European Strategy for Data).

[101] DGA, rec 6.

[102] *ibid.*

[103] DGA, art 1(1).

framework for voluntary registration of entities which collect and process data made available for **altruistic purposes**, and creates a **European Data Innovation Board.**[104]

3.1.2. Personal scope of the DGA

The DGA includes several actors within its framework. The first category that is relevant for the re-use of data is the **public sector bodies.** They are defined as the 'State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities, or one or more such bodies governed by public law'. As explained *infra,* public sector bodies may be competent to grant or refuse access for the re-use of certain categories of data in scope of the DGA. Closely related to public sector bodies are **the data intermediation service providers,** who render data intermediation services (see section 3.1.5). **Data cooperatives** may offer data intermediation services when their organisational structure is constituted by data subject, one-person undertakings or SMEs who are members of that structure having as its main objectives to support its members in the exercise of their rights, to exchange views on data processing purposes and conditions, and to negotiate terms and conditions for data processing on behalf of its members.[105] The entity or the natural person who has the right to grant access or to share certain personal data or non-personal data is meant by the Regulation as a **data holder.**[106] The natural or legal person who has lawful access to certain personal data or non-personal data and has the right to use that data for commercial or non-commercial purposes is called **data user.**[107]

3.1.3. Categories of data in the scope of application

The categories of data that are in scope of the regulation are enlisted under Article 3 of the DGA. They consist in those protected on the grounds of:

- **Commercial confidentiality**, including business, professional and company secrets
- **Statistical confidentiality**
- The protection of **intellectual property rights** of third parties, or
- The protection of **personal data,** insofar as such data fall outside the scope of the Open Data Directive[108].

3.1.4. The re-use of certain categories of protected data held by public sector bodies

Article 5 of the DGA establishes the conditions for the re-use of the data in scope of the Regulation. According to it, **public sector bodies** may grant or refuse access for the re-use of data.[109] To do so, they shall make publicly available the **conditions** for allowing such re-use and the procedure to request the re-use via a single information point. If they cannot grant access to certain data for re-use, public sector bodies should offer **assistance** to the potential re-user in seeking the individual's consent or the data users' authorisation.

For example, to ensure that the protected nature of data is preserved, they may provide some requirements, such as:

---

[104] *ibid.*

[105] DGA, art 2(15).

[106] DGA, art 2(8). The individual person shall not be a data subject with regard to the data in question.

[107] DGA, art 2(9).

[108] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ 172/56 (Open Data Directive).

[109] This section will refer to 'data' as data considered in the scope of DGA.

- The public sector or the competent body ensured that the data has been anonymized (in the case of personal data) and modified, aggregated or treated by any other method of disclosure control (in the case of commercially confidential information);[110]
- The access and re-use of data happen within a **secure processing environment**, provided or controlled by the public sector body;
- The access and re-use of data within the **physical premises** or remote access in certain circumstances.

National laws my provide additional confidentiality obligations relating to the re-use of data. In any case, the DGA makes clear that re-users shall be prohibited from re-identifying any data subject to whom the data relates. Also they shall take technical and operational measures to **prevent re-identification.** If re-identification occurs, this shall be notified as a personal data breach.[111] Specific rules govern data transfers to third countries.

Member States will have to ensure that the relevant information for the application of the above requirements is available and accessible through a **single information point** – which may linked to sectoral, regional or local information points.[112] The single information point will receive the enquiries or requests for the re-use of data, and will transmit them to the public sector or competent bodies.

The **procedure for requests for re-use** is detailed in Article 9 DGA. In essence, public sector or competent bodies have two months (extendable up to 30 days for exceptionally extensive and complex requests) as a rule to decide on the request.[113]

3.1.5. Data intermediation services

At the core of the DGA lies the framework setting the **requirements applicable to data intermediation services.**[114] Data intermediation services are services that aim to establish commercial relationships for the purposes of data sharing between data subjects and data holders on the one hand, and data users on the other.[115] The may consist in:[116]

- **Intermediation services between data holders and potential data users**. Those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabligh the exchange or joint use of data, or the establishment of other specific infrastructure for the interconnection of data holders with data users.
- **Intermediation services between natural persons** (either data subjects or persons that seek to make non-personal data available) **and potential data users.**
- Services of **data cooperatives**, which are data intermediation services offered by an organizational structure constituted by data subjects, one-person undertakings or SMEs who are members of that structures and that have the main objective to support their members in a certain aspects.

The DGA excludes some hypotheses where services are not considered as intermediation ones. These include services that focus on intermediation of copyright-protected content and services that are exclusively used by

[110] DGA, art 5(3).

[111] DGA, art 5(5).

[112] DGA, art 8.

[113] Running from the date of receipt of the request. DGA, art 9.

[114] DGA, Chapter III.

[115] DGA, art 2(11).

[116] DGA, art 10.

one data holder or a closed group.[117] Any data intermediation services provider who intends to provide these services will have to notify the competent authority for data intermediation services.[118]

Article 12 sets put the conditions for providing data intermediation services. These include the respect of intended purposes for the data use, interoperability, tools and services to facilitate the exchange of data, fair transparent and non-discriminatory procedures, data transfers, security, consent, log recording for the data intermediation activity.

3.1.6. Data Altruism

The DGA introduces provision on the so-called **data altruism**, which in the future could be relevant for *in silico trials.* Data altruism is defined by the DGA as the **voluntary sharing of data** on the basis of:

- the **consent** of data subjects to process personal data pertaining to them, or
- **permissions** of data holders to allow the use of their non-personal data

without seeking or receiving a reward that goes beyond the compensation related to the cost that they incur, for **objectives of general interest** provided by national law, such as **healthcare**, improving the provision of public services, public policy making or **scientific research** purposes in the general interest.[119] Member States may have in place organizational or technical arrangements to facilitate data altruism. To that end, they may establish **national policies for data altruism.**[120]

The Regulation recognizes the possibility for certain entities to qualify as **data altruism organisations.** An entity shall be registered in the public register of recognized data altruism organisations.[121] To qualify as such, the entity shall, *inter alia,* carry out data altruism activities; be a legal person established pursuant to national law to meet objectives of general interest as provided for in national law; operate on a not-for-profit basis and be legally independent from any entity that operates on a for-profit basis; carry out its data altruism activities through a structure that is functionally separate from its other activities, comply with the rulebook set by the Commission following Article 22 DGA.[122]

Data altruism organization will have to comply with **transparency** requirements[123] and specific requirements to **safeguard rights and interests of data subjects** and data holders with regard to their data.[124] The latter include information obligations, not going beyond the objectives of general interest for the use of data, modalities to obtain data altruism consent, security of data processing.[125] To facilitate the collection of data based on data altruism, the European Commission will be called to adopt implementing acts concerning a **European data altruism consent form**.[126]

[117] DGA, art 2(11)(a)-(d).

[118] DGA, art 11.

[119] DGA, art 2(16).

[120] DGA, art 16.

[121] DGA, art 17.

[122] DGA, art 18.

[123] DGA, art 20.

[124] DGA, art 21.

[125] *ibid*.

[126] DGA, art 25.

3.2. The European Health Data Space proposal

3.2.1. Subject matter and material scope of the proposed regulation

On May 3rd 2022, the European Commission put forward a legislative proposal on the European Health Data Space, seeking to establish rules for healthcare interoperability and patient empowerment issues that have existed in the EU for a long time. The European Health Data Space proposal provides rules, common standards and practices, infrastructures and a governance framework for the primary and secondary use of electronic health data.[127] The regulation aims at:

- Strengthening the **rights of natural persons** in relation to the availability and control of their electronic health data;
- Laying down rules for the placing on the market, making available or putting into service of **electronic health records systems** (EHR systems);
- Laying down rules and mechanisms supporting the **secondary use** of electronic health data;
- Establishing a mandatory **cross-border infrastructure** enabling the **primary use** of electronic health data across the Union;
- Establishing a mandatory **cross-border** infrastructure for the **secondary use** of electronic health data.

3.2.1. Personal scope of the EHDS proposal

Once approved, the regulations aim to apply to various actors within the data sharing environment. Firstly, it will apply to **manufacturers and suppliers** of EHR systems and wellness applications that will be placed on the market or put into service in the Union and the users of such products.[128] Secondly, the proposed regulation will apply to **controllers and processors of electronic health data.** Similarly, the EHDS proposal would apply to controllers and processors established in a third country following certain requirements.[129] Finally, the regulation will apply to **data users** to whom electronic health data are made available by data holders in the Union.[130]

All these actors may appear in the *in silico* trial environment EHR systems and wellness applications may be relevant as they could gather data that to be used in several phases of the drug or medical device lifecycle. For instance, they could serve as real-world data and support the pharmacovigilance of certain medicinal products. The same tools could be relevant for gathering clinical evidence data for medical devices. [131] Second, *in silico* actors most likely qualify as controllers and processors of electronic health data since they might process electronic health data – during personal data collection, the acquisition and training of datasets, and during data pseudonymization or anonymisation.

[127] EHDS proposal, art 1.

[128] EHDS proposal, art 1(3).

[129] EHDS proposal, art 1(3)(c).

[130] EHDS proposal, art 2(2)(z). In this case, data users are not the same 'data users' of the Data Act proposals, as they have a specific definition in the EHDS. They are defined as the 'natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use'.

[131] The example is for illustrative purposes only. In practice, several concerns may be raised about the issues concerning data quality, especially when sourced by wellness applications. See European Data Protection Board and European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en>.

Figure 1 - Personal scope of the EHDS proposal

The EHDS defines data users as natural or legal persons having lawful access data to electronic health data for secondary use.[132] As a possible example for *in silito* trials, regulatory authorities in the future may be users having regard to certain electronic health data when needed throughout the lifecycle of a medicinal product.

3.2.2. Other subjects established or identified by the EHDS

Beyond the entities identified in its personal scope, the EHDS proposal paves the way for the establishment of new figures in the data sharing landscape. These include the health **data access bodies, digital health authorities and the European Health Data Space Board**.

Health data access bodies (HDABs) are meant to facilitate the secondary use of electronic health data and ensure that electronic data are made available by data holders and data users. Data holders will be required to cooperate with the health data access body to ensure the availability of electronic health data for data users. According to the EHDS proposal Explanatory Memorandum, these bodies should help ensure predictable and simplified access to electronic health data and a higher level of transparency, accountability and security in data processing'.[133]

The EHDS proposal also establishes the **European Health Data Space Board** (EHDSB) to facilitate the cooperation and the exchange of information among Member States and the cooperation between digital health authorities and health data access bodies. The EHDSB shall be composed of the high representatives of digital health authorities and health data access bodies of the Member States.[134] Stakeholders and relevant third parties, such as patients' representatives, shall be invited to attend their meetings and participate in its work.

Finally, the EHDS proposal also mentions **digital health authorities**. Following the proposed regulation, digital health authorities should be established in all Member States (as separate organisations or as part of the currently existing authorities).[135] Once nominated, they shall ensure the implementation of the rights and obligations set by the EHDS concerning the primary use of data.[136] The tasks of the digital health authorities are enlisted in Article 10 EHDS proposal. Among the many competences, the digital health authorities are competent to receive complaints from natural and legal persons, following Article 11 of the EHDS proposal. Also, they will have to ensure that complete and up-to-date information about the implementation of rights and obligations for individuals is made readily available to natural persons, health professionals and healthcare providers.[137]

[132] In the sections that follow, the notion of 'secondary use' is explained in more depth. See *infra,* section 3.2.7.

[133] EHDS proposal, Explanatory Memorandum, 15.

[134] EHDS proposal, art 64(1).

[135] EHDS proposal, rec 22.

[136] EHDS proposal, art 10.

[137] EHDS proposal, art 10(2)(b).

3.2.3. Data definitions in the EHDS proposal

The proposal introduces new definitions concerning health data. **Electronic health data** is at the core of the proposed regulation. They consist of personal or non-personal electronic health data.[138] **Personal electronic health data** encompass a wide range of data, including data concerning health as defined in the GDPR[139], as well as data referring to determinants of health or data processed in relation to the provision of healthcare services, processed in electronic form.[140] Personal electronic health data could include personal data related to the physical or mental health of a natural person or on the provision of health care services revealing information about their health status. These could consist, for example[141], of 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 in question, as well as data determinants of health, such as behaviour, environmental, physical influences, medical care, social or educational factors.[142]

Non-personal electronic data are defined as 'data concerning health and genetic data in an electronic format that falls outside the definition of personal data' (as provided in Article 4 of the GDPR).[143] Recital 5 of the EHDS proposal clarifies that electronic health data also includes data that has been initially collected for research, statistics, policy-making or regulatory purposes. Moreover, following the same recital, electronic health data qualify as such regardless of the fact that such data is provided by the data subject or other natural or legal persons (such as health professionals).[144]

Electronic health data should include **inferred and derived data.** These are not defined by the proposal text, but they are exemplified as diagnostics, tests and medical examinations, as well as data, observed and recorded by automated means.[145] Further to inferred and derived data, electronic health data include **data observed and recorded by automatic means.**

3.2.4. The primary use of electronic health data

The proposal defines the **primary use of electronic health data** as the 'processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of the natural person to whom that data relates'.[146] It could include the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services.[147] The primary use of electronic health data entails consequences in several respects.

The first aspect concerns the **rights of natural persons.** In relation to the primary use of electronic health data, the EHDS proposal envisages a set of **rights** – which specifically concern **personal electronic health data (EHD).** In that regard, individuals will have the right to access their personal electronic health data 'immediately, free

[138] EHDS proposal, art 2(2)(c). 'Data' is meant as in the definition of the Data Governance Act. See DGA, art 2(2) 'any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording'

[139] See *supra,* section 2.1.4.

[140] EHDS proposal, art 2(2)(a).

[141] This exemplification is provided by the EHDS proposal itself. See EHDS proposal, rec 5.

[142] EHDS proposal, rec 5.

[143] EHDS proposal, art 2(2)(b).

[144] For a definition of data subject, see GDPR, art 2.

[145] For more remarks about inferred and derived data in the Data Act and the EHDS, see also Charlotte Ducuing and others, 'White Paper on the Data Act Proposal' [2022] SSRN Electronic Journal 85–92 <https://www.ssrn.com/abstract=4259428> accessed 17 November 2022.

[146] EHDS proposal, art 2(2)(d).

[147] EHDS proposal, art 2(2)(d).

of charge and in an easily readable, consolidated and accessible form'.[148] Furthermore, the proposal will allow individuals to receive an electronic copy of their EHD.[149] The said right could be restricted in its scope following art 23 GDPR. To enable the implementation of this provision, Member States may establish **electronic health data access services**, as well as **proxy services** to allow one authorize other persons to access their data on their behalf.[150] Interestingly, the EHDS proposal allows the natural person to insert their electronic health data in their own EHR [151] through electronic health data access services or applications linked to these devices. At the same time, natural persons retain the right to restrict access of health professionals to all or part of their electronic health data.[152] Finally, Article 3 of the proposal establishes that natural persons shall have the right to obtain information on the healthcare providers and health professionals that have accessed their electronic health data in the context of healthcare.

A second aspect concerns **health professionals**.[153] Health professionals shall have access to electronic health data of natural persons under their treatment.[154] They also have to ensure that the personal electronic health data of the natural persons they treat are updated with information related to the health services provided. Health professionals should access electronic health data[155] though **health professional access services**, free of charge.[156]

3.2.5. Priority categories of personal electronic health data for primary use

The EHDS proposal establishes a set of **priority categories** of personal electronic health data for primary use. The priority categories are enlisted in Article 5 of the proposal and further substantiated in Annex I. These consist of the following:

- **patient summaries**: these include personal details, contact information, information on insurance, allergies, medical alerts, vaccination/prophylaxis information, possibly in the form of a vaccination card, current, resolved, closed or inactive problems, textual information related to medical history, medical devices and implants, procedures, functional status, current and relevant past medicines, social history observations related to health, pregnancy history, patient provided data, observation results pertaining to the health condition, plan of care, information on a rare disease such as details about the impact or characteristics of the disease);
- **Electronic prescriptions**;[157]

[148] EHDS proposal, art 3.

[149] The proposal mentions 'at least their electronic health data in the priority categories referred to Article 5'. EHDS proposal, art 3(2).

[150] EHDS proposal, art (5).

[151] Or in that of natural persons whose health information they can access.

[152] EHDS proposal, art 3(9). Member States are required to establish the rules and specific safeguards regarding such restriction mechanisms.

[153] Health professionals are meant within the definition provided in Directive 2011/24: 'a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment'. See Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L88/45.

[154] That should be – from a logical interpretation – with the caveats of art 3.

[155] At list the priority categories identified under art 5 EHDS proposal.

[156] EHDS proposal, art 4.

[157] As defined in Article 3(k) of Directive 2011/24/EU.

- **Electronic dispensations**: information on the supply of a medicinal product to a natural person by a pharmacy based on an electronic prescription;
- **Medical images and image report:** electronic health data related to the use of or produced by technologies that are used to view the human body in order to prevent, diagnose, monitor, or treat medical conditions;
- **Laboratory results:** Electronic health data representing results of studies performed notably through in vitro diagnostics such as clinical biochemistry, haematology, transfusion medicine, microbiology, immunology, and others, and including, where relevant, reports supporting the interpretation of the results;
- **Discharge reports:** Electronic health data related to a healthcare encounter or episode of care and including essential information about admission, treatment and discharge of a natural person;

By means of implementing acts, the Commission will have to lay down the technical specifications for the priority categories of personal electronic health data, setting out the **European electronic health record exchange format.**[158]

3.2.6. Cross-border infrastructure for the primary use of electronic health data

As part of its main objectives, the regulation aims at establishing a **cross-border infrastructure for the primary use of electronic health data** in the EU. Article 12 of the proposal mandates the European Commission to establish a **central platform** for digital health to provide **services** and **facilitate the exchange** of electronic health data between national contact points for the digital health of the Member States.

Each Member State will have to designate one **national contact point for digital health** and the central platform for digital health. Each national contact point for digital health shall enable the exchange of personal electronic health data with all other national contact points, and that exchange will be based on the European health record exchange format.

Member States will be required to ensure the **connection of all healthcare providers to their national contact points for digital health** and shall ensure that those connected can perform a **two-way exchange** of electronic health data with the national contact point for digital health. Also, **pharmacies** may have a role within this cross-border infrastructure. They shall access and accept electronic prescriptions transmitted to them from other Member States through MyHealth@EU.[159]

3.2.7. The secondary use of electronic health data

The **secondary use of electronic health data** means the processing of electronic health data for a series of purposes, enumerated by Article 34 of the EHDS proposal (*infra*). The article explicates that health data access bodies where the intended purpose of processing pursued by the applicant complies with the following:

- Activities for reasons of **public interest** in the area of public and occupational health (for example: ensuring high levels of quality and safety of healthcare and of medicinal products or medical devices)
- To support **public sector bodies,** including regulatory authorities in the health or care sector, to carry out their tasks;
- **Scientific research** related to health or care sectors;
- **Development and innovation** activities for products or services contributing to public health or social security or ensuring high levels of quality and safety of health care, medicinal products or of medical devices;

[158] EHDS proposal, art 6.

[159] EHDS proposal, art 12(6).

- **Training, testing and evaluating of algorithms**, including in medical devices, AI systems and digital health applications, contributing to the public health or social security or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;
- Providing **personalised healthcare** consisting in assessing, maintaining or restoring the state of health of natural persons based on the health data of other natural persons;
- to produce national, multi-national and Union level official statistics related to health or care sectors;
- **education or teaching** activities in health or care sectors.

Following the definition of the EHDS proposal, the data used may include personal electronic health data initially collected in the context of primary use but also electronic health data collected for the purpose of the secondary use.[160] There are **minimum categories of electronic data** that data holders shall make available for secondary use. These include:[161]

- EHRs;
- person-generated electronic health data (including medical devices, wellness applications or other digital health applications);
- human genetic, genomic and proteomic data;
- identification data related to health professionals involved in the treatment of a natural person;
- population-wide health data registries (public health registries);
- electronic health data from medical registries for specific diseases;
- electronic health data from clinical trials;
- electronic health data from medical devices, and from registries for medicinal products and medical devices;
- research cohorts, questionnaires and surveys related to health;
- electronic health data from biobanks and dedicated databases.

Other kinds of categories still included in the minimum categories,[162] less relevant to In Silico trials are:

- data impacting on health (including social, environmental, behavioural determinants of health);
- health-related administrative data (including claims and reimbursement data);
- electronic data related to insurance status, professional status, education, lifestyle, wellness and behaviour data relevant to health;
- electronic health data containing various improvements such as correction, annotation, enrichment received by the data holder following processing based on a data permit.

The data above shall also cover data processed in the provision of healthcare, as well as research, innovation official statistics, patient safety or regulatory purposes, collected by entities in the healthcare sector.[163]

3.2.8. Prohibited secondary use of electronic health data

The proposal prohibits certain purposes of secondary uses of electronic health data when obtained via a data permit. For example, secondary use of electronic health data is prohibited for **advertising or marketing activities** towards health professionals, organisations in health or natural persons.[164] Alternatively, data

[160] EHDS proposal, art 2(2)(e).

[161] EHDS proposal, art 33(1).

[162] EHDS proposal, art 33(1).

[163] EHDS proposal, art 33(3).

[164] EHDS proposal, art 35(1)(c).

cannot be used to exclude persons or groups from the benefit of an insurance contract or modify their contributions and insurance premiums.

One cannot seek access to and process electronic health data to take **decisions**[165] **detrimental to a natural person based on their electronic data**. A another prohibited purpose concerns the **development of products or services that may harm individuals and societies at large.**[166]

The data permit shall mention the **third parties** with whom the access or making available of the electronic health data available is being issued. If this is not mentioned, the secondary use of electronic health data is prohibited.[167]

3.2.9. The data access application and the data permit

The **data permit** is the administrative decision issued to a data user by a health access body or data holder to process the electronic health data and the secondary use purposes specified in the data permit itself.[168]

Health data access bodies may issue a data permit following certain conditions. The application shall fulfil one of the purposes enlisted above[169] and should not imply the prohibited ones in Article 35 of the proposal. The health data access body can issue or refuse the data permit within two months – extendable of two months where necessary.[170] If the data access body fails to provide a decision within the time limit, the data permit must be submitted.

To obtain a data permit, it is necessary to submit a **data access application.** A data access application can be submitted by any natural or legal person. The application shall include a series of elements, enlisted under Article 45(2) of the EHDS proposal – for example, the detailed information of the intended use of the electronic health data, the description of the requested data, the indication whether data should be made available in an anonymised format; safeguards planned to prevent any other use of the data; safeguards planned to protect the rights and interests of the data holder and the natural persons concerned; estimated period for which the data is needed; a description of the tools and computing resources needed for a secure data environment. As Article 45(6) clarifies, the European Commission may set out **templates for the data access application** by means of implementing acts. Article 45 of the proposal suggests that data users seeking access to electronic health data from more than one Member State shall submit a **single application** to one of the concerned health data access bodies of their choice. The health data access body shall then notify the other relevant health data access bodies of the receipt of the application.[171]

3.2.10. Governance and mechanisms for the secondary use of electronic health data

To allow the secondary use of electronic health data, the EU Member States will be required to establish one or more **health data access bodies** for the secondary use of electronic health data and ensure that electronic data are made available by data holders for data users.[172] Health data access bodies are meant to be **responsible for granting access to electronic health data for secondary use.**

---

[165] In order to qualify as "decisions", the EHDS proposal specifies that they 'must produce legal effects or similarly significantly affect those persons'. EHDS proposal, art 35(1)(a).

[166] EHDS proposal, art 35(e).

[167] EHDS proposal, art 35(d).

[168] EHDS proposal, art 2(2)(aa).

[169] As enlisted under art 34 of the EHDS proposal; see *supra.*

[170] EHDS proposal, art 46(3).

[171] EHDS proposal, art 45(3).

[172] EHDS proposal, Explanatory Memorandum, 19.

Currently, the figure of 'health data access bodies' does not exist yet in the European Union. The Member States will have to establish them. They could be either newly established but also they decide to rely on existing public sector bodies or internal services of public sector bodies. In any case, if there is more than one health data access body in a country, the Member State shall identify one acting as a coordinator.[173]

Among the many tasks, the health data access bodies will have to **decide on data access applications** submitted by the subjects requesting a data permit[174] and thus **authorise and issue data permits**. They should also be competent in deciding on data requests following Chapter II of the DGA.[175] As part of their tasks, they may gather and compile *or* provide access to the necessary electronic health data from various data holders, and they must **put** those **data at the disposal of data users in a secure processing environment.**[176] They can also process electronic health data on the basis of a data permit,[177] or from other relevant data holders based on a data permit or request.[178]

Data access bodies would retain **obligations towards natural persons.** Article 38 of the proposal would require them to make publicly available and easily searchable the conditions under which electronic health data is made available for secondary use, with information concerning, for example, the legal basis under which access is granted, the technical and organisational measures taken, the applicable rights of natural persons, the results or outcomes of the projects for which the electronic health data were used.[179]

Finally, health data access bodies shall provide access to electronic health data only through a **secure**

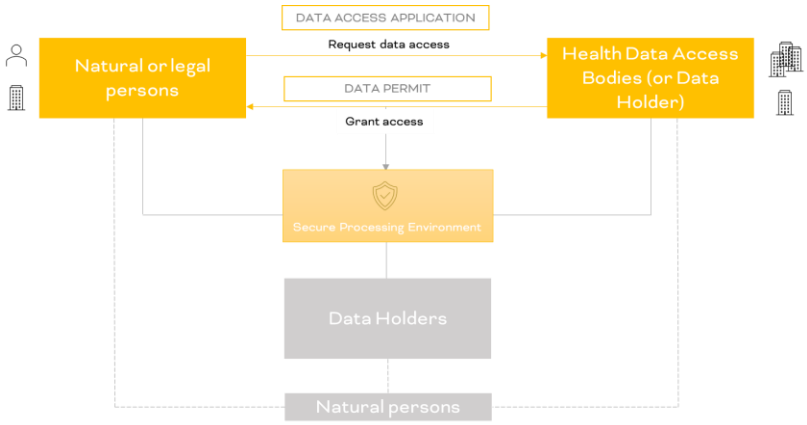

Figure 2 EHDS governance and mechanisms for data sharing

processing environment, with technical and organisational measures and security and interoperability requirements.[180] When processing electronic health data, **data altruism organisations** will have to comply with the rules set by Chapter IV of the DGA. In addition to these, where data altruism organisations process electronic health data using a secure processing environment, such environments shall also comply with the requirements set by the EHDS.

[173] EHDS proposal, art 36.

[174] On data access application, see *supra,* and EHDS proposal, art 45.

[175] EHDS proposal, art 37(1)(a).

[176] On secure processing environments, see EHDS proposal, art 50.

[177] EHDS proposal, art 37(d).

[178] EHDS proposal, art 37(e).

[179] EHDS proposal, art 38.

[180] EHDS proposal, art 50.

3.2.11. EHR systems and wellness applications

The EHDS proposal sets obligations of economic operators with regard to **Electronic Health Records (EHR) systems**. Electronic Health Records systems are defined as 'any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records[181]. For example, medical device software could be considered an EHR system. Software that imports electronic health records to be used for *in silico* trials or software that edits these records for virtual simulations, may be considered EHR systems.

The proposal sets several obligations for manufacturers of EHR systems, which shall be complied with to place them into the market or put into service. EHR systems will have to be in conformity with the essential requirements set by the proposal, be accompanied by technical documentation and instructions for use, have the CE marking affixed and comply with registration obligations.[182] Annex II of the proposal sets the essential requirements for those systems, which can be implemented by the Commission by means of common specifications.[183]

Along with EHRs, the proposal also addresses **wellness applications**, which are meant as 'any appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data for other purposes than health care, such as well-being and pursuing healthy lifestyles'.[184] Manufacturers of wellness applications may choose to undergo their **labelling** (on a **voluntary** basis).[185] Finally, Article 32 of the proposal mandates the Commission to establish a **publicly available database** where certified EHR systems and labelled wellness applications will be registered.

3.2.12. Mandatory cross-border infrastructure for secondary use of electronic health data

In addition to these, the proposal established rules for a **cross-border infrastructure for the secondary use of electronic health data** (HealthData@EU).[186] Each member will have to designate a national contact point for the secondary use of electronic health data, responsible for making electronic health data available for secondary use in a cross-border context.

3.2.13. Health data quality and utility for secondary use

A critical aspect regulated by the EHDS proposal concerns **data quality requirements.** Health data access bodies will have to inform the data users about the available datasets and their characteristics through a metadata catalogue. Each dataset will have to include information about the source, the scope, the main characteristics, the nature of electronic health data and the conditions for making electronic health data available.[187] The European Commission may set out the **minimum information elements** that data holders shall provide for datasets and their characteristics.

Moreover, **datasets** made available may have a **quality and utility label** provided by the data holders.[188] When datasets with electronic health data are collected and processed with the support of EU and national funding, they shall have a data quality and utility label. The label requires compliance with several elements, including

[181] EHDS proposal, art 2(2)(n). Electronic Health Records (EHR) are defined as a 'collection of electronic health data related to a natural person and collected in the health system, processed for healthcare purposes' (EHDS proposal, art 2(2)(m)).

[182] EHDS proposal, art 17.

[183] EHDS proposal, art 23.

[184] EHDS proposal, art 2(2)(o).

[185] EHDS proposal, art 31.

[186] EHDS proposal, art 52.

[187] EHDS proposal, art 55.

[188] EHDS proposal, art 56.

data documentation; technical quality; data quality management processes, coverage, information on access and provision, and information on data enrichments.[189]

The Commission will be called to establish an **EU Datasets Catalogue**, connecting the national catalogues of datasets established by the health data access bodies and other authorized participants in HealthData@EU.[190]

3.2.14. Open discussions about the European Health Data Space proposal

Almost one year after its release, healthcare stakeholders including industry, policymakers, and academia, have commented on the EHDS proposal. Overall, there is a general welcome of the European Health Data Space proposal as a possible tool to **overcome barriers to health data sharing**. Nevertheless, the proposal seems to raise some issues. These are reported in the following lines.

The main aspect that several stakeholders underscored is the **complex interaction** of the EHDS proposal with **the Data Act, the GDPR and DGA** – or other current and anticipated laws.[191] Shabani and Yilmaz underline possible tensions of secondary use of personal data having regard to the existing legal bases and consent.[192] Other authors comment on the possible shift that these legal bases may imply for individual **control** over personal data.[193] Hildebrandt further argues that purpose limitation oversight has been historically difficult in data protection, and it will likely be in the context of health data sharing.[194]

On the secondary use of health data, Marcus and others underlined that the **list of permitted purposes** is very **broad**, while the list of prohibited practices could be too rigid.[195]

On the role of the **health data access bodies**, a study commissioned by the European Parliament suggested that it may be unnecessary or unproductive to assign **too many different tasks** to the health data access body.[196] Further concerns relate to the coordination of **digital health authorities** with existing data protection authorities, which could require further substantiation.[197]

Some persons criticized the lack of patient involvement in the drafting of the EHDS proposal. This lack of involvement and consideration may imply that the EHDS proposal has failed to bridge **digital divides** and has the potential to **exacerbate digital inequalities**.[198] As Kessel and others put it, 'vulnerable population groups could be further disadvantaged through lack of access to digital infrastructure and underdeveloped digital skills'.[199] Civil society express is concerned that patient's privacy rights would not be respected and its security

---

[189] EHDS proposal, art 56(3).

[190] EHDS proposal, art 57.

[191] J Scott Marcus and others, 'The European Health Data Space' [2022] SSRN Electronic Journal <https://www.ssrn.com/abstract=4300393> accessed 25 January 2023.

[192] Shabani and Yilmaz (n 90).

[193] Teodora Lalova-Spinks, 'Data Control in the European Health Data Space Proposal: Highlights' (Data Week 2022, June 2022) <https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias3790964&context=SearchWebhook&vid=32KUL_KUL:Lirias&search_scope=lirias_profile&tab=LIRIAS&adaptor=SearchWebhook&lang=en>.

[194] Mireille Hildebrandt, 'Ground-Truthing in the European Health Data Space' (SocArXiv 2023) preprint <https://osf.io/uw4nq> accessed 20 January 2023.

[195] Marcus and others (n 191).

[196] ibid.

[197] European Data Protection Board and European Data Protection Supervisor (n 131).

[198] Robin van Kessel and others, 'The European Health Data Space Fails to Bridge Digital Divides' [2022] BMJ e071913.

[199] *ibid*.

standards are too low.[200] Finally, a prominent **worry** among healthcare stakeholders concerns the risk of having a regulation that, in practice, leaves room for **scattered implementation** at the national level, as some provisions of the EHDS proposal leave room for national implementation.[201]

3.3. The Data Act proposal

3.3.1. Subject matter and material scope of the Data Act proposal

The Data Act is another piece of proposed Regulation about data put forward by the European Commission. It lays down rules on **data sharing** between **business to consumer, business to business and business to government**. The proposed regulation lays down harmonised rules on the:

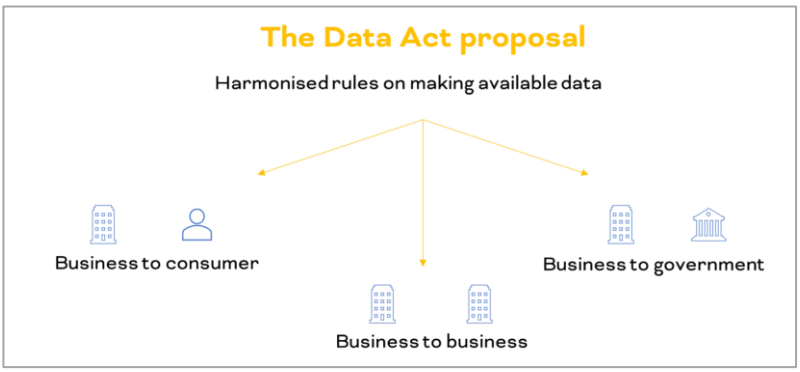

Figure 3 The Data Act proposal

- Making data generated by the use of a product or related service available to the user of that product or service
- On the making data available by data holders to data recipients
- On the making of data available from data holders to public sector bodies or Union institutions, agencies or bodies where there is an exceptional need for the performance of a task carried out in the public interest. (business to government)

3.3.2. Personal scope of the Data Act proposal

The personal scope of the proposed regulation encompasses different stakeholders. First, it addresses **manufacturers** of products and suppliers of related services placed on the market. In the *in silico* environment, manufacturers of products could include medical device manufacturers.[202]

Second, the regulation addresses **data holders** that make data available to data recipients in the Union. Data holders are defined by Article 2 as the 'legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make certain available data'.[203] Healthcare providers, for example, could be considered data holders for the purposes of this Regulation. Also, medical device manufacturers could be considered as such – depending on the circumstances.

Third, the regulation concerns **data recipients.** These are the natural or legal persons to whom the data holders make data available. **Public sector bodies** are also within the scope of the proposed Regulation. Public sector bodies may be national, regional, or local authorities of the Member States and bodies governed by public law of the Member States or associations formed by one or more such authorities or one or more such

[200] European Digital Rights, 'EHDS: Ignoring Patients' Privacy' (*European Digital Rights (EDRi)*, 6 March 2023) <https://edri.org/our-work/eu-proposed-health-data-regulation-ignores-patients-privacy-rights/> accessed 27 April 2023.

[201] For instance, see EHDS proposal, art 3.9 on the possibility to restrict access to EHD from data subject, or art 4 – where it states that the Member States may establish rules providing for the categories of personal electronic health data required by different health professions.

[202] Data Act proposal, rec 14.

[203] Data Act proposal, art 2.

bodies. Finally, the Data Act proposal includes some exemptions. Small and micro enterprises are not subject to the obligations of Chapter II on business-to-consumer and business to business data sharing.[204]

3.3.3. Data definitions in the Data Act proposal

One notable aspect of the Data Act proposal is the proposed definition of '**data**'. These are defined as any digital representation of acts, facts, or information, any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording.[205]

The scope of the Regulation is limited to data generated by the use of products and related services. Recital 14 of the proposal clarifies that the regulation's scope does not include **inferred or derived data.**[206] Users may have the right to access **data generated by a product** or a related **service** – irrespectively as to whether they are personal or non-personal data; or if they are actively or passively observed data. The Data Act proposal does not offer any reference to an existing definition of inferred or derived data. A possible interpretation may stem from data protection law – although it is worth noting that here the Data Act proposal would also cover non-personal data.

In data protection, these categories depend on the origin of the data.[207] In its guidance on data portability, the WP29 distinguishes between **data actively provided** by the data subjects (e.g. mailing address, user name, etc.)*;* and **observed data** provided by the data subject by virtue of the use of the service or the device (e.g. person's search history, traffic data, location data). These two kinds of data are juxtaposed to **inferred and derived data** that are 'created by the data controller on the basis of the data "provided by the data subject"'.[208] For example, the outcome of an assessment regarding a user's health in the context of risk management and financial regulations (e.g. to assign credit score) is deemed by WP29 as not 'provided by the data subject'. Furthermore, as part of the objectives of data portability, data 'provided by the data subject' should be intended broadly and should exclude inferred and derived data, which include **personal data that are created by a service provider** (for example, algorithmic results).[209] By an *a contrario* interpretation, inferred data are data that are the subsequent analysis of individual behaviour, whereas data relating to the data subject's activity or resulting from the individual's behaviour should be considered as 'provided by the data subject'.

This is an interpretation that indeed may help in understanding the meaning of inferred or derived data for the purposes of the Data Act proposal, although it concerns only personal data. The EHDS proposal includes further references about inferred or derived data that might be relevant to this discussion. In its Recital 5, it states that inferred and derived data may be 'diagnostics, tests and medical examinations, as well as data, observed and recorded by automated means'.[210] If the proposal reference remains in its final text, it may mean that they will be **excluded** from Data Act proposal provisions, especially those about **business-to-consumer data sharing**.[211]

---

[204] Data Act proposal, art 7.

[205] Data Act proposal, art 2.

[206] see also Matthias Leistner and Lucie Antoine, 'Attention, Here Comes the EU Data Act! A Critical in-Depth Analysis of the Commission's 2022 Proposal' (2022) 13(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 339.

[207] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability'.

[208] ibid 10.

[209] Article 29 Data Protection Working Party, 'WP 242 Rev.01' (n 207).

[210] EHDS proposal, rec 5.

[211] Data Act proposal, rec 14.

3.3.4. Business-to-consumer and business-to-business data sharing

Chapter II of the proposal introduces an **obligation to make data generated by the use of products or related services accessible** in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible by the user.[212]

These rules may become relevant for *in silico* technology. Products or related services within the Data Act proposal could include medical devices, and thus it is reasonable to consider also including medical device software. It is still early to imply final considerations about this legislative proposal[213]; however, the proposed text may suggest that medical device software or medical devices tested following *in silico* trials could in principle, fall under certain requirements of Chapter II of the Data Act.

The proposal establishes that products shall be designed and manufactured, and the related services shall be provided in such a manner that **data generated** by their use are, by default, easily, securely and, where relevant and appropriate, directly **accessible to the user**.[214] In this case, the user could consist in healthcare providers that own a medical device processing data. In principle, users could also be patients that receive a services in the form of medical device software – that could be inter-connected with another medical technology owned by the healthcare provider or even with an app.[215]

Even in the cases where data cannot be directly accessed by the user, the **data holder** shall **make available to the user the data generated** by its use of a product or related service, free of charge and, where applicable, continuously and in real-time.[216] The same provision of the Data Act proposal tackles and applies some exemptions when it comes to trade secrets. In any case, where the user is not a data subject, any personal data generated by the use of the product or related service shall only be made available by the data holder to the user when there is a **valid legal basis.** Article 4(5) mentions consent for general categories of personal data and all the conditions set by Article 9 of the GDPR.

Finally, Chapter II of the Data Act proposal includes some provisions on data sharing with third parties (also referred to as **data portability**).[217] If a user requests it[218], the data holder shall make available the data generated by the use of a product or service to a third party – without undue delay, free of charge, of the same quality as is available to the data holders and where applicable, continuously and in real-time.

3.3.5. Business to government data sharing

Rules on business-to-government data sharing are foreseen under Chapter V of the Data Act proposal. Article 14 of the proposed Regulation sets up obligations for the data holders to make data available whenever, upon request; a public sector body demonstrates an **exceptional need to use the data requested.** The Data Act proposal considers 'exceptional need' in the occurrence of one of the following circumstances.[219]

---

[212] Data Act proposal, art 3.

[213] The proposal needs to undergo through the all necessary steps of the legislative process, therefore the final text could be different from the initial text.

[214] Data Act proposal, art 3(1).

[215] See 'Medtronic Enables Pacemaker Monitoring by Smartphone' (*Healthcare IT News*, 20 November 2015) <https://www.healthcareitnews.com/news/medtronic-enables-pacemaker-monitoring-smartphone> accessed 8 March 2023.

[216] AI Act proposal, art 4(1).

[217] Data Act proposal, art 5.

[218] Or a party acting on behalf of the user. *ibid.*

[219] Data Act proposal, art 15.

The first one consists of the data request to **respond to a public emergency**. The second would be that the data request is limited in time and scope and necessary to **prevent** a public emergency **or to assist the recovery from a public emergency**. The third occurs when the **lack of available data** prevents the public sector body from fulfilling a specific task in the public interest explicitly provided by the law. For this third one, however, two additional disjunctive conditions apply. Either the public sector body has been unable to obtain such data through alternative means, or obtaining the data with this procedure would substantively reduce the administrative burden for the data holders or other enterprises.[220]

This chapter becomes relevant within the in silico technologies environment because certain data (one may hypothesise, research data) may become useful to help those facing a health emergency – which is an example of an exceptional need for the public sector bodies. In fact, **public health emergencies** are regarded as 'public emergencies' within the proposal's recitals.[221] Finally, it is interesting to notice that the current definition of '**public sector body**' encompasses 'national, regional or local authorities of the Member States and bodies governed by public law of the Member States or associations formed by one or more such authorities or one or more such bodies'.[222] This provision seems broad enough to open the possibility that, in some cases, even developers of *in silico* technologies could also qualify as public sector bodies, inasmuch they are bodies governed by public law (e.g. a hospital, a university in certain Member States). Therefore, not only – as one could *prima facie* expect – could these stakeholders qualify as data holders obliged to make data available; they could also be 'on the other side', requesting data to respond to a public emergency. The latter case, nevertheless, will ultimately depend also on how public law regulates certain public entities in the territories of the Member States.

4. Clinical Trials, Medicinal Products and Medical Devices

4.1. Selected aspects of clinical trials and medicinal products regulation for in silico trials

4.1.1. The use of AI in the development of medicinal products

The technical, legal and regulatory landscape for **digital technologies**[223] in medicines development is rapidly evolving. Digital technologies are becoming part of some existing processes in clinical trials. For example, AI is used for patient monitoring for clinically relevant parameters, the electronic data capture of laboratory values, digital/remote monitoring of drug intake, and electronic signature on consent forms.[224] There are several ways where AI may have potential in the product lifecycle:[225]

[220] *ibid*.

[221] Data Act proposal, rec 57.

[222] Data Act proposal, art 2(9). The same public emergencies should be determined according to the respective procedures in the Member States; therefore, national implementations may influence this aspect

[223] This section adopts the wording 'digital technologies' as meant by EMA in its guidance document. See European Medicines Agency, 'Questions and Answers: Qualification of Digital Technology-Based Methodologies to Support Approval of Medicinal Products' (2020) 4. In essence, while the focus of these sections will concern novel methodologies for drug development, digital technologies can be used in the context of medicinal product development and can influence, even potentially, the benefit-risk assessment of a Marketing Authorisation Application (MAA).

[224] European Medicines Agency, 'Questions and Answers: Qualification of Digital Technology-Based Methodologies to Support Approval of Medicinal Products' (n 223).

[225] Philip A Hines and others, 'Artificial Intelligence in European Medicines Regulation' (2023) 22 Nature Reviews Drug Discovery 81.

- In **preclinical settings**, AI could be used for **drug discovery** (for instance, predicting molecular interactions and pharmacokinetics/pharmacodynamics).[226] AI could also be used in **protocol, study design, recruitment**, and patient cohort composition.[227]
- In **clinical evidence generation**, AI could help **generate evidence for regulatory assessment**[228] or optimize patient populations (for instance, to predict the relationships between different patients' characteristics and a medicine's safety and efficacy).[229]
- In **clinical use**, to support medicine administration (for example, a digital insulin pump using AI as part of its administration).[230]
- During **manufacturing**, for example, to predict the outcomes of process or reagent changes and continually improve production.[231]
- During **pharmacovigilance**, to classify individual case safety reports,[232] screen academic literature, optimize medical treatment process and screen real-world data.
- In the **post-authorisation management**, in repurposing (for example, to screen real-world data and suggest changes to dosing or patient population).

In silico trials and technologies may play a role in many aspects mentioned above. Evidence generation for regulatory assessment is at the core of *in silico trials.* The following sections will analyse this aspect, with a focus on the existing EU/EMA regulatory pathways for evidence generation through *in silico* trials, which are related to the issue of '**novel methodologies for drug development**'.

4.1.2. The legal basis concerning novel methodologies for drug development

The legal basis concerning novel methodologies for drug development may be primarily found in Regulation 726/2004 on authorisation procedures and establishing EMA.[233]

Title IV establishes and regulates the administrative structure of the EMA, its tasks and responsibilities. Concerning the **administrative structure**, article 56 enlists the main entities that the Agency shall comprise,

[226] Sheela Kolluri and others, 'Machine Learning and Artificial Intelligence in Pharmaceutical Research and Development: A Review' (2022) 24 The AAPS Journal 19; E Hope Weissler and others, 'The Role of Machine Learning in Clinical Research: Transforming the Future of Evidence Generation' (2021) 22 Trials 537; Radek Kaminski, 'AI in Pharma. What Does Artificial Intelligence Bring to the Pharmaceutical Industry?' (*Nexocode*, 2 March 2021) <https://nexocode.com/blog/posts/ai-in-pharma/> accessed 7 December 2022.

[227] Stefan Harrer and others, 'Artificial Intelligence for Clinical Trial Design' (2019) 40 Trends in Pharmacological Sciences 577.

[228] Tina M Morrison and others, 'Advancing Regulatory Science With Computational Modeling for Medical Devices at the FDA's Office of Science and Engineering Laboratories' (2018) 5 Frontiers in Medicine 1; Francesco Pappalardo and others, 'In Silico Clinical Trials: Concepts and Early Adoptions' (2019) 20 Briefings in Bioinformatics 1699.

[229] Hines and others (n 225); Harrer and others (n 227).

[230] Hines and others (n 225).

[231] Dorota Owczarek, 'The Future of Pharmaceutical Manufacturing Process: Artificial Intelligence' (*nexocode*, 7 July 2021) <https://nexocode.com/blog/posts/ai-in-pharmaceutical-manufacturing/> accessed 8 December 2022.

[232] Hines and others (n 225); Reza Ebrahimi Hariry, Reza Vatankhah Barenji and Anant Paradkar, 'Towards Pharma 4.0 in Clinical Trials: A Future-Orientated Perspective' (2022) 27 Drug Discovery Today 315.

[233] Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency [2004] OJ L136/1 (hereinafter Regulation 726/2004).

including the Committee for Medicinal Products for Human Use (CHMP)[234], the Pharmacovigilance Risk Assessment Committee (PRAC), the Committee for Veterinary Medicinal Products (CVMP), the Committee on Orphan Medicinal Products, the Committee on Herbal Medicinal Products, the Committee for Advanced Therapies, the Paediatric Committee, a Secretariat, an Executive Director and the Management Board. Concerning the **tasks and responsibilities** for the purposes of *in silico* trials is worth analysing Article 57 Regulation 726/2004. According to this article, the EMA is established to provide the Member States and the EU with 'the best possible scientific advice on any question relating to the evaluation of the quality, safety and efficacy of medicinal products for human use or veterinary medicinal products'.[235] The same paragraph provides a list of tasks carried out by the EMA, one of which – the most relevant for *in silico* trials – is **advising undertakings on the conduct of the various tests and trials** necessary to demonstrate the quality, safety, and efficacy of medicinal products for human use and of veterinary medicinal products.[236] For the development of advice for undertakings, Article 56(3) Regulation 726/2004 foresees that the EMA Executive Director, in consultation with the CHMP and CVMP, may set up administrative structures and procedures, including **advice on the use of novel methodologies and tools in research and development** and committees shall establish a standing working party for this purpose, with the sole remit of **providing scientific advice to undertakings.**[237]

In light of this, the EMA foresees a **voluntary scientific procedure** to establish the **regulatory acceptability** for novel methodologies for developing medicinal products. The EMA **Committee for Medicinal Products for Human Use** (CHMP) is qualified to issue opinions on the acceptability of a specific use or method, including those involving a novel methodology such as those entailed by *in silico* trials. In August 2014, the EMA and the CHMP established an internal EMA horizontal cross-sectorial group, the EMA **Innovation Task Force** (ITF).[238] The ITF represents a discussion platform for early dialogue with applicants on emerging therapies and technologies.

The aspects concerning the regulatory acceptability for using novel methods are further substantiated in the recent guidance provided by the EMA. The first guidance produced by the EMA on this matter is the 2009 '**Qualification of novel methodologies for drug development**'.[239] Others followed this: in 2017, the EMA published the 'Essential considerations for successful qualification of novel methodologies';[240] in 2020, the EMA issued Q&As on the **qualification of digital technology-based methodologies to support the approval of medicinal products.**[241]

The documents refer to the "**qualification process**" as the scientific pathways leading to a CHMP qualification opinion or advice concerning innovative methods or drug development tools. One applicant may seek a

[234]The CHMP in general plays a fundamental role within the medicines authorisation process, as it is the committee responsible for human medicines. Within the medicines' centralised procedure, it is responsible for conducting the initial assessment of EU MAAs, assess their modifications or extensions, considering recommendations on the safety of medicines. The CHMP bases its assessments on a comprehensive scientific evaluation of data. They decide if a medicine fulfils the quality, safety and efficacy requirements and it has a positive risk-benefit balance European Medicines Agency, 'Committee for Medicinal Products Human Use (CHMP)' (*European Medicines Agency*, 17 September 2018) <https://www.ema.europa.eu/en/committees/committee-medicinal-products-human-use-chmp> accessed 1 April 2023.

[235] Regulation 726/2004, art 57(1).

[236] Regulation 726/2004, art 57(1)(n).

[237] Regulation 726/2004, art 56(3), second part.

[238] European Medicines Agency, 'Mandate of the EMA Innovation Task Force (ITF)' (2014).

[239] European Medicines Agency, 'Qualification of Novel Methodologies for Drug Development: Guidance to Applicants' (2009).

[240] European Medicines Agency, 'Essential Considerations for Successful Qualification of Novel Methodologies' (2017).

[241] European Medicines Agency, 'Questions and Answers: Qualification of Digital Technology-Based Methodologies to Support Approval of Medicinal Products' (n 223).

qualification opinion which will concern the acceptability of a specific use of the proposed method (such as a novel methodology) in a research and development (R&D) context (non-clinical or clinical studies); or, the applicant may ask for a **qualification advice**, which will be about future protocols and methods for further method development towards qualification.[242]

The first document issued in 2009 guides applicants for the qualification of novel methodologies for drug development. It establishes the main terms of references, the operations, fees, interaction and the expected output of the procedure. Furthermore, it sets out the **procedure** for submitting a qualification opinion or advice and includes a draft proposed **format** for the applicants' requests. For example, it enlists a table of contents, an executive summary tackling the objective or the request, the need and impact of proposed novel technologies, characteristics of proposed novel methodologies, Context of Use for which qualification is requested, sources of data and major findings, remaining gaps and conclusion.[243]

The Q&As guidance of 2020 further supports applicants using methodologies based on digital technologies in developing medicinal products.[244] For instance, it clarifies that the EMA may be **consulted in advance of a planned submission** in the form of scientific advice pre-submission, ITF pre-discussion, and regulatory-only questions.[245] Further, it clarifies the **content of a request for qualification advice/opinion,** considerations regarding the **Context(s) of Use** of a digital technology, **clinical usefulness,** and **best practice** guides**.**

4.1.3. The current state of the art of *in silico* trials for medicinal products

In silico trials insist on a rapidly evolving regulatory landscape. The EMA strongly encourages stakeholders to engage in the process of drug development and regulatory science, and several schemes are in place at EMA to support the process.[246] Existing guidance encourages or supports applicants in engaging with the authority from the early stages of drug development. In its 2020 Q&A guidance, the EMA (mirrored by Cerreta and others[247]) provided **insights to facilitate the qualification processes** for the submission of marketing authorization applications (MAAs) making use of digital technologies to support regulatory decision-making, such as:

- **Timing**: It is recommended that developers start interaction with the EMA at the earliest stages. This helps identify the most appropriate regulatory interactions to achieve the applicant's objectives and efficient data exchanges.
- **Research question**: There are some formal and substantial requirements worthy of consideration when identifying a research question. For example, it is essential to make clear which components of technology fall under the EMA's competence and which that are not; the concept of interest, the context of use and the identification of a clinically meaningful change; the benefits of using digital measures instead of the existing methods.[248]

---

[242] European Medicines Agency, 'Qualification of Novel Methodologies for Drug Development: Guidance to Applicants' (n 239).

[243] ibid 10.

[244] European Medicines Agency, 'Questions and Answers: Qualification of Digital Technology-Based Methodologies to Support Approval of Medicinal Products' (n 223) 3. The guidance does not define or provides a precise definition or an exhaustive list of specific use of methodologies as it could have resulted in the exclusion of innovative approaches.

[245] ibid 5.

[246] Flora T Musuamba and others, 'Scientific and Regulatory Evaluation of Mechanistic *in Silico* Drug and Disease Models in Drug Development: Building Model Credibility' (2021) 10 CPT: Pharmacometrics & Systems Pharmacology 804.

[247] Francesca Cerreta and others, 'Digital Technologies for Medicines: Shaping a Framework for Success' (2020) 19 Nature Reviews Drug Discovery 573, 574.

[248] ibid 2.

- **Documentation**: Documentation should be appropriately set up. It should offer 'insights about the methodology's reliability, repeatability, accuracy and clinical applicability to be qualified'.[249] In the MAA, the applicant should provide a 'risk assessment of the impact on the validity of the supporting clinical data of any changes introduced to the final digital technology element during development'.[250]
- **Additional requirements**: where the digital tools submitted under regulatory evaluation are medical devices or in vitro medical devices, the applicant is expected to comply with existing requirements, e.g. from the MDR/IVDR. If personal data is processed, compliance with GDPR is expected, too.
- **Developing best practices, with input from users**: applicants should set up a user guide for patients or healthcare professionals and explain the methodology's key points.

4.1.4. Avenues for in silico trials

However, notwithstanding the existing references in the above state of the art and regulations, there are few challenges that need to be addressed for the advancement of the *in silico* trials regulatory pathways. The core regulatory challenge of *in silico* trials for medicinal product development is the lack of specific guidance documents on **reporting, verification and validation** of *in silico* models for development and approval.[251] Some experts of the *in silico* trials community are of the opinion that a framework similar to the one existing in ASME V&V40 in the domain of medical devices could and should be used to guide the **evaluation process of models and associated simulation** in a holistic and comprehensive manner. [252] Its adoption could help increase the rigour and transparency of the methods used for model development and validation. There is a **lack of international standards, best practices and regulatory guidance in that respect**, and ASME V&V40 (in its analogous use) for medicinal products, is deemed appropriate to meet the need of the EU and relevant international stakeholders.[253]

Beyond the regulatory technicalities, further and broader considerations are worth mentioning from the legal framework side. The **EU Pharmaceutical Strategy for Europe**, released by the European Commission in November 2020, puts a strong accent on AI-related aspects of the pharmaceutical sector. Concerning clinical trials, the document comments, for example, that the Clinical Trials Regulation '**will address** new developments such as adaptive and complex trials, and the use of **in-silico techniques** and virtual approaches'.[254] Most notably, the document specifies that the Commission will propose to **revise the pharmaceutical legislation** to address new developments in digital transformation, including **new methods of evidence generation and assessment**, such as analysis of big and real-world data to support the development, authorisation and use of medicines. Therefore, one could reasonably expect significant developments towards

[249] ibid.

[250] ibid.

[251] Flora T Musuamba and others, 'Verifying and Validating Quantitative Systems Pharmacology and *In Silico* Models in Drug Development: Current Needs, Gaps, and Challenges' (2020) 9 CPT: Pharmacometrics & Systems Pharmacology 195.

[252] See Musuamba and others (n 246). The authors propose that the needed framework should be needed to the ASME V&V40 framework for medical devices. See *Assessing the Credibility of Computational Modeling through Verification and Validation: Application to Medical Devices* (American Society of Mechanical Engineers 2018).

[253] The ISW partners have extensively provided scientific work to maintain this argument For an example, see Cristina Curreli and others, 'A Credibility Assessment Plan for an In Silico Model That Predicts the Dose–Response Relationship of New Tuberculosis Treatments' (2023) 51 Annals of Biomedical Engineering 200.

[254] Emphasis added. See Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions' COM(202) 761 final, 13.

in silico trials from the forthcoming pharmaceutical legislation – whose proposal might be put forward during the second half of 2024.[255]

4.2. Selected aspects of medical device regulation for in silico trials

4.2.1. The MDR: overview and main requirements

The EU legal framework on medical devices is mainly composed of the Medical Device Regulation (MDR) [256]and the In Vitro Diagnostic Regulation (IVDR)[257]. The first concerns medical devices, the second in vitro diagnostic medical devices. The **MDR/IVDR** are two risk-based regulations[258] aiming to ensure the smooth functioning of the internal market as regards medical devices.[259]

They set quality and safety standards for medical devices in order to meet common safety concerns for such products.[260] In this perspective, the MDR develops harmonised rules for placing on the market and putting into service medical devices and their accessories in the Union. The EU body **Medical Device Coordination Group (MDCG)** interpretates its rules and issues non-binding documentation on specific issues concerning medical devices and in vitro medical devices. Health authorities in their respective national territories may provide additional guidance. Other transnational sources are relevant to the framework of EU medical devices. Worth mentioning is the documentation provided by the International Medical Device Regulators Forum (IMDRF), which influences the guidance issued by EU regulators and national authorities, and the documents provided by the World Health Organisation (WHO).

To be placed on the market, a medical device shall meet the general safety and performance requirements that are set out in Annex I of the MDR.[261] As part of their general obligations, the manufacturer must adopt a quality management system,[262] which is audited during the **conformity assessment**. The manufacturer shall demonstrate the device's conformity with the general safety and performance requirements.[263] Once these are demonstrated, the manufacturer may obtain a **CE marking** for the medical devices.[264] Harmonised standards play a fundamental role in medical device compliance. Devices that comply with the relevant harmonised standards, or the relevant parts of those standards, shall be presumed to be in conformity with the requirements of the MDR.[265] To verify the **safety and performance** of a medical device, manufacturers

---

[255] Gerardo Fortuna, 'EU Pharma Reform Delayed Again Due to Commission's Busy Agenda – EURACTIV.Com' (*EURACTIV*, 22 March 2023) <https://www.euractiv.com/section/health-consumers/news/eu-pharma-reform-delayed-again-due-to-commissions-busy-agenda/> accessed 3 April 2023.

[256] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L117/1 (MDR).

[257] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L117/176 (IVDR).

[258] On medical device law and risk-based regulation, see also Anthony Wilkinson, 'Medical Device Regulation and Litigation: A Comparative Analysis of Australia, the United Kingdom and the United States of America' (PhD, Queensland University of Technology 2021) <https://eprints.qut.edu.au/209677> accessed 14 September 2022.

[259] MDR, rec 2.

[260] *ibid*.

[261] MDR, art 5(2).

[262] MDR, art 10.

[263] MDR, art 5(3).

[264] MDR, art 20.

[265] MDR, art 8.

shall conduct a clinical evaluation.[266] Moreover, manufacturers of devices shall draw up and keep up-to-date technical documentation, which shall include the elements set out in Annexes II and III of the MDR.

Annex I of the MDR contains the general **safety and performance requirements** for medical devices. Annex I, namely, includes general requirements[267], design and manufacture requirements[268], and requirements regarding the information supplied with the device (labelling and instructions for use)[269].

As per the **general requirements**, devices shall achieve the performance intended by their manufacturer and shall be designed and manufactured in such a way that are suitable for their intended purpose. They shall be safe and effective and not compromise the clinical condition or safety of patients, users or other persons. Any risks associated with their use should constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety.[270] The same Annex details the risk management system requirements, which manufacturers are called to adopt within the medical device lifecycle. Chapter II of Annex I contains requirements regarding **design and manufacturing**, including those about security measures and medical device software. Chapter III concerns the requirements regarding the **information** supplied with the device. Annex II is about the elements that the **technical documentation** of medical devices should include (for example, the device's description and specification or the product's verification and validation).

4.2.2. The IVDR: overview and main requirements

The second core piece of legislation on medical devices is the IVDR. **In vitro diagnostic medical devices** have a different definition from the medical devices' in the MDR.[271] In vitro medical devices are, for example pregnancy tests, SARS-CoV-2 rapid tests, or insulin devices. Obligations of the manufacturer stemming from the IVDR include, similarly to the MDR, the establishment, implementation and maintenance of a risk management system, as well as technical documentation. Differently from the MDR, which is centred around clinical evidence, the IVDR requires the manufacturers to conduct a '**performance evaluation**'.[272] They shall apply a conformity assessment procedure, and once they have fulfilled their obligations, manufacturers may draw up a declaration of conformity and apply CE marking to the devices. In vitro devices were formerly regulated via Directive 98/79/EC about in vitro diagnostic medical devices.[273] Following the MDR/IVDR recast, the new IVDR introduced some substantial changes. Among the core aspects, the IVDR increased the

[266] MDR, art 61. A clinical evaluation is a 'systematic and planned process to continuously generate, collect, analyse and assess the clinical data pertaining to a device in order to verify the safety and performance, including clinical benefits, of the device when used as intended by the manufacturer' (MDR, art 2(44)).

[267] MDR, Annex I, ch I.

[268] MDR, Annex I, ch II.

[269] MDR, Annex I, ch III.

[270] MDR, Annex I, req 1.

[271] see art 2(2) IVDR 'any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following: (a), concerning a physiological or pathological process or state; (b), concerning congenital physical or mental impairments; (c), concerning the predisposition to a medical condition or a disease; (d), to determine the safety and compatibility with potential recipients; (e), to predict treatment response or reactions; (f), to define or monitoring therapeutic measures.'

[272] IVDR, art 56.

[273] Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices [1998] OJ L331/1.

involvement of notified bodies, proposed a new device reclassification rule in line with international guidance, and extended its scope to include, for instance, diagnostic services.[274]

The general safety and performance requirements for in vitro diagnostic devices are included in Annex I of the IVDR. The annex includes general requirements (Chapter I). For example, Requirement 1 mandates that devices shall achieve the performance intended by their manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, they are suitable for their intended purpose. Requirement 2 sets rules about risks management systems obligations. Other chapters concern performance, design and manufacturing requirements (Chapter II); requirements regarding the information supplied with the device (Chapter III). The remaining Annexes concern technical documentation (II and III), declaration of conformity and CE marking (IV and V), classification rules (VIII), conformity assessments (IX, X, XI), performance evaluation, performance studies, and post-market performance follow up or other performance studies (XIII, XIV).

4.2.3. The current state of the art of *in silico* trials applied to medical devices

The current regulatory situation about medical devices for ***in silico* trial solutions** is complex.[275] From the MDR and theorical level, it can be observed that the regulation *per se* does not prohibit using **evidence** generated through computer modelling and simulation.[276] In the **MDR Annexes**, **computer modelling and simulation** are mentioned in some requirements. Computer modelling is present in Annex VII in the requirements for notified bodies for the pre-clinical evaluation assessment. There, the MDR states that:

> 'the notified body shall examine, validate and verify that manufacturer's procedures and documentation adequately address the planning, conduct, assessment, reporting and, where appropriate, updating of pre-clinical evaluation, in particular of (…) the preclinical testing, for example laboratory testing, s*imulated use testing, computer modelling*, the use of animal models' (emphasis added).[277]

More plainly, notified bodies in their pre-clinical evaluation assessment could evaluate the documents that the manufacturers present about **pre-clinical testing**, which could include simulated use testing and computer modelling.

Further, Annex II on technical documentation mentions **simulation** as part of the requirements of product verification and validation. According to Requirement 6, the product documentation shall contain the results and critical analysis of all verification and validation tests and/or studies undertaken to demonstrate conformity of the device. Requirement 6.1 includes in pre-clinical and clinical data 'results of tests, such as engineering, laboratory, *simulated use* and animal tests'.[278] As pre-clinical/clinical data on software verification and validation contemplate, *inter alia*, the testing in a simulated environment prior to final release.[279]

Modelling (**modelling** research) is also referred to in Annex I, Chapter II, under the requirements regarding design and manufacture for certain medical devices (namely, requirements 10: 'Chemical, physical and

[274] These are genetic tests and other tests providing information on the predisposition of patients to develop a disease or on sensitivity to medical therapy. See IVDR, art 2.

[275] This section analyses the specific issue of medical products whose regulatory scrutiny happen through evidence generated via in silico trials solutions. In their recent position paper, Pappalardo and others explain comprehensively the current state of the art. See Francesco Pappalardo and others, 'Toward A Regulatory Pathway for the Use of in Silico Trials in the CE Marking of Medical Devices' (2022) 26 IEEE Journal of Biomedical and Health Informatics 5282.

[276] ibid 5283.

[277] MDR, Annex VII, req 4.5.4.

[278] MDR, Annex II, req 6.1.

[279] MDR, Annex II, req 6.1.(b).

biological properties'). Requirement 10.1 mandates that devices must be manufacturers shall be designed and manufactured as to fulfill the MDR general requirements, and 'particular attention shall be paid to (…) where appropriate, the results of biophysical or modelling research the validity of which has been demonstrated beforehand' (emphasis added).[280]

4.2.4. Avenues for *in silico* trials

The current medical devices legal framework does not exclude the use of *in silico* trials. On the contrary, computer **modelling and simulation are mentioned** in some of the requirements of the MDR. This means that there is a possibility of submitting modelling and simulation data to Notified Bodies within the regulatory approval process. Nevertheless, the actual status of implementation has not reached a level of maturity, allowing legal certainty for the execution of *in silico* trials on medical devices.[281]

In other words, the adoption of *in silico* trials in the regulatory certification of new medical devices is **not uniform**. While in the United States the Food and Drug Authority (FDA) has an established regulatory pathway for the qualification for in Silico methodologies to be used to produced regulatory evidences for medical devices – a pathway largely based on the **ASME VV40:2018** technical standard – **in the EU, use of modelling and simulation in the certification process is currently limited to the refinement or reduction of in vitro preclinical experiments**.

In practice, notified bodies do accept in some cases *in silico* evidences to optimise or select the worst case for in vitro experiments. [282] The In Silico World project, in collaboration with the Avicenna Alliance, is working toward an alignment with the USA system, so that also for the CE-marking companies can used models assessed using the ASME VV40. However, it should be noted that in the European Union no qualification for new methodologies exist for medical devices; such evaluation is provided by EMA, but only for methodologies for drug development. This implies that companies should produce evidence of models' credibility as part of the new device submission.

Finally, both at the EU level and internationally, many **questions remain open**– as the Avicenna Alliance points out, which are: 'How should models be verified and validated? Who will be reviewing and assessing the simulation results, and following which approval process? What standard requirements should medical device [manufacturers] meet when submitting CM&S data to support a market authorization or when seeking reimbursement?'[283] Therefore, given the existing references in the MDR, and the increasingly use of AI-based technologies for the development of medical products, **the existing EU regulatory entities should consider producing *ad hoc* guidance for evidence generation through *in silico* trial solutions**.

[280] MDR, Annex I, req 10.1.(e).

[281] For example, Pappalardo and others report they have no knowledge of whether any EU notified body has accepted in silico evidence in recent regulatory submissions for medical devices. Pappalardo and others (n 275). Furthermore they point out, *inter alia,* the lack of an 'harmonized standard to demonstrate the credibility of an In Silico Trial solution, which the America Society of Mechanical Engineers Verification & Validation 40 (AMSE VV-40) provides'.

[282] For example various manufacturers now replace a whole experimental campaign based on the ISO 7206-4 experimental protocol with a model prediction based on the ASTM F2996 "Standard Practice for Finite Element Analysis (FEA) of Non-Modular Metallic Orthopaedic Hip Femoral Stems" to choose the experimental conditions to conduct a single pass-fail experimental test, so reducing the number of experiments.

[283] Avicenna Alliance, 'Modelling and Simulation as a Transformative Tool for Medical Devices: The Transatlantic Regulatory Perspective' (2018) 6.

5. Artificial Intelligence

5.1. The AI Act proposal

5.1.1. An evolving framework

The EU legal framework regulating Artificial Intelligence has been rapidly evolving. D9.1 described the EU policy-making initiatives that preceded the AI Act proposal, which was released in April 2021. At the moment of writing, the AI Act proposal seems to be at the final stages of negotiations at the EU policy level. This report will consider the latest publicly available version, i.e. the compromise proposal tabled by the Council of the EU in November 2022 and published in December 2022.[284]

5.1.2. The AI Act proposal: subject matter and material scope

The AI Act proposal laws down harmonised **rules for the placing on the market, the putting into service and use AI systems** in the Union. It prohibits certain artificial intelligence practices[285], and it sets specific requirements for **high-risk AI systems** and obligations for such systems, including rules on market monitoring market surveillance and governance.[286] The regulation applies to providers of AI systems, users of AI systems, their importers and distributors, product manufacturers and authorised representatives.[287]

At the moment of writing, there is lively discussion about the final **definition of an 'AI system'**. The December version of the AI Act defines the AI system as 'a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as a content (generative AI systems) predictions, recommendations or decisions, influencing the environments with which the AI system interacts'.[288] The definition lets us assume easily that *in silico* tools may fall under the definition of the AI Act. A medical device software simulating the effects of a given medicinal product could qualify as an AI system. An AI-based tool that virtually simulates new compounds for medicinal products may also fall under the definition, regardless of whether it processes personal data or raw personal data.

The new compromise text also includes a definition of '**general purpose AI system**', which is 'an AI system that – irrespective of how it is placed on the market or put into service, including as open source software – is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others; a general purpose AI system may be used in a plurality of context can be integrated in a plurality of other AI systems'.[289] General purpose AI may also be relevant in certain healthcare applications. For example, question-answering systems could be used in an app to detect certain symptoms. The proposal requires that general purpose AI systems

[284] Council of the EU, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (2021/0106(COD)), 25 November 2022 (hereinafter AI Act proposal (Council)).

[285] The regulation differentiates between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk. See Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (2021/0106(COD)) (AI Act proposal Commission)), 21 April 2021, Explanatory Memorandum, 12.

[286] AI Act proposal (Council), art 1.

[287] ibid, art 2.

[288] ibid, art 3(1).

[289] ibid, art 1b.

shall only comply with certain requirements, depending whether they are used as high risk systems or as components of high risk AI systems.

5.1.3. Focus: The main requirements

The AI Act proposal includes a list of **prohibited artificial intelligence practices**. These include AI systems deploying subliminal techniques, AI practices exploiting vulnerabilities, social scoring systems and 'real time' remote biometric identification systems.[290]

After that, the proposal includes **classification rules** for AI systems as high-risk.[291] Annex III of the text includes a list of systems considered high-risk.[292] AI systems that are themselves products or safety components of the product are classified as high-risk systems if the product undergoes a conformity assessment procedure with a third-party conformity assessment body according to EU legislation.[293] Therefore, as also Recital 30 of the Council proposal clarifies, **medical devices and in vitro diagnostic medical devices** are in the scope of the legislation. These may be considered high-risk products for the purposes of the AI Act (but not as high-risk within the MDR/IVDR laws).[294]

The proposal includes **risk management requirements** for high-risk AI systems.[295] High-risk AI systems involving the training of models with data shall be developed on the basis of training, **validation and testing data sets** according to the specific criteria delineated in Article 10 of the Council proposal. For medical devices, the current version of the text seems to add further elements to those foreseen by medical device laws and regulatory instruments. Further, the proposal sets technical documentation, record keeping, transparency and requirements. Article 14 of the proposal adds human oversight rules, while Article 15 regulates the accuracy, robustness and cybersecurity of high-risk AI systems.

The **obligations of providers of high-risk AI systems** will include ensuring compliance with the risk management requirements, having a quality management system in place, complying with documentation duties, ensuring the execution of a conformity assessment procedure before placing on the market, registration obligations, taking corrective actions, affix CE marking.[296] **Users of high-risk AI systems** will have to use the systems in accordance with the instructions of use accompanying the system; they implement human oversight requirements, and comply with registration obligations. Similarly to medical device legislation, AI legislation establishes **notified bodies** and notification procedures. On the same note, systems that are in conformity with **harmonised standards** or parts thereof are presumed to be in conformity with the relevant requirements of the AI Act, and the Commission retains the capacity to issue **common specifications**.

5.1.4. Open discussions about the AI Act proposal

There are several open discussions on the AI Act proposal, which could not be treated extensively in this report. However, there is a new crucial point of the most recent version of the AI Act proposal that should deserve more attention. It concerns the application of the AI Act for **AI systems in scientific research**.

---

[290] See Rostam Josef Neuwirth, 'Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act' [2022] SSRN Electronic Journal <https://www.ssrn.com/abstract=4261569> accessed 3 April 2023.

[291] AI act proposal (Council), Title III.

[292] 'Unless the output is purely accessory in respect of the relevant action or decision to be taken and is not therefore likely to lead to a significant risk to health, safety or fundamental rights'; ibid, art 6(3).

[293] ibid, rec 30.

[294] ibid, rec 31.

[295] ibid, art 9.

[296] ibid, art 16.

Article 2(6) of the proposal excludes the applicability of the regulation to 'AI systems, including their output, specifically developed and put into service for the sole scope of scientific research and development'. The seventh paragraph states that the Regulation shall not apply 'to any research and development activity regarding AI systems'.[297]

Further, the current recital 12b states that the Regulation should not undermine research and development activity and should respect freedom of science.[298] 'It is, therefore, necessary to exclude from its scope AI systems specifically developed and put into service for the sole purpose of scientific research and development'.[299] The recital adds that the above is without prejudice if an AI system is placed on the market or put into service as a result of such research. These rules should apply **without prejudice to** applying provisions on **regulatory sandboxes and testing in real-world conditions.** Finally, the recital states that 'any other AI system that may be used for the conduct of any research and development activity should remain subject' to the provision of the AI Act.[300] In other words, if the AI system is not developed for *the sole purpose* of scientific research and development, then the AI Act would apply.

It might be early to comment on this specific aspect of the AI Act. As a preliminary comment, it might be noted that the notion of scientific research is not defined in the AI Act proposal itself – meaning that scientific research could be intended very broadly. Secondly, it might be difficult to draw the line between the purpose and the 'sole purpose' of scientific research and it might be unclear in that respect for AI system providers. As it stands, the provision is likely to create more legal uncertainty than certainty.

6. Ethics Principles

6.1. Practical application of the biomedical ethics principles for in silico trials

6.1.1. Autonomy

The **autonomy principle** is the first of the four principles of Biomedical Ethics.[301] The principle implies that the moral decision-making of rational agents shall be based on an informed and voluntary decision. It consists of the **negative obligation not to interfere in a patient's choice** and the positive obligation to provide appropriate information to make informed decisions.[302] The substantiation of this principle consists in telling the truth, respecting the privacy of others, protecting confidential information, obtaining consent for interventions with patients, and, when asked, helping others make important decisions.[303] In healthcare, the principle of autonomy is often associated with **privacy** and informed consent – both of which may be seen as intrinsically related to an individual's fundamental right of **self-determination**.[304] Conceptions of autonomy

[297] ibid, art 2(7).

[298] ibid, rec 12b.

[299] ibid.

[300] ibid.

[301] This section follows the analysis carried out in D9.1, section 7 'Ethics Principles'. The principles identified by the High Level Expert Group on Trustworthy AI and depicted in D9.1, section 6 'Artificial Intelligence', will be further scrutinised in D9.3 'Implementation guidance and guidelines'.

[302] Tom L Beauchamp and James F Childress, *Principles of Biomedical Ethics* (5th ed., New York : Oxford university press 2001) 64.

[303] Biasin, 'In Silico World D9.1 Legal and Ethical Inventory' (n 1) 41.

[304] For an exploration of the concept of autonomy vis-a-vis the moral duty to share health data, see Vedder and Spajić (n 86). For an exploration of autonomy in the new data legislation, including the Data Act proposal, see M Gartner, 'Regulatory Acknowledgment of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act' (2022) 8 European Data Protection Law Review 462.

are closely connected to those of identity and individuality. In the case of *in silico* technologies, an individual's self-determination could be influenced by the results rendered by data-driven or AI-based profiles. Let us consider the following:

> Example: An *in silico* technology reproduces a digital twin of an individual through the processing of personal data. The processing of personal data is based on the collection from eHealth devices. The data are processed to form the patient's 'avatar' and health profile.

In this example, there could be a risk that, if the errors are present in the data, inaccuracies could lead to harm, such as wrong diagnoses or improper symptom checking. The 'health profile' of the individual could not correspond to the factual situation, and consequently the ability of the patient to make informed decisions for the benefit of their state of health could be hindered. The principle of autonomy could guide the developer of the *in silico* tool or the healthcare facilities using it in supporting the patient to keep control of their personal data. For example, considering this principle could entail setting up data quality mechanisms for more accurate personal data; security measures to prevent tampering by external malicious actors; or establishing technical and organizational mechanisms to help the healthcare practitioners or patients rectify the **data inaccuracy**, where appropriate.

6.1.2. Beneficence

From an ethical standpoint, morality requires that not only are patients treated autonomously but also to **contribute to the welfare of a patient**. These beneficial actions fall under the **principle of beneficence**. Its duties are viewed as self-evident and accepted as the proper goal of medicine. The principle stands at the core of healthcare, involving that the patient can enter into a relationship with the healthcare provider, trusting that its primary objective is to help. The objective of contributing to welfare can be meant for individual patients but also the good of society as a whole.[305] D9.1 reported that the rules of this principle include the protection and defence of the rights of others; prevention of harm from occurring to others; removal of conditions that will cause harm to others; helping persons with disabilities; rescuing persons in danger.[306]

One possible example of beneficence could be seen the so-called '**incidental findings**'. Incidental findings (also known as 'secondary findings' or 'unexpected findings') consist of previously undiagnosed medical conditions discovered unintentionally and during evaluation for a medical condition. For *in silico* trials, one could imagine the case of an incidental finding brought by AI-powered tools of *in silico* technologies:

> Example: A patient's MRI image is processed to generate an *in silico* model. The data processing for that purpose generates an incidental finding not foreseen during the consent process.[307] The researcher now faces the question of whether it should be communicated to the patient.

Incidental findings are not a new problem in ethical and legal literature.[308] At the international level, the ethical question of informing or not the patient about the incidental findings is not resolved.[309] Regional bodies have

[305] Tom Beauchamp, 'The Principle of Beneficence in Applied Ethics' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Spring 2019, Metaphysics Research Lab, Stanford University 2019) <https://plato.stanford.edu/archives/spr2019/entries/principle-beneficence/> accessed 22 March 2023.

[306] Beauchamp and Childress (n 302) 167.

[307] Treating extensively the whole issue of incidental findings would go beyond the scope of this deliverable. This section, therefore, offers the perspective only from the perspective of beneficence principle, the role of researchers, and their duty to manage incidental findings.

[308] See Susan M Wolf, Jordan Paradise and Charlisse Caga-Anan, 'The Law of Incidental Findings in Human Subjects Research: Establishing Researchers' Duties' (2008) 36 Journal of Law, Medicine & Ethics 361.

[309] For a broad examination, see also Ó Cathaoir and others (n 73).

issued different recommendations based on the type of incidental finding (e.g. in genetics, radiology, etc.).[310] An interesting example of guidance on incidental findings was produced by the Canadian Panel on Research Ethics in 2020, which offered recommendations on 'How to Address Material Incidental Findings'.[311] In some cases, incidental finding policies are addressed by healthcare organizations.[312] In ethics literature, there appears to be a shared sense that researchers bear the responsibility of handling incidental findings.[313] In those circumstances, careful examination of the case is needed, having consideration of the many ethical principles and values involved.

From the researcher's perspective involved in managing the incidental finding identified within the context of *in silico* trials, the principle of beneficence might offer support. The researchers could, in light of the principle, decide to emphasize the concerns towards the enhancement of the **patient's welfare**. With a view to promoting the patient's welfare, the researcher could decide to communicate the incidental finding to the patient. This decision could be seen also in the perspective of fostering **trust** (which the patient is deemed to have) towards the healthcare system. [314] Also, by interpreting the principle of beneficence, the researchers could consider their own ethical decision-making as being part of their **ancillary care obligations** towards the patient.[315] In this view, the researchers could consider the duty of beneficence as the duty to secure patients, maximise their benefits and reduce harm. [316]

6.1.3. Non-maleficence

The principle of non-maleficence consists of the **duty not to harm other persons**. It is often associated with the maxim *Primum non nocere* (first, do no harm), known within the context of the Hippocratic Oath. According to Beauchamp and Childress, the principle of non-maleficence includes the following rules: do not kill; do not cause pain or suffering; do not incapacitate; do not cause offence; do not deprive others of the goods of life.[317] The non-maleficence principle also entails obligations of not imposing **risks** of harm.[318]

---

[310] See eg the European Society of Human Genetics recommendations on behalf of the ESHG Public and Professional Policy Committee and others, 'Whole-Genome Sequencing in Health Care: Recommendations of the European Society of Human Genetics' (2013) 21 European Journal of Human Genetics 580.

[311] Interagency Advisory Panel on Research Ethics Government of Canada, 'How to Address Material Incidental Findings - Guidance in Applying TCPS 2 (2018) Article 3.4' (15 March 2019) <https://ethics.gc.ca/eng/incidental_findings.html?wbdisable=true#a3> accessed 22 March 2023.

[312] See eg John Hopkins Medicine Institutional Review Board, 'Plans for Detecting and Managing Incidental Findings Associated with Research Imaging Procedures' (2016) <https://www.hopkinsmedicine.org/institutional_review_board/guidelines_policies/guidelines/incidental_findings.html> accessed 22 March 2023.

[313] Wolf, Paradise and Caga-Anan (n 308) 5.

[314] In Grossman and Bernat's words '[w]hen an important abnormality is present, the subject trusts that the research will observe it'. Robert I Grossman and James L Bernat, 'Incidental Research Imaging Findings: Pandora's Costly Box' (2004) 62 Neurology 849.

[315] The vulnerability of the patient and the entrustment of their well-being to researchers could be read by researchers as part of their ancillary care obligations. See Henry S Richardson and Leah Belsky, 'The Ancillary-Care Responsibilities of Medical Researchers: An Ethical Framework for Thinking about the Clinical Care That Researchers Owe Their Subjects' (2004) 34 The Hastings Center Report 25.

[316] This section provides one example of potential considerations made by researchers. In other cases, considerations based on the beneficence principle could lead to even an opposite result than the one proposed in this section. The decision process requires a case-by-case basis therefore it is plausible that in other instances the researchers could deem the communication of the incidental finding as not appropriate.

[317] Beauchamp and Childress (n 302) 115.

[318] Biasin, 'In Silico World D9.1 Legal and Ethical Inventory' (n 1) 41.

From this latter obligation, we could carve out an example of the practical application of this principle vis-à-vis **safety risks brought by the lack of security** of data, information systems or devices. In many circumstances, **data insecurity** may bring legal consequences. For example, a data breach usually requires the controller to notify the breach to the data protection authority; a cybersecurity incident in a hospital may require its reporting to the competent authority. Several **ethical aspects** could be entailed, too. Non-maleficence may be linked to safety related to healthcare technologies and security of data. [319]

> Example 1: The data concerning a person's state of health is leaked, and the data in question reveal a health disease for which the individual is stigmatised by the community. The individual may face discriminatory harm from their peers. Their privacy is breached, causing them emotional suffering.
>
> Example 2: A dataset used by an AI-based medical device is poisoned by a cyberattack.[320] Because of the data poisoning, the AI-based medical device functions incorrectly. Results suggested by the device are incorrect, and their predictions are inaccurate, resulting in a misjudgment of a patient's state of health.

Security of data, information systems and devices is fundamental for safety and the protection of patients and to ensure medical confidentiality. The non-maleficence principle, in this case, may provide guidance. For the first one, it could guide the healthcare actors, for example, in ensuring the safety of the data by establishing trusted access control schemes.[321] In the second case, the non-maleficence principle may support healthcare stakeholders of the device manufacturers in setting security requirements for data access and AI safety performance.

Therefore, the consideration of the non-maleficence principle for harm following data or AI insecurity may help healthcare professionals ensure patients' safety and, thus, their health and well-being.

Some authors in the literature have studied cybersecurity aspects against the principlist approach: Loi and others,[322] Weber and Kleine[323]. Those interested in further addressing this compelling issue should consult their studies (see excerpt in Figure 4).[324]

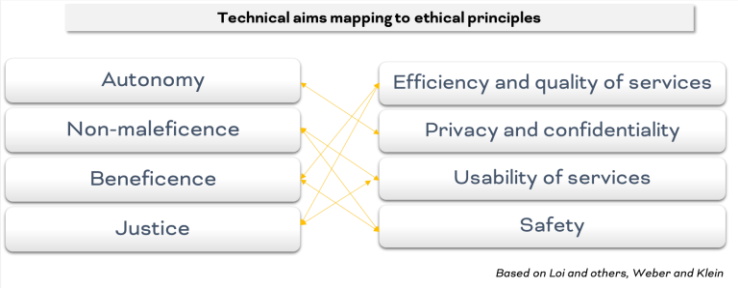

Figure 4 Technical aims mapping to ethical principles

[319] Whereas safety can be defined as the reduction of health-threatening risks and risks to a person's health. See Michele Loi and others, 'Cybersecurity in Health – Disentangling Value Tensions' (2019) 17 Journal of Information, Communication and Ethics in Society 229, 237. On the terminological differentiations between safety and security, see Anton Vedder, 'Safety, Security and Ethics', vol 7 (Intersentia; Cambridge, Antwerp, Chicago 2019).

[320] The example is taken and further explored from a regulatory perspective in Elisabetta Biasin and others, 'Cybersecurity of AI Medical Devices: Risks, Legislation, and Challenges' (Edward Elgar 2023).

[321] Griet Verhenneman and Anton Vedder, 'WITDOM D6.1 – Legal and Ethical Framework and Privacy and Security Principles'' 43 <http://www.witdom.eu/deliverables>.

[322] Loi and others (n 319).

[323] Karsten Weber and Nadine Kleine, 'Cybersecurity in Health Care' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer International Publishing 2020) <https://link.springer.com/10.1007/978-3-030-29053-5_7> accessed 20 March 2023.

[324] For a descriptive overview on the ethical aspects on cybersecurity, see also Elisabetta Biasin and Erik Kamenjasevic, 'Cybersecurity of Medical Devices: Legal and Ethical Challenges' (2020) <https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias3078888&context=SearchWebhook&vid=32KUL_KUL:Lirias&search_scope=lirias_profile&tab=LIRIAS&adaptor=SearchWebhook&lang=en>.

6.1.4. Justice

The Biomedical Ethics principle of Justice is oriented at highlighting **fairness and equality among individuals.** First, the principle requires the fair distribution of goods in society and implies looking at the role of entitlement (distributive justice). Secondly, the principle implies that socio-economic inequalities have to generate the greatest benefits from the lower-advantaged members (the difference principle).[325] As part of this second principle, decision-makers should compare different policy options and privilege the ones that benefit the least-advantaged the most.[326]

According to Beauchamp and Childress, society uses a variety of factors as criteria for distributive justice, including the following: [327]

1. 'To each person an equal share
2. To each person according to need
3. To each person according to effort
4. To each person according to contribution
5. To each person according to merit
6. To each person according to free-market exchanges'.

In the healthcare domain, issues of distributive justice concern, for example, the allotment of scarce resources – i.e. technology or equipment or tests such as the COVID-19 tests during the pandemic – or the allotment of time for outpatient visits.[328] This principle is violated, for example, when a practitioner suggests a specific treatment option over another commercially-driven choice.[329]

The principle of justice may offer guidance in the realm of *in silico* trials. For example, it may be of help in algorithmic-driven decision-making systems.[330]

> Example 1: *In silico* clinical trials of a medicinal product. The *in silico* technology simulates the testing of the medicinal product on synthetic population.
>
> Example 2: An *in silico* technology reproduces in a graphical representation a cohort of virtual patients.

The first example above brings the case of **population representativeness in AI-based clinical trials**. For clinical representation, it is widely known that the testing of medicinal products has been traditionally based on healthy Caucasian male individuals.[331] In recent years, research showed that clinical trials in the EU and the US had shown underrepresentation issues, and there is founded concern that AI-based technologies could

---

[325] See John Rawls, *A Theory of Justice* (Cambridge, Massachusetts : The Belknap Press of Harvard University Press, [1971] ©1971 1971) <https://search.library.wisc.edu/catalog/999472448502121>.

[326] John Rawls 1921-2002, *Justice as Fairness : A Restatement* (Cambridge, Mass : Harvard University Press, 2001 2001) 59 <https://search.library.wisc.edu/catalog/999913858702121>.

[327] Tom L Beauchamp and James F Childress, *Principles of Biomedical Ethics / Tom L. Beauchamp, James F. Childress* (4th ed, Oxford University Press 1994) 330.

[328] B Varkey, 'Principles of Clinical Ethics and Their Application to Practice' (2021) 30 Medical Principles and Practice 17.

[329] ibid.

[330] The work of Naudts on algorithmic-driven decision making systems is a useful resource. In his work, Naudts suggests to pivot on Nussbaum's capability approach to build an evaluative benchmark for algorithmically-guided decisions. See Laurens Naudts, 'Fair or Unfair Differentiation? Reconsidering the Concept of Equality for the Regulation of Algorithmically Guided Decision-Making' (2023).

[331] There are many reasons for that, which are not reported here for reasons of scope and space. For futher context, see Caroline Criado-Perez, *Invisible Women: Exposing Data Bias in a World Designed for Men* (Vintage 2020).

further amplify this issue. [332] Underrepresentation may concern, among other things, sex and gender,[333] age[334], and race/ethnicity (or a mix thereof). Diversity in clinical trials may be of particular relevance since symptoms for certain diseases vary depending on the factor in question (for example, sex and gender for multiple sclerosis or specific heart diseases[335]). Also, these factors are relevant for monitoring an individual's health status (see the case of pulse oximeters for race/ethnicity[336]). From the perspective of clinical trials, either for the traditional or for the simulated *in silico* ones, the principle of justice may help evaluate the composition of the population dataset in a manner that it can consider different variables for the studied population.[337] Virtually testing a medicinal product taking into account synthetic population representativeness could help better study the effects of the product. Ultimately, it could benefit a wider range of patients, and it could enhance the safety and efficacy of the medical product itself.

The second example entails the representation of patients. Similarly to clinical trials, **patient representation in medical illustrations** has traditionally focused only on the white male standard, leaving aside the others.[338] The virtual digital representation of patients (real or fictitious) within *in silico* technologies may be guided by the principle of justice, too. If virtual patients are represented synthetically, this principle may serve as a supporting tool for enhancing diversity and inclusiveness in their representation.

7. Conclusion

The purpose of this deliverable was to follow the overview carried out in D9.1 by offering a more in-depth analysis of the core legal and ethical issues of *in silico trials.* The deliverable focused on the following areas of legislation: privacy and data protection, data governance, clinical trials, medicinal products and medical devices, and artificial intelligence. The **'Privacy and Data Protection'** section (section 2) introduced the data processing principles and underlined the importance of distinguishing between different types of health data and the legal basis of their processing. The analysis showed common legal challenges in data protection as inherent to *in silico* trials. These include the categorisation of synthetic data and the rules on further processing of personal data, which have generated legal uncertainty in health data sharing. Section 3 on '**Data Governance**' described the changes the new data legislation will bring to healthcare. The new regulations will likely bring new questions about the legal bases for data sharing and hold potential for possible risks of

[332] The analysis considers the US for this aspect as the history of medicinal product and medical devices regulation of the EU has been heavily influenced by the US one. For further references, see Luca Arnaudo and Giovanni Pitruzzella, *La Cura Della Concorrenza: L'industria Farmaceutica Tra Diritti e Profitti* (1. ed, Luiss University Press 2019).

[333] Concerning sex and gender aspects in clinical research, see, for example, the Women's Brain Project 'Home - Women's Brain Project' (3 November 2021) <https://www.womensbrainproject.com/> accessed 21 March 2023; Eva Becher and Sabine Oertelt-Prigione, 'Chapter One - History and Development of Sex- and Gender Sensitive Medicine (SGSM)' in Elena Moro and others (eds), *International Review of Neurobiology*, vol 164 (Academic Press 2022) <https://www.sciencedirect.com/science/article/pii/S0074774222000666>.

[334] see, eg Rob J Marum, 'Underrepresentation of the Elderly in Clinical Trials, Time for Action' (2020) 86 British Journal of Clinical Pharmacology 2014.

[335] Donato Gemmati and others, '"Bridging the Gap" Everything That Could Have Been Avoided If We Had Applied Gender Medicine, Pharmacogenetics and Personalized Medicine in the Gender-Omics and Sex-Omics Era' (2019) 21 International Journal of Molecular Sciences 296.

[336] Byron S Kennedy, Robert P Richeson and Amy J Houde, 'Racial Bias in Pulse Oximetry Measurement' (2020) 383 New England Journal of Medicine 2479.

[337] For a concrete example of justice-related aspects in *in silico* technology, see Lesley Cockmartin, 'Virtual Imaging Trials for Breast X-Ray Imaging' (KU Leuven iSi Health Institute Seminars, Leuven, 2023). Ethical analysis in Elisabetta Biasin, 'Legal & Ethical Aspects of in Silico Health' (KU Leuven iSi Health Institute Seminars, Leuven, 2023).

[338] Criado-Perez (n 331) 197; Sarah Cascone, 'A Nigerian Medical Student Wondered Why His Textbooks Only Depict White Patients. So He Drew His Own Illustrations—and They Went Viral' (*Artnet News*, 7 December 2021) <https://news.artnet.com/art-world/diversity-medical-illustrations-chidiebere-ibe-2045122> accessed 21 March 2023.

fragmentation in the EU. Section 4, '**Clinical Trials, Medicinal Products and Medical Devices**' assessed the relevant frameworks with a critical view on the legal and regulatory challenges that insist towards *in silico* trials. On a regulatory level, the report observed the need for harmonized standardization and best practices concerning model validation for medicinal products and medical devices. On the legal level, the report pinpointed the legal references for *in silico* trials and commented on the opportunities that the upcoming pharmaceutical law reform could bring in the EU. Section 5, '**Artificial Intelligence**', discussed the AI Act proposal, its main requirements and focused on one specific new question, i.e. the exclusion of scientific research from the scope of the regulation. The last section on the '**Ethics Principles**' (section 6), continued the analysis of the biomedical ethics principles started in D9.1 and offered some indicative examples of how ethics principles could help stakeholders address the moral questions that could be brought by *in silico* trials in healthcare settings.

References

Anton Vedder and Daniela Spajić, 'Moral Autonomy of Patients and Legal Barriers to a Possible Duty of Health Related Data Sharing' (2023) 25 Ethics and Information Technology 23.

Aljaaf AJ and others, 'Partially Synthesised Dataset to Improve Prediction Accuracy' in De-Shuang Huang, Vitoantonio Bevilacqua and Prashan Premaratne (eds), *Intelligent Computing Theories and Application* (Springer International Publishing 2016)

Arnaudo L and Pitruzzella G, *La Cura Della Concorrenza: L'industria Farmaceutica Tra Diritti e Profitti* (1. ed, Luiss University Press 2019)

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data'

——, 'Advice Paper on Special Categories of Data ("sensitive Data")'

——, 'Annex to Letter from the WP29 to the European Commission - Health Data in Apps and Devices'

——, 'Guidelines on the Right to Data Portability'

Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

Assessing the Credibility of Computational Modeling through Verification and Validation: Application to Medical Devices (American Society of Mechanical Engineers 2018)

Avicenna Alliance, 'Modelling and Simulation as a Transformative Tool for Medical Devices: The Transatlantic Regulatory Perspective' (2018)

Avicenna CSA, 'In Silico Clinical Trials: How Computer Simulation Will Transform the Biomedical Industry' (2016)

Azizi Z and others, 'Can Synthetic Data Be a Proxy for Real Clinical Trial Data? A Validation Study' (2021) 11 BMJ Open e043497

Beauchamp T, 'The Principle of Beneficence in Applied Ethics' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Spring 2019, Metaphysics Research Lab, Stanford University 2019) <https://plato.stanford.edu/archives/spr2019/entries/principle-beneficence/> accessed 22 March 2023

Beauchamp TL and Childress JF, *Principles of Biomedical Ethics / Tom L. Beauchamp, James F. Childress* (4th ed, Oxford University Press 1994)

Beauchamp TL and Childress JF, *Principles of Biomedical Ethics* (5th ed., New York : Oxford university press 2001)

Becher E and Oertelt-Prigione S, 'Chapter One - History and Development of Sex- and Gender Sensitive Medicine (SGSM)' in Elena Moro and others (eds), *International Review of Neurobiology*, vol 164 (Academic Press 2022) <https://www.sciencedirect.com/science/article/pii/S0074774222000666>

Biasin E, 'Why Accuracy Needs Further Exploration in Data Protection', *Proceedings of the 1st International Conference on AI for People: Towards Sustainable AI, CAIP 2021, 20-24 November 2021, Bologna, Italy* (EAI 2021) <http://eudl.eu/doi/10.4108/eai.20-11-2021.2314205> accessed 22 January 2023

——, 'In Silico World D9.1 Legal and Ethical Inventory' <https://zenodo.org/record/7104079> accessed 10 January 2023

——, 'Legal & Ethical Aspects of in Silico Health' (KU Leuven iSi Health Institute Seminars, Leuven, 2023)

——, 'Cybersecurity of AI Medical Devices: Risks, Legislation, and Challenges' (Edward Elgar 2023)

Biasin E and Kamenjasevic E, 'Cybersecurity of Medical Devices: Legal and Ethical Challenges' (2020) <https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias3078888&context=SearchWebhook&vid=32KUL_KUL:Lirias&search_scope=lirias_profile&tab=LIRIAS&adaptor=SearchWebhook&lang=en>

——, 'Cybersecurity of Medical Devices: Regulatory Challenges in the European Union' in Carmel Shachar and others (eds), *The Future of Medical Device Regulation: Innovation and Protection* (Cambridge University Press 2022) <https://www.cambridge.org/core/books/future-of-medical-device-regulation/cybersecurity-of-medical-devices/AC01289C2DB05E44D0D98A9E66666562>

Cascone S, 'A Nigerian Medical Student Wondered Why His Textbooks Only Depict White Patients. So He Drew His Own Illustrations—and They Went Viral' (*Artnet News*, 7 December 2021) <https://news.artnet.com/art-world/diversity-medical-illustrations-chidiebere-ibe-2045122> accessed 21 March 2023

Cerreta F and others, 'Digital Technologies for Medicines: Shaping a Framework for Success' (2020) 19 Nature Reviews Drug Discovery 573

César Augusto FL and Abdullah E, 'On the Legal Nature of Synthetic Data' (2022)

Clifford D and Ausloos J, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130

Cockmartin L, 'Virtual Imaging Trials for Breast X-Ray Imaging' (KU Leuven iSi Health Institute Seminars, Leuven, 2023)

Comandè G and Schneider G, 'Differential Data Protection Regimes in Data-Driven Research: Why the GDPR Is More Research-Friendly Than You Think' (2022) 23 German Law Journal 559

Council of Europe, 'Recommendation CM/Rec2019(2). Protection of Health-Related Data' <https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html>

Criado-Perez C, *Invisible Women: Exposing Data Bias in a World Designed for Men* (Vintage 2020)

Curreli C and others, 'A Credibility Assessment Plan for an In Silico Model That Predicts the Dose–Response Relationship of New Tuberculosis Treatments' (2023) 51 Annals of Biomedical Engineering 200

Dahi A and Compagnucci MC, 'Device Manufacturers as Controllers – Expanding the Concept of "Controllership" in the GDPR' (2022) 47 Computer Law & Security Review 105762

Dove ES, 'The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era' (2018) 46 Journal of Law, Medicine & Ethics 1013

Dove ES and Chen J, 'Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis' (2020) 10 International Data Privacy Law 117

Drexl J, 'The (Lack of) Coherence of Data Ownership with the Intellectual Property System' in Niklas Bruun and others (eds), *Transition and Coherence in Intellectual Property Law* (1st edn, Cambridge University Press 2021)

<https://www.cambridge.org/core/product/identifier/9781108688529%23CN-bp-16/type/book_part> accessed 4 April 2023

Ducuing C, 'An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses' (2022) CiTiP Working Paper

——, 'What Can We Still Learn from Data Ownership?' (ELI Digital Law SIG Seminar, 1 June 2022)

——, 'White Paper on the Data Act Proposal' [2022] SSRN Electronic Journal <https://www.ssrn.com/abstract=4259428> accessed 17 November 2022

Ducuing C and Schroers J, 'The Recent Case Law of the CJEU on (Joint) Controllership: Have We Lost the Purpose of "Purpose"?' (2020) 2020 Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht

El Emam K, 'Seven Ways to Evaluate the Utility of Synthetic Data' (2020) 18 IEEE Security & Privacy 56

European Data Protection Board, 'Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (Art. 70.1.b))' (2019)

——, 'Guidelines 05/2020 on Consent under Regulation 2016/679' <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>

——, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en>

European Data Protection Board and European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en>

European Data Protection Supervisor, 'Mobile Health' <https://edps.europa.eu/sites/default/files/publication/15-05-21_mhealth_en_0.pdf>

——, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (2017)

——, 'A Preliminary Opinion on Data Protection and Scientific Research' <https://edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf>

European Digital Rights, 'EHDS: Ignoring Patients' Privacy' (*European Digital Rights (EDRi)*, 6 March 2023) <https://edri.org/our-work/eu-proposed-health-data-regulation-ignores-patients-privacy-rights/> accessed 27 April 2023

European Medicines Agency, 'Qualification of Novel Methodologies for Drug Development: Guidance to Applicants' (2009)

——, 'Mandate of the EMA Innovation Task Force (ITF)' (2014)

——, 'Essential Considerations for Successful Qualification of Novel Methodologies' (2017)

——, 'Committee for Medicinal Products Human Use (CHMP)' (*European Medicines Agency*, 17 September 2018) <https://www.ema.europa.eu/en/committees/committee-medicinal-products-human-use-chmp> accessed 1 April 2023

——, 'Questions and Answers: Qualification of Digital Technology-Based Methodologies to Support Approval of Medicinal Products' (2020)

European Digital Rights, 'EHDS: Ignoring Patients' Privacy' (European Digital Rights (EDRi), 6 March 2023) <https://edri.org/our-work/eu-proposed-health-data-regulation-ignores-patients-privacy-rights/> accessed 27 April 2023

Fontanillo López CA and Elbi A, 'On Synthetic Data: A Brief Introduction for Data Protection Law Dummies' (2022)

Fortuna G, 'EU Pharma Reform Delayed Again Due to Commission's Busy Agenda – EURACTIV.Com' (*EURACTIV*, 22 March 2023) <https://www.euractiv.com/section/health-consumers/news/eu-pharma-reform-delayed-again-due-to-commissions-busy-agenda/> accessed 3 April 2023

Gartner M, 'Regulatory Acknowledgment of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act' (2022) 8 European Data Protection Law Review 462

Gemmati D and others, '"Bridging the Gap" Everything That Could Have Been Avoided If We Had Applied Gender Medicine, Pharmacogenetics and Personalized Medicine in the Gender-Omics and Sex-Omics Era' (2019) 21 International Journal of Molecular Sciences 296

Gonzales A, Guruswamy G and Smith SR, 'Synthetic Data in Health Care: A Narrative Review' (2023) 2 PLOS Digital Health e0000082

Government of Canada IAP on RE, 'How to Address Material Incidental Findings - Guidance in Applying TCPS 2 (2018) Article 3.4' (15 March 2019) <https://ethics.gc.ca/eng/incidental_findings.html?wbdisable=true#a3> accessed 22 March 2023

Grossman RI and Bernat JL, 'Incidental Research Imaging Findings: Pandora's Costly Box' (2004) 62 Neurology 849

Hariry RE, Barenji RV and Paradkar A, 'Towards Pharma 4.0 in Clinical Trials: A Future-Orientated Perspective' (2022) 27 Drug Discovery Today 315

Harrer S and others, 'Artificial Intelligence for Clinical Trial Design' (2019) 40 Trends in Pharmacological Sciences 577

Hildebrandt M, 'Ground-Truthing in the European Health Data Space' (SocArXiv 2023) preprint <https://osf.io/uw4nq> accessed 20 January 2023

Hines PA and others, 'Artificial Intelligence in European Medicines Regulation' (2023) 22 Nature Reviews Drug Discovery 81

'Home - Women's Brain Project' (3 November 2021) <https://www.womensbrainproject.com/> accessed 21 March 2023

'Is the Future of Privacy Synthetic? | European Data Protection Supervisor' (14 July 2021) <https://edps.europa.eu/press-publications/press-news/blog/future-privacy-synthetic> accessed 14 March 2023

John Hopkins Medicine Institutional Review Board, 'Plans for Detecting and Managing Incidental Findings Associated with Research Imaging Procedures' (2016) <https://www.hopkinsmedicine.org/institutional_review_board/guidelines_policies/guidelines/incidental_findings.html> accessed 22 March 2023

Kaminski R, 'AI in Pharma. What Does Artificial Intelligence Bring to the Pharmaceutical Industry?' (*Nexocode*, 2 March 2021) <https://nexocode.com/blog/posts/ai-in-pharma/> accessed 7 December 2022

Kennedy BS, Richeson RP and Houde AJ, 'Racial Bias in Pulse Oximetry Measurement' (2020) 383 New England Journal of Medicine 2479

Kokosi T and Harron K, 'Synthetic Data in Medical Research' (2022) 1 BMJ Medicine e000167

Kolluri S and others, 'Machine Learning and Artificial Intelligence in Pharmaceutical Research and Development: A Review' (2022) 24 The AAPS Journal 19

Lalova-Spinks T, 'Data Control in the European Health Data Space Proposal: Highlights' (Data Week 2022, June 2022) <https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias3790964&context=SearchWebhook&vid=32KUL_KUL:Lirias&search_scope=lirias_profile&tab=LIRIAS&adaptor=SearchWebhook&lang=en>

——, 'Challenges Related to Data Protection in Clinical Research before and during the COVID-19 Pandemic: An Exploratory Study' (2022) 9 Frontiers in Medicine 995689

Leistner M and Antoine L, 'Attention, Here Comes the EU Data Act! A Critical in-Depth Analysis of the Commission's 2022 Proposal' (2022) 13(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 339

Liddell K, Simon DA and Lucassen A, 'Patient Data Ownership: Who Owns Your Health?' (2021) 8 Journal of Law and the Biosciences lsab023

Liguori L and Todisco C, 'Il riutilizzo dei dati personali a fini di ricerca anche alla luce dei più recenti orientamenti del Garante' (*AboutPharma*, 1 December 2022) <https://www.aboutpharma.com/legal-regulatory/il-riutilizzo-dei-dati-personali-a-fini-di-ricerca-anche-alla-luce-dei-piu-recenti-orientamenti-del-garante/> accessed 5 April 2023

Loi M and others, 'Cybersecurity in Health – Disentangling Value Tensions' (2019) 17 Journal of Information, Communication and Ethics in Society 229

Marcus JS and others, 'The European Health Data Space' [2022] SSRN Electronic Journal <https://www.ssrn.com/abstract=4300393> accessed 25 January 2023

Marum RJ, 'Underrepresentation of the Elderly in Clinical Trials, Time for Action' (2020) 86 British Journal of Clinical Pharmacology 2014

'Medtronic Enables Pacemaker Monitoring by Smartphone' (*Healthcare IT News*, 20 November 2015) <https://www.healthcareitnews.com/news/medtronic-enables-pacemaker-monitoring-smartphone> accessed 8 March 2023

Morrison TM and others, 'Advancing Regulatory Science With Computational Modeling for Medical Devices at the FDA's Office of Science and Engineering Laboratories' (2018) 5 Frontiers in Medicine 1

Musuamba FT and others, 'Verifying and Validating Quantitative Systems Pharmacology and *In Silico* Models in Drug Development: Current Needs, Gaps, and Challenges' (2020) 9 CPT: Pharmacometrics & Systems Pharmacology 195

——, 'Scientific and Regulatory Evaluation of Mechanistic *in Silico* Drug and Disease Models in Drug Development: Building Model Credibility' (2021) 10 CPT: Pharmacometrics & Systems Pharmacology 804

Naudts L, 'Fair or Unfair Differentiation? Reconsidering the Concept of Equality for the Regulation of Algorithmically Guided Decision-Making' (2023)

Neuwirth RJ, 'Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act' [2022] SSRN Electronic Journal <https://www.ssrn.com/abstract=4261569> accessed 3 April 2023

Ó Cathaoir K and others, 'EUSTANDS4PM Report. Legal and Ethical Review of in Silico Modelling' (2020)

on behalf of the ESHG Public and Professional Policy Committee and others, 'Whole-Genome Sequencing in Health Care: Recommendations of the European Society of Human Genetics' (2013) 21 European Journal of Human Genetics 580

Owczarek D, 'The Future of Pharmaceutical Manufacturing Process: Artificial Intelligence' (*nexocode*, 7 July 2021) <https://nexocode.com/blog/posts/ai-in-pharmaceutical-manufacturing/> accessed 8 December 2022

Pappalardo F and others, 'In Silico Clinical Trials: Concepts and Early Adoptions' (2019) 20 Briefings in Bioinformatics 1699

——, 'Toward A Regulatory Pathway for the Use of in Silico Trials in the CE Marking of Medical Devices' (2022) 26 IEEE Journal of Biomedical and Health Informatics 5282

Rawls J, *A Theory of Justice* (Cambridge, Massachusetts : The Belknap Press of Harvard University Press, [1971] ©1971 1971) <https://search.library.wisc.edu/catalog/999472448502121>

Rawls J 1921-2002, *Justice as Fairness : A Restatement* (Cambridge, Mass : Harvard University Press, 2001 2001) <https://search.library.wisc.edu/catalog/999913858702121>

Richardson HS and Belsky L, 'The Ancillary-Care Responsibilities of Medical Researchers: An Ethical Framework for Thinking about the Clinical Care That Researchers Owe Their Subjects' (2004) 34 The Hastings Center Report 25

Rubin DB, 'Statistical Disclosure Limitation' (1993) 2 Journal of Official Statistics 461

Shabani M and Yilmaz S, 'Lawfulness in Secondary Use of Health Data' [2022] Technology and Regulation 128

Studio Legale Stefanelli & Stefanelli, 'Databases: Legal Protection between Italian Copyright and Sui Generis Right - Lexology' (2022) <https://www.lexology.com/library/detail.aspx?g=e4cb0182-b3b8-429c-9ac0-51325d8eca36> accessed 4 April 2023

Surendra H and Mohan HS, 'A Review of Synthetic Data Generation Methods For Privacy Preserving Data Publishing' (2017) 6 International Journal of Scientific & Technology Research

Van Alsenoy B, 'Regulating Data Protection : The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing' (2016)

van Kessel R and others, 'The European Health Data Space Fails to Bridge Digital Divides' [2022] BMJ e071913

Varkey B, 'Principles of Clinical Ethics and Their Application to Practice' (2021) 30 Medical Principles and Practice 17

Vedder A, 'Safety, Security and Ethics', vol 7 (Intersentia; Cambridge, Antwerp, Chicago 2019)

Vedder A and Spajić D, 'Moral Autonomy of Patients and Legal Barriers to a Possible Duty of Health Related Data Sharing' (2023) 25 Ethics and Information Technology 23

Verhenneman G, 'The Patient's Right to Privacy and Autonomy against a Changing Healthcare Model' (KU Leuven Faculteit Rechtsgeleerdheid 2020)

Verhenneman G and Vedder A, 'WITDOM D6.1 – Legal and Ethical Framework and Privacy and Security Principles'' <http://www.witdom.eu/deliverables>

Weber K and Kleine N, 'Cybersecurity in Health Care' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer International Publishing 2020) <https://link.springer.com/10.1007/978-3-030-29053-5_7> accessed 20 March 2023

Weissler EH and others, 'The Role of Machine Learning in Clinical Research: Transforming the Future of Evidence Generation' (2021) 22 Trials 537

Wilkinson A, 'Medical Device Regulation and Litigation: A Comparative Analysis of Australia, the United Kingdom and the United States of America' (PhD, Queensland University of Technology 2021) <https://eprints.qut.edu.au/209677> accessed 14 September 2022

Wolf SM, Paradise J and Caga-Anan C, 'The Law of Incidental Findings in Human Subjects Research: Establishing Researchers' Duties' (2008) 36 Journal of Law, Medicine & Ethics 361

WP29, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679'

Zuiderveen Borgesius F, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (2017) 3 European Data Protection Law Review 130