Big Data and Artificial Intelligence

EU Policy Briefing for Patient Organisations

European Patients' Forum, April 2020

Contents

Introduction

Digitalisation is rapidly changing society and touches on health and healthcare in many ways. Digitalisation presents enormous promise for improving healthcare, but also challenges both in terms of ensuring that the regulatory and policy framework is fit for purpose. While digitalisation has been happening for years, progress has been uneven. The **COVID-19 pandemic** that unfolded in early 2020 has led to a rush to implement eHealth services, including telemedicine consultations, in countries such as China, the US, Canada and the UK, at a scale and pace that is "unprecedented". Other countries have seen an explosion in demand but run up against limited infrastructure and technical resources as well as staff, as has happened in many Italian hospitals. Digital tools are proposed as a solution to controlling the spread of infections, once countries start relaxing initial controls. Some commentators welcome these developments as something that should have happened a long time ago; others have cautioned against undermining the quality of care and possible erosion of people's privacy. [1,2,3]

What is clear is that the pandemic has revealed the urgency of finding effective digital solutions that really work for patients. The present crisis might hasten the digitalisation of health systems – and the patient voice will need to be at the centre of policy and practice.

> **"Digitalisation in healthcare should lead to better quality, safety and sustainability of care – but it also promises to transform care into a much more participatory process."**
>
> EPF Elections Manifesto, 2019

This policy briefing was prepared by the EPF Secretariat, with the support of the **Digital Health Working Group**, whom we would like to thank for their contribution. The paper aims to provide an overview of two areas of technology that are particularly in the focus of EU policy: big data, and artificial intelligence. Its purpose is to support the engagement of patient organisations in EU policy discussions around digital health, with special focus on the above-mentioned topics, in line with our commitment to bringing a meaningful and robust patient perspective into EU policy debates. It is not a position paper nor does it aim to be comprehensive. The first part of the paper outlines EPF's past engagement in this arena and gives an overview of two important concepts: big data and artificial intelligence. The second part discusses the European Union's current policy priorities regarding digital health. EPF will use this briefing as a background document and to support consultations with its membership and on discussions around common principles on patient-centred digital health.

Background on EPF's engagement in digital health

Digital health refers to healthcare practices supported by electronic processes and communication. It includes a wide range of services and information technology such as electronic medical records, telemedicine, evidence-based medicine, consumer health informatics, etc. The World Health Organization defines digital health as "an overarching term that comprises eHealth (which includes mHealth), and emerging areas, such as the use of computing sciences in the fields of artificial

---

[1] https://www.politico.eu/article/coronavirus-bundles-greece-into-the-digital-era/. A French company is offering free online consultation tools: https://www.safesante.fr/search . A Spanish company Eurecat is providing 3D-printed medical devices, such as protective screens, to fight coronavirus. https://eurecat.org/actualitat/

[2] Prof. Eric Topol quoted in The Lancet, "Virtual health care in the era of COVID-19". Vol 395 April 11, 2020.

[3] Council of Europe Committee on Bioethics, DH-BIO Statement on human rights considerations relevant to the COVID-19 pandemic. DH-BIO/INF(2020)2. Strasbourg, 14 April 2020.

intelligence, big data and genomics." eHealth is defined as the "use of information and communications technology (ICT) in support of health and health-related fields, including health care services, health surveillance, health literature, and health education, knowledge and research. mHealth is a component of eHealth."[4]

Digital health relates to EPF's strategic priorities set out in the EPF Strategic Plan 2014-2020[5], and has been developed in subsequent annual work plans. Our early work focused on participation in various EU-funded eHealth projects that helped us gather evidence and develop a knowledge base. Drawing on the findings of those projects, EPF published a *position paper on eHealth* in 2016.[6] The paper makes recommendations in areas such as health literacy, patients' access and rights with regards to their to health data, and the safety and quality of eHealth devices and remains a major reference point for our advocacy.

EPF engaged substantially with the development of the EU General Data Protection Regulation. Our 2012 *position paper*[7] set out the patient community's views on the Commission's legislative proposal. Once the new Regulation was adopted, EPF published a *guide for patient organisations* setting out the implications of the GDPR, in 2016.

Summary of EPF's policy and advocacy work related to digital health, 2012-2019

Position Statement	on the **General Data Protection Regulation** – *December 2012*
Position Statement	on **Informed consent** in **clinical trials** – *May 2016*
Guide for patients' organisations	**EU Regulation on the protection of personal data:** what does it mean for patients? – *Autumn 2016*
Position Paper	on **eHealth** - *December 2016*
Reply	**Public consultation** on Transformation of Health and Care in the Digital Single Market – *October 2017*
Working Group	**Digital Health –** set up to support our work in this area and provide expertise – *February 2018*
Briefing on big data	Enabling patient communities to provide meaningful input to policy discussions – *2019-20*
Patient survey	Electronic health records and data sharing – *2019*

A 2018 consultation process with our membership identified digital health as one of the five policy priorities for the new European Commission and Parliament. In the same year EPF set up an *internal working group on digital health* to guide our work.

Priority no.3 of the **EPF Manifesto for the 2019 European elections**, *Driving the development of digital health*, states: "the EU should ensure that Europe's future digital health tools and systems start from patients' priorities and are co-developed with patients." Our message is clear: digital tools should start

---

[4] WHO Guideline: "Recommendations on digital interventions for health system strengthening", 2019. Available at https://www.who.int/reproductivehealth/publications/digital-interventions-health-system-strengthening/en/
[5] EPF, Strategic Plan 2014-2020, https://www.eu-patient.eu/globalassets/library/strategic-planning/epf-strategic-plan-2014-2020-final.pdf
[6] Our past projects on eHealth included SUSTAINS – Support USers To Access INformation and Services; Chain of Trust; Renewing Health; Calliope, and SmartCare. For more background see the position paper on eHealth, available at https://www.eu-patient.eu/globalassets/policy/ehealth/epf-final-position-paper-on-ehealth_19december2016.pdf
[7] EPF, Position Statement on EU General Data Protection Regulation (2012), https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection_position-statement_10-12-2012.pdf

from the needs of healthcare users and be developed with the users, to ensure technology actually facilitates participatory, person-centred healthcare and leads to better outcomes for patients, and better value for society.

In follow-up to the EU elections, the **EPF Congress on Meaningful Patient Involvement**: The Path to More Effective Health Systems[8] held in November 2019 dedicated a parallel working session to digital health. Key outcomes from the session "How to ensure digital health brings real-life benefits for patients?" are integrated in the Congress report.[9]

EPF is currently involved as partner in **several ongoing digital health-related projects**. These projects not only help us engage with current research and initiatives, collect further evidence and knowledge, but also contribute a patient perspective and patient voice to the projects with the aim of improving the conduct and outcomes of projects.

EPF was a member of the European Commission's advisory group that provided input on the shaping of the European eHealth Action plan 2012-2020. EPF was again invited to participate in the renewed **eHealth Stakeholder Group 2019-2022**.

- **Digital Health Europe** is a Horizon 2020 project that aims to support the digital transformation of health and care priorities of the EU's Digital Single Market. It works around three pillars corresponding to the Commission's priorities: citizens' secure access to and sharing of health data across borders; better data to advance research, prevention and personalised care; and digital tools for person-centred care and empowerment.

- **The European Health Data and Evidence Network**, EHDEN, is an IMI project that supports large-scale deployment of digital solutions for person-centred, integrated care.

- **Data Saves Lives** is a collaborative initiative to create a "health data community" that can function as a safe space where all stakeholders can openly discuss views and ideas on data and policy at European and national level. It will also develop an informative web platform for lay-friendly information for patients and citizens. www.eu-patient.eu/whatwedo/Projects/

Emerging technologies: Big Data and Artificial Intelligence

Below we provide a brief overview of big data and artificial intelligence, and their implications for healthcare and for patients. While it should be borne in mind that the two concepts are very closely linked and interdependent, we chose to present each of them in turn, followed by a discussion of their possible benefits and risks, including ethical issues.

Big data

The term "big data" originates in computer science. Current definitions of big data vary, but they all refer to a "very large amount of data, much larger than what can be analysed on a single computer today, coming from different sources and in different, often unstructured, formats."[10] Characteristics of big data include large data volumes; a fast accumulation of new data; challenges with the reliability of data sources and accuracy; and the diversity and complexity of the data and how it is structured.

---

[8] EPF Congress 2019, https://epfcongress.eu/
[9] EPF, EPF Congress 2019 – Report, https://www.eu-patient.eu/News/News/epf-congress-2019-theres-nothing-for-patients-without-patients/
[10] European Commission, Study on Big Data in Public Health, Telemedicine and Healthcare (2016), https://ec.europa.eu/digital-single-market/en/news/study-big-data-public-health-telemedicine-and-healthcare

In healthcare, but the term "big data" is most often used to mean large healthcare databases, such as electronic health record systems, or networks of interconnected healthcare databases. Big data repositories might typically contain information on a million or more patients, perhaps reflecting the population of a health region, country, or all of the people with a particular condition across Europe. The European Commission has proposed the following definition for big data: "large routinely or automatically collected datasets, which are electronically captured and stored. They are reusable in the sense of multipurpose data and comprise the fusion and connection of existing databases for the purpose of improving health and health system performance."[11]

Uses of big data in healthcare

Researchers need to study the data on large numbers of patients to identify very specific or unusual patterns of a health condition, interactions, know the long-term effects of different treatments, and to identify rare side-effects which might occur only in very few patients. Because of this research need, and the opportunities to interconnect health data originating from multiple sources, national health systems and private companies are increasingly investing in infrastructures to enable big data analysis.

Big data can be used for improving public health, disease prevention as well as treatment and care. Examples include new understanding of disease mechanisms or associations; discovery or validation of new biomarkers for patient stratification for targeted therapies ("personalised medicine"); new markers[12] for identifying people with a disease who were formerly undiagnosed; and medicines safety monitoring and studies. Societal benefits can include faster development of new medicines, increasing the effectiveness and efficiency of treatments through targeted or personalised medicine; identifying risk factors; and possibly preventing certain diseases.

Examples of studies using big data:

- In Taiwan a study of >782 million outpatient visits in the National Health Insurance database was used to identify previously unmapped cancer–disease associations across ages and genders. The tool developed is able to detect cancer comorbidities earlier than would be possible by manual inspection and identify potential effect modifiers or new risk factors.
- Analysis of 25 million patient records of the US Veterans Administration discovered that patients with periodontal disease were more likely to have rheumatoid arthritis.
- A study of 27 million patient records that accurately determined individual risk factors post knee arthroplasty
- Algorithm-enabled rapid searching of an EHR database of 2.5 million people to accurately identify systemic lupus erythematosus – potential for application to other autoimmune disorders
- Claims-based surveillance of over 17 million vaccinations did not indicate a statistically significant rise in Guillain–Barré syndrome following seasonal influenza vaccination.
- Nine million clinical notes for over 1 million patients detected statistically significant safety signals. ([Singh et al (2018)](#))

---

[11] European Commission, Study on Big Data in Public Health, Telemedicine and Healthcare (2016)

[12] A biomarker is something that can be measured (e.g. via a blood test, imaging, or physical examination) that points to the presence of a disease, physiological change, response to treatment, or psychological condition. For example, blood glucose levels are used as a biomarker in managing diabetes, whilst brain images can provide information about the progression of multiple sclerosis; presence of antibodies can be a sign of an infection; body temperature is a biomarker for fever. Biomarkers nowadays can also be mutations identified in genomic tests.

Real-world data is also key to improving the performance of healthcare systems through better monitoring of **health outcomes** over time, leading to the ability of healthcare providers and policymakers to use available resources more efficiently and to identify best practices in care. This is conditional on having the right infrastructure in place as well as the right indicators that capture the outcomes that matter to patients (especially quality of life). Patients' expertise, is based on experiential knowledge, is starting to be recognised as valid and important for complementing scientific knowledge. Patient input into research and development is an opportunity to develop new treatments and technologies that better meet patients' needs and are also cost-effective. This will require a culture change and re-assessment of priorities, and the patients' voice is of critical importance.

In medicines regulation, big data can improve the **benefit-risk assessment of medicines** across their lifecycle. Types of data can include real-world data such as EHRs, registries, spontaneous adverse drug reaction reports, social media, and wearable devices. To understand the current and emerging data landscape and advanced analytical methods, the HMA/EMA Task Force on big data looked at challenges and opportunities posed by big data in medicine regulation by mapping the sources and characteristics of big data; exploring its potential applicability and impact on medicines regulation; assessing the need for changes to legislation or guidelines; and making recommendations for change to strengthen medicines regulation in support of public health. Data forms a key element of the European medicines regulatory network's EU Network Strategy to 2025.[13] Relevant reports and documents are available online, including the phase I Summary report published in February 2019,[14] phase II report "Evolving Data-Driven Regulation" (2019).[15]

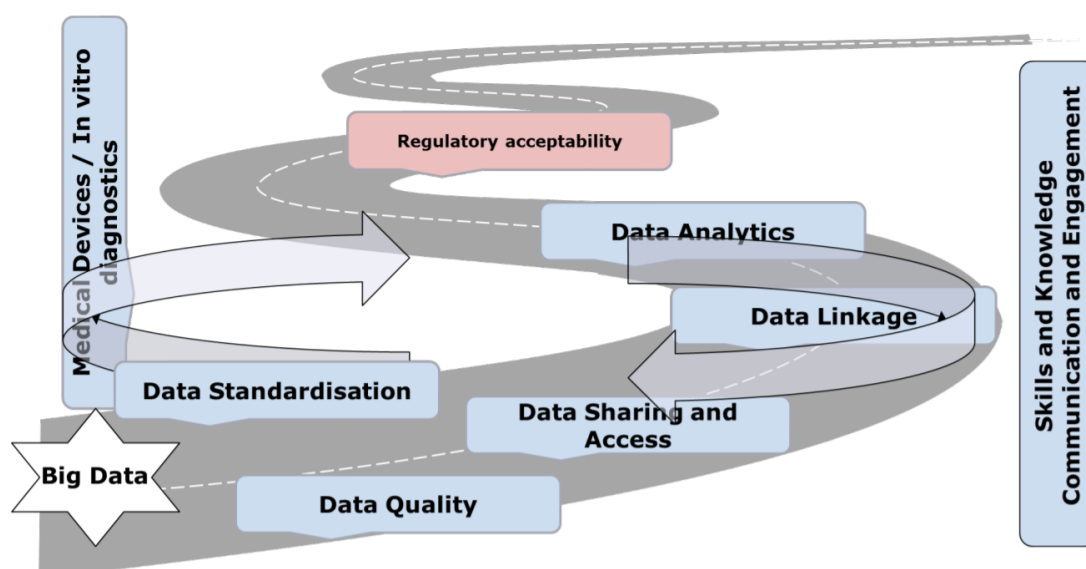**The road to regulatory acceptability of big data**

Figure 1: The Road to Regulatory acceptability: an integrated strategy reflecting core recommendations to support the use of Big Data in the assessment and monitoring of medicinal products in Europe. The individual steps are not necessarily sequential, may not be required across all datasets, many are interdependent and all will require active and iterative communication between all stakeholders.

Source: EMA/HMA Task Force summary report 2019, p. 25

---

[13] For more information and access to all relevant documents, visit https://www.hma.eu/506.html?&L=0

[14] HMA-EMA Joint Big Data Taskforce, Summary Report (2019), https://www.hma.eu/fileadmin/dateien/HMA_joint/00-_About_HMA/03-Working_Groups/Big_Data/2019_02_HMAEMA_Joint_Big_DataTaskforce_summary_report.pdf

[15] HMA-EMA Joint Big Data Taskforce, Phase II report: 'Evolving Data-Driven Regulation' (2019), https://www.hma.eu/fileadmin/dateien/HMA_joint/00-_About_HMA/03-Working_Groups/Big_Data/HMA-EMA_Joint_Big_Data_Taskforce_Phase_II_report_Evolving_Data-Driven_Regulation.pdf

The Task force has released a set of priority recommendations that address the need for skills and capacity-building, but also developing a secure EU data platform for accessing and analysing healthcare data from across the EU to support better decision-making on medicines; establishing an EU framework for data quality and representativeness; and the creation of an EU big data "stakeholder implementation forum" for dialogue with patients, health professionals, industry, HTA bodies, payers, device regulators and technology companies.[16]

Possible risks of big data relevant to patients

The term *big data* refers only to the data itself – not to the purposes for which the data may be used, how the data should be protected, or how its uses should be regulated. Issues that need to be considered and resolved when policies and practices for collection and use of big data are developed include:
- ensuring patients' privacy is respected.
- ensuring appropriate use and preventing inappropriate use of patients' data.
- security, i.e. preventing unauthorised use of data and ensuring its safe transmission, confidentiality and integrity.
- ensuring the data is of high enough quality for use in research.
- addressing any ethical concerns and ensuring human rights are respected.
- ensuring all data processing is ethical
- addressing all implications of primary and secondary use, including unintended consequences
- addressing issues of patient anonymity and possible identification

Some of these issues are now being addressed by the European Commission (see sections below).

Artificial Intelligence

Big data and *artificial intelligence* are closely connected. Often, artificial intelligence is used to analyse the information that is collected in the form of big data (which due to its sheer size cannot be analysed by human means). It is therefore very much dependent on the quality of the data that is processed, and the two should be viewed as interlinked.

The term "artificial intelligence" was coined by John McCarthy, an American computer scientist, in 1956 at the first artificial intelligence conference, which explored ways to make a machine that could reason like a human. The definition used in most dictionaries today is very much linked to the initial idea. The English Oxford Living Dictionary defines artificial intelligence as: "The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."[17] This definition is very broad and is not specific to any policy sector. It can thus be applied to different fields in different ways – including healthcare.

The European Commission uses the following definition of AI: "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots,

---

[16] HMA-EMA Joint Big Data Taskforce, Priority Recommendations, https://www.hma.eu/fileadmin/dateien/HMA_joint/00-_About_HMA/03-Working_Groups/Big_Data/Final_-_Priority_Recommendations_of_the_HMA-EMA_joint_Big_Data_Task_Force.pdf
[17] https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095426960

autonomous cars, drones or Internet of Things applications)."[18] The Commission's High Level Expert Group has developed a document that expands the above definition."[19]

A key challenge will be ensuring that AI is developed and used in a way that is transparent and policies are centred around the public interest – not only a focus on stimulating innovation per se.

Machine learning is the underlying approach of many current AI applications. Machine learning "allows systems to discover patterns and derive its own rules when it is presented with data and new experiences."[20] It uses statistical techniques to give computer systems the ability to "learn" (get better at specific tasks) from data, without being explicitly programmed. The computer uses an algorithm to gain "understanding" about a set of data and then makes predictions based on its understanding. In practical terms, this means that the more data is fed into the system, the more the system can improve itself. Machine learning is thus dependent on big data. There are different types of machine learning techniques. In *supervised machine learning* the system is trained through human input. Based on labelled examples of data the system "learns" to replicate a certain output based on the input. *Unsupervised machine learning* is when the system "learns" from test data that has not been labelled, classified, or categorised. The system itself identifies commonalities in the data and reacts to them. Big data, because of its unstructured and unclassified nature, provides a good way for machines to identify patterns in vast amounts of information. *Deep learning* techniques are based on the way the human brain processes information. A deep learning model comprises several levels of representation, in which every level uses the information from the previous level to "learn".

Uses of Artificial Intelligence in healthcare

AI together with big data has the potential to transform several aspects of how care is delivered. The 2020 EIT Health-McKinsey report "Transforming healthcare with AI – the impact on the workforce and organisations" highlights six areas where AI has a direct impact on the patient: self-care, prevention and wellness, triage and early diagnosis, diagnostics, clinical decision support, and care delivery in the context of chronic care management. The report also identifies three areas of the healthcare value chain that could benefit from introducing AI: improving population health, healthcare operations and healthcare-related innovation.[21]

Uses for AI are similar as for big data in general – in research, clinical care, organisation of healthcare, public health, and in consumer health/wellness apps. One of the potentially very valuable benefits of AI would be to **save the time of medical professionals** for other things – such as interacting with patients in a more meaningful way. AI-supported tools can also result in reduced costs, and support patients take control of their health.

---

[18] European Commission, Communication – Artificial Intelligence for Europe, COM(2018) 237 final, Brussels, 25.04.2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625
[19] High-Level Expert Group on Artificial Intelligence, A definition of AI: Main capabilities and scientific disciplines (2019), https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines
[20] Nuffield Council on Bioethics, Artificial intelligence (AI) in healthcare and research (2018), https://www.nuffieldbioethics.org/wp-content/uploads/Artificial-Intelligence-AI-in-healthcare-and-research.pdf
[21] EIT Health – McKinsey & Company – Transforming healthcare with AI – The impact on the workforce and organisations (2020), https://www.mckinsey.com/~/media/McKinsey/Industries/Healthcare%20Systems%20and%20Services/Our%20Insights/Transforming%20healthcare%20with%20AI/Transforming-healthcare-with-AI.ashx

Exhibit 1.3 – Areas of impact for AI in healthcare
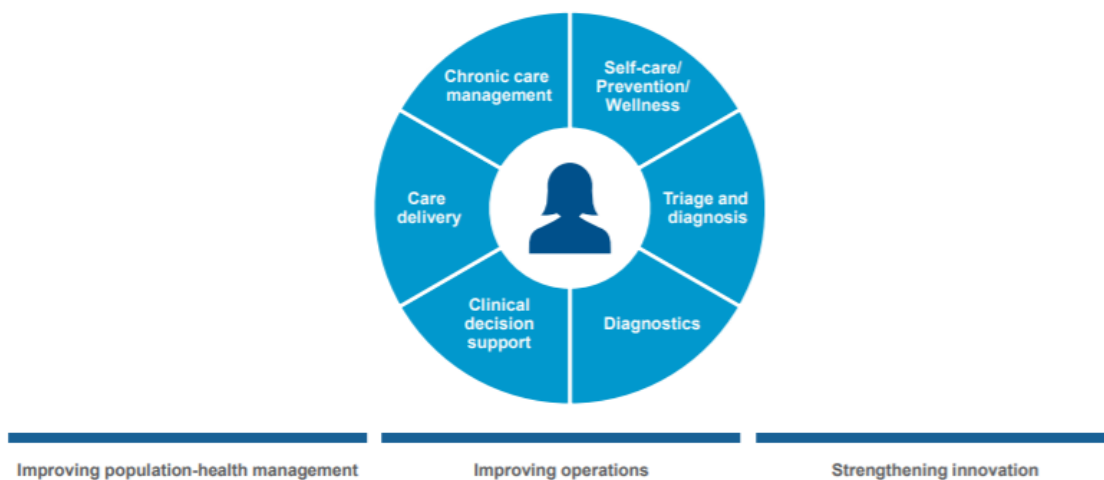
Source: EIT-McKinsey report 2020, page 29

In research, as AI can analyse very large and complex data sets and identify patterns, it can be used to search scientific literature for relevant studies and to combine different kinds of data. Very recently, AI has been used in efforts to **develop new antibiotics**. A machine-learning system was trained to predict which molecules would be effective against a specific bacterium and only screen molecules that are different from conventional antibiotics. The model identified several candidates from a pool of more than 100 million molecules, at least one of which – named *halicin* – is a strong candidate for further development. AI can be used to **match patients to clinical trials**.

In clinical care, use of AI is becoming established in the interpretation of **medical imaging** and **supporting accurate diagnosis**. By comparing the thousands of images that are collected every day, AI can be trained to perform an initial comparison and spot problems, which may reduce the time that health professional must spend analysing images. In fact, AI can sometimes analyse medical scans faster and more accurately than humans.[22] Deep learning algorithms are currently being used in mammography for breast cancer detection[23], CT for colon cancer diagnosis, chest radiographs for the detection of pulmonary nodules, MRI for brain tumour segmentation, and for the diagnosis of neurologic disorders, such as Alzheimer's disease. Algorithms can help dermatologists make better diagnoses, for example detecting 95% of skin cancers by learning from large sets of medical images.[24] Speech recognition can assist in diagnosis if the patient talks or writes to an artificial doctor to give their medical information and history.[25]

In **clinical care**, examples of AI use include the **artificial kidney**, which has the potential to revolutionise treatment for kidney patients (with the caveat the warning system must be reliable and fully transparent).[26] Some countries, for example Sweden, are starting to look at AI for decision-making in **organ donation**. Linking organ donors to patients required doctors to analyse blood types

---

[22] Nuffield Council on Bioethics, Artificial intelligence (AI) in healthcare and research (2018)

[23] Killock D., AI outperforms radiologists in mammographic screening, Nature Reviews Clinical oncology 17, 134 (2020), https://www.nature.com/articles/s41571-020-0329-7

[24] Horgan D., Romao M., Morré S.A., Kalra D., Artificial Intelligence: Power for Civilisation – and for Better Healthcare, Public Health Genomics 2019;22:145–161 (2019), https://www.karger.com/Article/FullText/504785

[25] Abhimanyiu S. Ahuja, The impact of artificial intelligence in medicine on the future role of the physician, PeerJ. 2019; 7: e7702, (2019) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6779111/

[26] Vellido A., Societal Issues Concerning the Application of Artificial Intelligence in Medicine, Kidney Dis 2019;5:11–17, (2018), https://www.karger.com/Article/Pdf/492428

and tissue variations in patients' and potential donors' charts, which is very time-consuming. AI can now perform they analyses and make these complicated matches.[27]

In **public health**, AI is used in epidemiology. During the **COVID-19 pandemic**, artificial intelligence has played a role in diagnosis and modelling the spread of new cases.[28]

Care organisation examples include a council in England that is piloting IBM Watson to match patients with care providers that meet their needs within their allocated budget and to design individual care plans, with the aim of using resources in a more cost-effective way.

Artificial Intelligence can be used in tools to **support empowerment and self-management**. Health apps on the market using AI include those that provide a personalised health assessment and home care advice, and those developed to support chronic disease management. The "Ada Health Companion" uses AI to operate a chat-bot, which combines information about symptoms from the user with other information to offer possible diagnoses. The "Arthritis Virtual Assistant" app developed by IBM for Arthritis Research UK "learns" through interactions with patients to provide personalised information and advice concerning medicines, diet, and exercise. Another example is a technology called "Imagine", which enables patients with skin conditions to monitor themselves. Initially the tool only offered the possibility of taking photos of the skin between consultations and forwarding this to their dermatologist. This enabled the dermatologist to have a better view of the changes as they occurred overtime. By having analysed thousands of the collected images, the AI technology is now able to suggest possible causes of the skin condition, assisting the doctors in their diagnosis.

Other tools use AI to analyse information collected by sensors worn by patients in order to detect signs of deterioration in their health and prompt early intervention, thus potentially preventing unnecessary hospital admissions. AI apps that monitor and support patients' **adherence to treatment** have been trialled with promising results, for example, in patients with tuberculosis. AI tools could also enable old people, for example, to live independently at home for longer.

Limitations and risks of artificial intelligence

The examples above illustrate the potential positive impact that AI can have on healthcare. They include potential time savings for healthcare professionals, reduced costs, and development of tools that can help support patients take control of their health. But, as with any new technology, there may be unrealistic expectations. Artificial Intelligence also has risks. Limitations and concerns include both technical and ethical / legal issues, which are sometimes closely connected.

On a technical level, AI depends on the availability of very large amounts of **good/quality data**. If the available data are not enough, not good quality, inconsistent, or biased, this limits the potential of AI to be useful. AI also has the potential to make wrong decisions; **reliability and safety** are particularly critical in healthcare, where errors can have serious consequences. This raises questions of **accountability**, liability, and redress. The underlying logic of AI systems and their algorithms that results in certain outputs or decisions can be impossible to ascertain ("black box" effect). Machine learning systems adjust themselves as they "learn", which can lead to problems in validating the outputs.

---

[27] Purtill C, How AI changed organ donation in the US, Quartz (2018), https://qz.com/1383083/how-ai-changed-organ-donation-in-the-us/

[28] McCall B. COVID-19 and artificial intelligence: protecting health-care workers and curbing the spread. Lancet Digital Health 2020 Apr; 2(4): e166–e167., https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7129544/

Ethicists have identified a risk on **limiting human autonomy** if AI were to make a calculation on risk or restrict a patient's right to free, fully informed choice of (for example) treatment, if an AI system made certain decision based on what it "thinks" is the best for the patient. Human oversight of the system and the decisions flowing from it is thus particularly important in healthcare.

Lack of **interoperability** and **standardisation** of data sets, such as electronic health record systems, is a major challenge. Sometimes traditional analytical methods outperform machine learning, or the addition of AI does not improve results.[29] As with any scientific endeavour, correct use of AI hinges on whether the correct scientific question is being asked, and whether one has the right high-quality data to answer that question. As machine learning is based on patterns in big data, the system is only as good as the data that is fed to it.

Biases in data also introduce ethical issues in terms of the potential for AI-enabled decisions themselves to be biased or discriminatory. Biases in data collection can affect the type of patterns AI will identify. This is an issue since, for example, women and ethnic minorities are often under-represented clinical trials and large data sets used to train AI. Bias in the data will have an effect on the algorithm that is developed, replicating the bias found in society.[30] Patients with multiple or rare diseases may also be affected by this.[31] Other issues need to be considered in using AI relate to fundamental rights, privacy and protection of personal data; the latter is covered in more detail in the next section.

A rather specific concern is that artificial intelligence might be so good at picking up anomalies, for example in medical imaging such as x-rays and MRI scans, that it will end up **increasing overdiagnosis** and overtreatment. As people age, most develop some anomalies that do not cause any symptoms and do not need treating; furthermore, some cancerous growths never become malignant. Symptom checker apps present an interesting case, as "their recommendations might be overly cautious, potentially increasing demand for unnecessary tests and treatments."[32] Overdiagnosis by AI can increase the number of unnecessary medical interventions and – as any medical intervention carries potential risks – actually increase harm to patients.[33] A key challenge will be to develop a system that can recognise those anomalies there the patient will really benefit from treatment.

Public-private partnerships between national health systems and large multinational corporations or AI developer companies – such as IBM, DeepMind, and Babylon Health in the UK– have raised concerns about private companies gaining access to people's sensitive data, often without their consent or knowledge. Lack of AI expertise in the public sector may also inadvertently lead to an embedding of corporate actors – who bring specialist knowledge but also their own interests and agendas – in public health systems. This is potentially a serious issue when it comes to establishing public trust in the new technologies.[34]

Finally, an important limitation and ethical implication of AI is that it does not possess all **human qualities** that have a bearing on healthcare – which is fundamentally about human relationships. "Clinical practice often involves complex judgments and abilities that AI currently is unable to

---

[29] Austin PC, Tu JV, Lee DS, Logistic regression had superior performance compared with regression trees for predicting in-hospital mortality in patients hospitalized with heart failure, J Clin Epidemiol. 2010 Oct;63(10):1145-55. doi: 10.1016/j.jclinepi.2009.12.004. Epub 2010 Mar 21.https://www.ncbi.nlm.nih.gov/pubmed/20304609

[30] Nuffield Council on Bioethics, Artificial intelligence (AI) in healthcare and research (2018)

[31] Treviranus J., Sidewalk Toronto and Why Smarter is Not Better (2018), https://medium.com/datadriveninvestor/sidewalk-toronto-and-why-smarter-is-not-better-b233058d01c8

[32] Nuffield Council on Bioethics, Artificial intelligence (AI) in healthcare and research (2018)

[33] https://www.theverge.com/2020/1/27/21080253/ai-cancer-diagnosis-dangers-mammography-google-paper-accuracy

[34] Nuffield Council on Bioethics, Artificial intelligence (AI) in healthcare and research (2018)

replicate, such as contextual knowledge and the ability to read social cues."[35] Technology, if used to replace real human contact, may actually increase social isolation. Moreover, some systems called "social AI", such as virtual reality avatars, interact with humans by simulating human social characteristics. Confusion "between humans and machines could have multiple consequences such as attachment, influence, or reduction of the value of being human. The development of human-like robots should therefore undergo careful ethical assessment."[36]

Sharing and protecting patients' data

Privacy is a fundamental right enshrined in international conventions and in EU law – Articles 7 and 8 of the EU Charter of Fundamental Rights. It is also potentially affected by Artificial Intelligence. Therefore, this section is specifically focused on data-related issues, some of which are ethical.

EPF's work with its members has found that generally patients are comfortable and willing to share their health data. Patients understand its vital importance for advancing health research, helping other patients, and ultimately benefiting society. Effective and ethical sharing of patient data is important for finding solutions to patients' unmet needs, not only but especially in rare diseases; and to develop solutions for improving quality of care, treatment pathways, and patients' quality of life. However, protection of patients' privacy is a key element in engendering trust.[37] As described in EPF's 2016 position paper on eHealth, "undue disclosure of medical information can have very negative consequences for patients, whether at work or in other areas of their life. Stigma is still attached to some medical conditions in various EU countries."[38] At the same time, it impossible to do research and discover or advance treatments without the necessary data. Therefore, a balanced approach to data privacy is crucial.

Data privacy and *data protection* are very closely interconnected, so much so that users often think of them as synonymous. But the distinctions between data privacy vs. data protection are fundamental to understanding how one complements the other. Privacy concerns arise wherever personally identifiable information is collected, stored, or used. Data privacy is about authorized access — who has it and who defines it. Data protection is about securing data against unauthorized access. Another way to look at it is this: data protection is essentially a technical issue, whereas data privacy is a legal one.

Data privacy cannot be ensured unless the personal data is protected by technology. If someone can steal personal data, its privacy is not guaranteed, which puts the person the data refers to at risk for identity theft and other personal security breaches. But the opposite relationship is not always true: personal data can be *protected* while still not being reliably *private*. This is the case if someone voluntary decides to share his data with another person or institution, the data will not be private anymore, but if the right technical infrastructure is in place, the data will be protected.

Protection of the user's data includes "both the information initially provided by the user as well as information generated about the user over the course of their interaction with the system … Digital records of human behaviour may allow AI systems to infer not only individuals' preferences, but also

---

[35] Ibid.

[36] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (2019), p.33, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai,

[37] EPF position paper on eHealth (2016); Courbier et al.,"Share and protect our health data: an evidence based approach to rare disease patients' perspectives on data sharing and data protection - quantitative survey and recommendations", *Orphanet Journal of Rare Diseases* (2019) 14:175, https://ojrd.biomedcentral.com/articles/10.1186/s13023-019-1123-4

[38] EPF, EPF position paper on eHealth (2016); https://www.eu-patient.eu/globalassets/policy/ehealth/epf-final-position-paper-on-ehealth_19december2016.pdf

their sexual orientation, age, gender, religious or political views. To allow individuals to trust the data gathering process, it must be ensured that data collected about them will not be used to unlawfully or unfairly discriminate against them." [39]

In order to ensure data protection, different techniques can be used. Although similar, *anonymisation* and *pseudonymisation* are two distinct techniques that permit to use de-identified data. The difference between the two techniques rests on whether the data can be re-identified.[40] True data anonymisation is extremely difficult, if not impossible, which means that in practice, all data is actually pseudonymised. Through pseudonymised data, data controllers can benefit from new, more unrestrained standards under the GDPR: for instance, Article 6(4)(e)[41] permits the processing of pseudonymised data for uses beyond the purpose for which the data was originally collected. The challenge here focuses, as briefly mentioned above, on ensuring that data collected from individuals (e.g. through wearables) does not end up to be used in ways to the detriment of the patients (e.g. to restrict or deny coverage or increase premiums of healthcare insurances).

Blockchain technology[42] offers possibilities for improving data security – including cybersecurity in hospitals, for example. Blockchain is a public record of transactions. It is also distributed, so instead of one person controlling everything, there are thousands of computers around the world connected to a network, and these thousands of computers together come to an agreement on which transactions are valid. Whenever someone makes a transaction, it is broadcasted to the network, and the computers run complex algorithms to determine if the transaction is valid. If it is, they add it to the record of transactions, linking it to the previous transaction. This chain of linked transactions is known as the blockchain. Since the transactions all reference the one before them, you can figure out which ones came first, thus ordering them.

The EU is supporting several projects on blockchain technologies under its current research framework programme Horizon 2020.[43] The technology is also relevant in domains such as patient records, protection and interoperability of data between systems, helping to fight counterfeit medicines, protecting large pools of patient data, and creating virtual infrastructures to better control and disseminate clinical trials data.[44]

> The "**My Health My Data**" EU-funded project looks at the potential that all the data generated and stored every year can have if analysed with the help of blockchain. Data can have enormously beneficial effects on health research and practice, yet privacy breaches can be damaging. Blockchain is used for different objectives in the project: (1) to increase security and provide the capacity to detect any fraudulent activities in real time, and (2) to de-identify and encrypt data, thus making its use more secure. The results of this project will show to what extent Blockchain can provide a solution in the area of healthcare.
>
> http://www.myhealthmydata.eu/

---

[39] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (2019), p. 19

[40] The GDPR defines anonymized data as "data rendered anonymous in such a way that the data subject is not or no longer identifiable.". By contrast to anonymisation, Article 4(5) of the GDPR defines pseudonymisation as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information (key-coding system)"

[41] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[42] https://en.wikipedia.org/wiki/Blockchain

[43] European Union Blockchain Observatory & Forum), What happened at the European Union Blockchain Observatory & Forum workshop on Use cases in healthcare in Frankfurt on 4 September, 2019, (2019) https://www.eublockchainforum.eu/news/feeling-good-healthcare-data-and-blockchain

[44] Brickwood B., Blockchain: the trust solution for the healthcare industry?, Health Europa (2020), https://www.healtheuropa.eu/blockchain-the-trust-solution-for-healthcare/96840/

Overview of related EU policy developments

This section outlines key EU policy developments relating to digital health, up until the most recent European Commission overarching strategy on digital,[45] released in February 2020.

Digital health as an EU policy priority

One of the headline priorities of the new European Commission that took office on 1 December 2019, set out in the [political guidelines](#) of Commission President Ursula von der Leyen, is **"A Europe fit for the digital age"**.[46] From this overall priority flow several areas of action.

The mission letter of Stella Kyriakides,[47] Commissioner for Health, included a mandate to create a so-called **European Health Data Space** "to promote health-data exchange and support research on new preventive strategies, as well as on treatments, medicines, medical devices and outcomes" in compliance with the EU data protection rules. As part of this it should be ensured that citizens have control over their own personal data.

On 19 February 2020, the Commission published several documents to take forward its strategy on digital health:

- A communication titled "**Shaping Europe's digital future**"[48] which sets out priority actions under three headings: technology that works for people; a fair and competitive economy; and an open, democratic and sustainable society – all of which relate to health in some way. Artificial intelligence is included under the first heading; the EU data strategy under the second, and a proposal on electronic health records under the third heading.
- A communication titled a **"European strategy for data"**[49]
- A white paper "**Artificial intelligence – a European approach to excellence and trust**"[50]

The 2020 strategy builds on previous publications, including key documents addressing the future of digital health in Europe. In April 2018, the Commission presented its **communication on the digital transformation of health and care in the digital single market** (COM (2018) 233 final),[51] which set out its plan on digital health for the coming years. The Communication includes measures to enable people to access and share their health data safely; to pool data across Europe to boost research and spur the development of personalised medicine; and for scaling up of digitally-enabled person-centred care models. The three pillars are all relevant to EPF's vision on person-centred digital health.

---

[45] European Commission, A Europe Fit for Digital Age 2020 Strategy (2020), https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en#introduction

[46] Von der Leyen U., A Union that strives for more – My Agenda for Europe (2019), https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[47] European Commission, Mission Letter – Stella Kyriakides (2019), https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-stella-kyriakides_en.pdf

[48] European Commission, Communication - Shaping Europe's Digital Future (2020), https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[49] European Commission, A European strategy for Data, COM(2020) 66 final, Brussels 19.02.2020, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

[50] European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, Brussels 19.02.2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[51] European Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 final, Brussels, 25.04.2018, https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

In January 2019, the European Commission's Expert Panel on effective ways of investing in Health (EXPH) published a report "Assessing the impact of digital transformation of health services", in which the group proposes a framework for assessment the impact of the Commission's strategy and generating the evidence required for decision-making to embed digital health in the healthcare systems.[52]

In a Recommendation published in February 2019,[53] the European Commission also addressed the issue of a **European Electronic Health Record (EHR) exchange format**. The recommendations included in the document are structured around tree main pillars; (1) a set of principles governing access and exchange of EHRs, (2) common technical specifications, and (3) further collaboration. Amongst other things, the Recommendation calls for a baseline exchange format for patient summaries and refers to several elements identified as important to patients. In particular, the Recommendation focus on better access to EHRs, data security and safety, EHRs sharing freedom of choice for patients, and an overall citizen-centred approach. EPF welcomed the Recommendation as a step towards a patient-centred European digital health framework, while calling for stronger involvement of patients considering their needs and preferences to achieve the Recommendation's vision.[54]

EPF explored patients' views on EHRs through a dedicated survey in 2019.[55] The survey results show that many patients across the EU either do not have access to their EHRs or are not aware of it. In addition, EHR information should be easier to find and understand. The survey results also show that patients would like to be able to better interact with their EHR, by providing comments and new information, reporting inaccuracies, etc.

EU policy on big data

The idea of big data has been central to developing plans for a European Digital Single Market. In 2017, the European Commission published a **Communication on a *European data economy***.[56] The document does not, in itself, refer to "big data" but states that data "has become an essential resource for economic growth, job creation and societal progress. Data analysis facilitates the optimisation of processes and decisions, innovation, and the prediction of future events. This global trend holds enormous potential in various fields, ranging from health, environment, food security, climate and resource efficiency to energy, intelligent transport systems and smart cities." By "data economy" the Commission refers to "an ecosystem of different types of market players – such as manufacturers, researchers and infrastructure providers – collaborating to ensure that data is accessible and usable. This enables the market players to extract value from this data, by creating a variety of applications with a great potential to improve daily life (e.g. traffic management, optimisation of harvests or remote health care)."

In 2018 the Commission announced a package of initiatives relating to data, including the health-specific Communication, "**Enabling the digital transformation of health and care in the Digital Single**

---

[52] Expert panel on effective ways of investing in Health (EXPH), Report – Assessing the impact of digital transformation of health services (2019),
https://ec.europa.eu/health/expert_panel/sites/expertpanel/files/docsdir/022_digitaltransformation_en.pdf
[53] European Commission, Recommendation on a European Electronic Health Record exchange format, C(2019) 800 final, Brussels 06.02.2019, https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format
[54] EPF, Response to EC Recommendation on EHR exchange format (2019), https://www.eu-patient.eu/globalassets/news/ehr_epfresponse.pdf
[55] Full results to be published on www.eu-patient.eu
[56] European Commission, Communication – Building a European Data Economy, COM (2017) 9 final, Brussels, 10.01.2017, https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy

Market: empowering citizens and building a healthier society", which we have referred to above, and another Communication on ''**Artificial intelligence for Europe**,'[57] setting out the European approach on AI, further elaborated in the following section of this paper.

A European Commission study from 2016, *Big Data in Public Health, Telemedicine and Healthcare,*[58] addresses healthcare specifically. It gives examples of existing applications of big data identifying 10 priorities in relation to the topic and give 10 policy recommendations.

The policy recommendations can be summarised as follows:

- Communication to increase awareness of the added value of big data in health.
- Education and training to ensure health workers can use its potential.
- Expand existing data sources and explore new ones, while securing quality and safety.
- Promote open use and sharing without compromising privacy and confidentiality.
- Targeted analysis of big data in health based on needs and interests of stakeholders.
- Identify potentials of big data analysis and improve analytical methods.
- Governance mechanisms to ensure secure and fair access and use of big data for research.
- Standards for big data in health, e.g. for better interoperability.
- Purposeful investment steered by the European Commission.
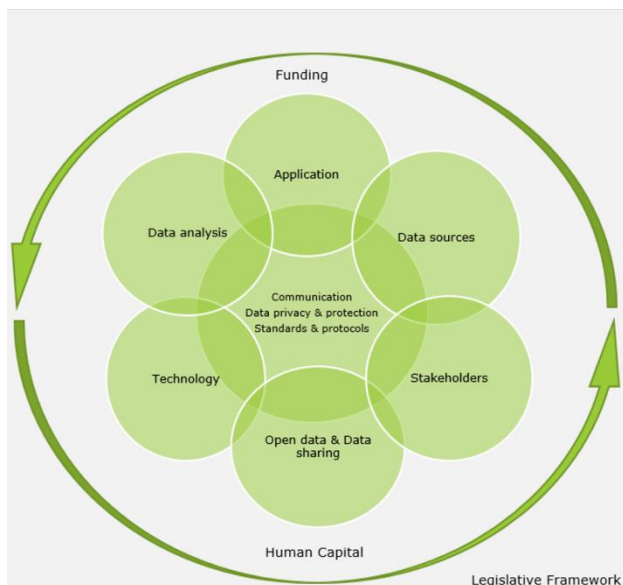- Clarify and align existing legal and privacy regulation of big data in health.

The European Economic and Social Committee's 2017 study, *Ethics of big data: Balancing economic benefits and ethical questions of big data in the EU policy context*, proposes five actions to help find a balance between making most out of the use of big data, while at the same time protecting fundamental human rights. The proposals, listed below, are mostly not health specific.[59]

1. *An EU privacy management platform*. The report suggests that citizens should be empowered by providing them with a concrete instrument to take control over their data. This can be done via establishment of a pan-European we portal where citizens could know all about entities, both public and private, that have stored, processed, shared, or re-used their personal data.

2. *Ethical Data Management Protocol.* It could be possible to design a "sound European certification system" to identify "virtuous" companies in the field of data protection.

3. *Data Management Statement.* Organisations could submit declarations on how they collect, use, or eventually sell personal data coming from customers and in general business activities. The statement proposed would describe companies' adopted policies, description of the data collected, and plans.

4. *European eHealth database*. This would entail a European database that would contain health-related data of citizens, based on consent. Data access would be managed differently for different stakeholders.

5. *Digital education on big data*. To create a broader digital culture a series of educational programmes is envisaged, aimed at different age groups. These would include curricula on big data for schools, universities and research institutes, MOOCs (massive open online courses) for the general population, and others.

---

[57] European Commission, Communication – Artificial Intelligence for Europe, COM(2018) 237 final, Brussels, 25.04.2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625

[58] European Commission, Study on Big Data in Public Health, Telemedicine and Healthcare (2016), https://ec.europa.eu/digital-single-market/en/news/study-big-data-public-health-telemedicine-and-healthcare

[59] European Economic and Social Committee, Study – The Ethics of Big Data (2017), https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/ethics-big-data

Fields of policy action and their interactions

(Source: Study on Big Data in Public Health, Telemedicine and Healthcare, 2016)

As previously mentioned, in 2020 and as part of its new overarching approach on digital, the Commission released a dedicated Communication '**A European strategy for data'.**[60] The Communication recognises the rising importance of data in our society and economy and the defines strategic elements to make the EU a global leader in a data-driven society. The Strategy focuses on the creation of a single market for data, which would enable data flow within the EU and across sectors, full respect of European rules, in particular privacy and data protection, and ensure fair, practical and clear rules for access and use of data.

> *"**Individuals value the high level of protection granted by the GDPR and ePrivacy legislation. However, they suffer from the absence of technical tools and standards that make the exercise of their rights simple and not overly burdensome"***
>
> *Communication - A European Strategy for Data, 2020*

The Commission identifies several **challenges** to its goals, including infrastructure gaps, issues in data availability, interoperability, security and governance and imbalances in market power. Improving skills and data literacy and the empowerment of individuals to exercise their rights granted by EU legislation (GDPR and ePrivacy) are also clearly identified as crucial issues to be tackled by the future strategy.

To realise its vision and address the mentioned challenges, the Strategy identifies as set of key pillars:

- o A cross-sectoral governance framework for data access and use, including a Data Act and review of the existing policy framework
- o Investments in data and strengthening Europe's data infrastructure, interoperability, and cloud services; enhanced capacity building for SMEs
- o Empowering individuals, for example by enhancing the portability right for individuals[61] and more control over access and use of data
- o Investing in skills and general data literacy, in particular through an updated Digital education Action Plan[62]

---

[60] European Commission, A European strategy for Data, COM(2020) 66 final
[61] General Data Protection Regulation (GDPR), Art 20, Regulation(EU) 2016/679, https://gdpr.eu/article-20-right-to-data-portability/
[62] The updated Digital Education Action Plan will reinforce better access to and use of data as one of its key priorities, in order to make education and training institutions fit for the digital age and equip them with the capabilities needed for making better decisions and improving skills and competences.

The last pillar, finally, promotes the development of **European data spaces** in strategic sectors, including healthcare. The framework for a **European health data space** described in the Strategy focuses on the importance of enhancing use and re-use of health data: to improve health systems sustainability through evidence based decision making, to innovate the healthcare sector, to

"A Common European health data space, [...] essential for advances in preventing, detecting, and curing diseases as well as for informed, evidence-based decisions to improve the accessibility, effectiveness and sustainability of the healthcare systems"

Communication – A European Strategy for Data, 2020

contribute to the competitiveness of the EU's industry and to support the work of regulatory bodies in healthcare. Particular attention is also devoted to citizens' rights, access and management of their data. Broader access to Electronic Health Records and data portability; consent and ethical use of data and less fragmentation in the GDPR and digital health services landscape (within and across borders) are clearly identified as key elements of a potential European Health Data Space.

To achieve the Health Data Space, the Commission proposes a set of options:

- Develop sector-specific legislative or non-legislative measures for the European health data space, complementing the horizontal framework of the common data space.
- Facilitate the establishment of a Code of Conduct for Processing of personal data in health sector (Art. 40 of the GDPR).
- Deploy infrastructures, tools and capacity, in particular to support development of EHRs and their interoperability.
- Enable exchange of electronic patient summaries and ePrescriptions between Member States participating in the eHealth Digital Service Infrastructure (eHDSI) by 2022
- Enhance cross-border exchanges and virtual consultation model and registries of the European Reference Networks.

EU policy on artificial intelligence

Leading the debate at EU level, the European Parliament[63] in January 2017 called on the European Commission to assess the impact of artificial intelligence and made wide-ranging recommendations on civil law rules on robotics. The European Economic and Social Committee (EESC) also issued an opinion in May 2017.[64] Against this background, the European Council of October 2017 invited the Commission to put forward a European approach to artificial intelligence.[65]

On 10 April 2018, 25 European countries signed a Declaration of cooperation on Artificial Intelligence.[66] Moreover, the Commission adopted a **Communication on "Artificial intelligence for Europe"**, outlining the EU's strategy on this topic. The strategy has three dimensions: boosting Europe's technology and industrial capacity; preparing for socio-economic changes; and ensuring an

---

[63] European Parliament, Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html
[64] Artificial Intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (own-initiative opinion) (2017), https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence-consequences-artificial-intelligence-digital-single-market-production-consumption-employment-and
[65] European Council, European Council meeting (19 October 2017) – Conclusions, https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf
[66] https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence

appropriate ethical and legal framework.[67] Building on the Communication, few months later the Commission presented a coordinated plan prepared with Member States to foster the development and use of AI in Europe.[68] In particular, the plan revolves around enhanced coordination in four key areas: increasing investment, making more data available, fostering talent and ensuring trust. Stronger coordination is essential for Europe to become the world-leading region for developing and deploying cutting-edge, ethical, and secure AI.

To collect inputs on its AI work, the Commission also launched a **High-Level Expert Group on Artificial Intelligence (AI HLEG)**, composed of 52 appointed experts comprising representatives from academia, civil society, and industry. In April 2019, the High-Level Expert Group presented its *Ethics guidelines for trustworthy artificial intelligence*. This document considers AI from the perspective of the fundamental rights enshrined in the EU Charter of Fundamental Rights and in international conventions. The AI HLEG concludes that AI which is beneficial for human societies, individual and societal wellbeing must be human-centric; the benefits of technology must be maximised while its risks and unintended adverse consequences must be minimised.[69] The Ethics Guideline sets out four ethical principles that must be ensured in a future EU framework on AI:

1. *Respect for human autonomy*. Humans interacting with AI must be able to maintain their self-determination and should not be coerced, deceived, or manipulated. AI systems should have human oversight.
2. *Prevention of harm*. AI must not cause or exacerbate harm to people, society, or the environment, but should protect human dignity and enhance people's mental and physical integrity. Particular attention must also be paid to situations where there is asymmetry of power or information.
3. *Fairness*. Fairness relates to equal opportunity, freedom of choice and a just distribution of benefits and costs: freedom from bias, stigmatisation and discrimination, and access to effective redress to challenge decisions made by or with AI.
4. *Explicability*. Explicability relates to the transparency of processes, the capacities, and purposes of AI systems, as well as decisions reached by them as far as possible. Other measures such as traceability, auditability and transparent communication are critical as sometimes AI systems are too complex to be fully understandable.

The authors then propose **seven principles** that must be realised for trustworthy AI (see illustration on the following page).

All are equally important and complementary, but the way they are applied will depend on the context. All principles should be applied and monitored throughout a product's lifecycle. The fifth principle of diversity also refers to **stakeholder participation**. This is relevant in terms of patient participation in the design and development, evaluation, and governance of AI-enabled systems in healthcare.

---

[67] European Commission, Communication – Artificial Intelligence for Europe, COM(2018) 37 final, Brussels, 25.04.2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625
[68] European Commission, Communication – Coordinated Plan on AI, COM(2018) 795 final, Brussels, 07.12.2018, https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence
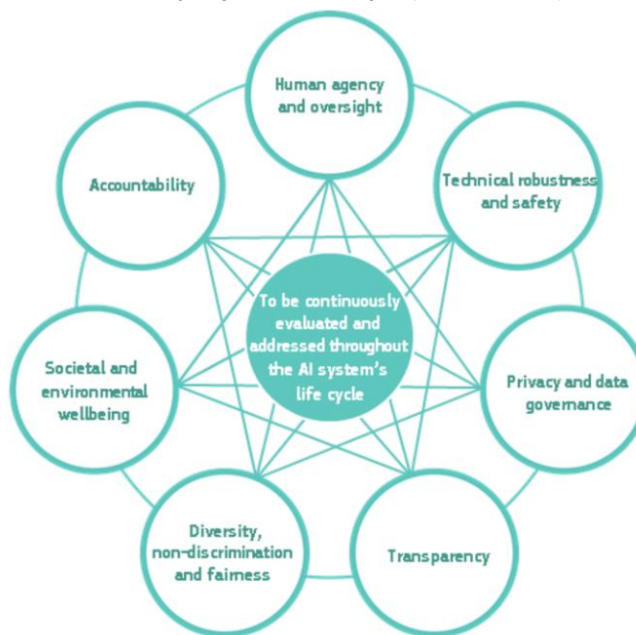[69] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (2019), https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

At European level it is recognised that **healthcare has different and specific issues** and indeed the Commission is moving towards the adoption a sector-specific approach to Artificial intelligence. In particular, the above-mentioned High-Level Expert Group organised a series of workshops, in April 2020 with a specific focus on recommendations for the healthcare sector.[70] These recommendations will be shaped in a specific Annex to the 2019 AI HLEG Report – Policy and investment recommendations for trustworthy Artificial intelligence.[71] The annex will be published in July 2020.

As part of its five-years digital strategy, in February 2020 the European Commission published its **White Paper on Artificial intelligence** – a European approach to excellence and trust.[72] The White Paper sets out policy options to enable trustworthy and secure development of AI in Europe, while addressing values and rights of EU citizens. To this end, the Paper revolves around two main building blocks: develop a policy framework to foster an '**ecosystem of excellence**' supporting the entire AI value chain, and define the priorities for a future regulatory framework for AI, aimed at creating an '**ecosystem of trust**'.

The '**ecosystem of excellence**' should support the development and uptake of AI

Seven Principles for Trustworthy AI (AI HLEG, 2019)

across the EU economy and public administration. The Paper proposes a set of actions building on the Commission's 2018 strategy on AI[73] and 2018 Coordinated Plan.[74] The actions include improved cooperation between Member States, streamlined research and improved investments, a new public-private partnership in AI, data, and robotics. To achieve excellence, the White Paper also includes a focus on skills and education, both in terms of upskilling the European workforce to and to increase awareness of AI at all levels: "*The updated Digital Education Action Plan […] will also increase awareness of AI at all levels of education in order to prepare citizens for informed decisions that will be increasingly affected by AI*". [75]

---

[70] EPF participated in the workshop organised on 21 April 2020.
[71] AI HLEG, Study – Policy and investment recommendations for trustworthy Artificial Intelligence (2019), https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence
[72] European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM (2020) 65 final. Brussels, 19.2.2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
[73] European Commission,Artificial Intelligence for Europe, Brussels, 25.4.2018, COM(2018) 237 final https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF
[74] European Commission, Coordinated Plan on Artificial Intelligence (2018), Brussels, 7.12.2018, COM(2018) 795 final, https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0002.02/DOC_1&format=PDF
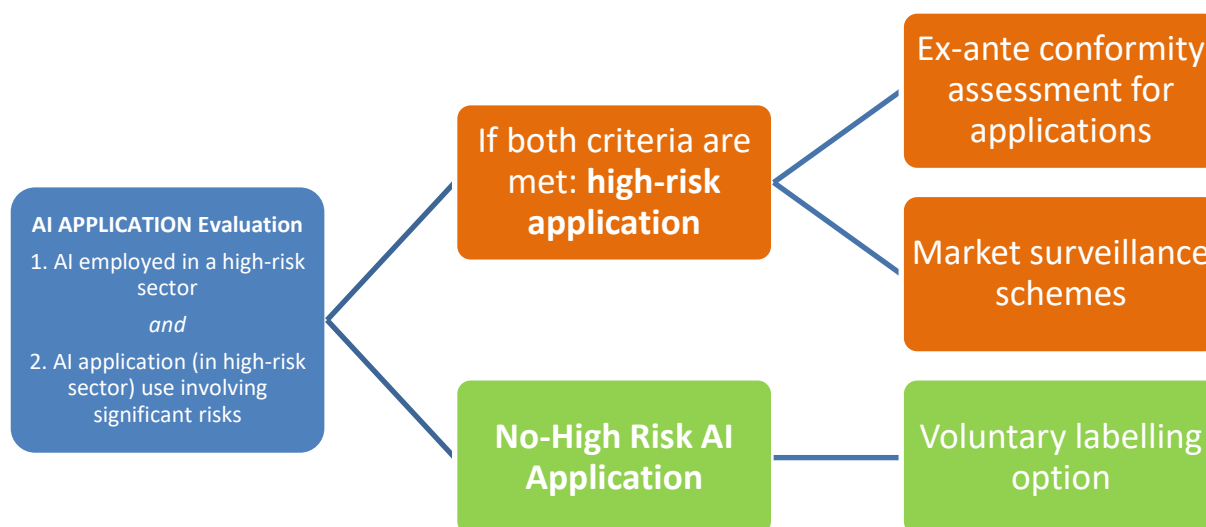[75] European Commission, White Paper on AI (2020)

The second pillar of the AI White Paper is centred on the importance of creating an **'ecosystem of trust'** for AI through a revised and updated clear European regulatory framework. The framework would have to consider both the transformative potential of AI but also potential risks and challenge. New legislation should therefore be effective and adapted to the risks, while not limiting innovation.

"A solid European regulatory framework for trustworthy AI will protect all European citizens and help create a frictionless internal market for the further development and uptake of AI as well as strengthening Europe's industrial basis in AI"

European Commission – White Paper on AI, 2020

To achieve this complex goal, the Commission sets out a **risk-based approach**, identifying two key cumulative criteria for the identification of ''high-risk'' applications. AI applications should be identified as ''high-risk'' if both the sector of employment <u>and</u> the intended use involve significant risks, in terms of safety, consumer rights and fundamental rights. The White Paper actually focuses on healthcare as a key example for this approach. **While healthcare is clearly acknowledged as one of the ''high-risk'' sectors**, the Paper highlights how 'softer' application of AI in healthcare, for example AI-driven appointment scheduling system in a hospital, would not be flagged as ''high-risk''.[76]

Illustration based on European Commission White Paper on AI (2020)

AI APPLICATION Evaluation
1. AI employed in a high-risk sector
and
2. AI application (in high-risk sector) use involving significant risks

If both criteria are met: high-risk application

Ex-ante conformity assessment for applications

Market surveillance schemes

No-High Risk AI Application

Voluntary labelling option

For high-risk AI application, the Commission **identifies the need for a pre-marketing prior conformity assessment to verify and ensure compliance with a set of additional mandatory requirements**. This set of additional requirements, building on the abovementioned guidelines of the High-Level Expert Group, would consist of a number of key features largely focused on transparency, data traceability and human oversight.

In addition to the mandatory conformity assessment, the Commission proposes an option for **voluntary labelling scheme for** non-high-risk AI application, to facilitate users' recognition of trustworthy AI-enabled products and services. The White Paper finally identifies the need for a dedicated European governance structure on AI as a key tool to avoid fragmentation and increase

---

[76] The White Paper on AI clearly identifies that already existing specific rules for certain sectors, including healthcare (e.g. Medical devices), would continue to apply in relation to AI.

capacity, in particular for testing and certification. Such structure should take the form of a framework for cooperation of national competent authorities, guarantee stakeholders participation, and avoid duplication of existing structures.

A **report by the Commission's Expert Group on the safety and liability implications** of AI, released as accompanying document to the White Paper, concludes that emerging technologies – AI, the Internet of Things and robotics – raise new challenges for product safety and liability. While EU product safety legislation is based on the principle that all products and services put on the market should be safe throughout their lifespan, it contains gaps that will need to be addressed. Features of AI that challenge the current legislative framework include its connectivity,[77] dependency on certain amounts and quality of data, autonomy, and opacity,[78] complexity of the products and systems, software updates and complex safety management and value chains. Liability legislation needs to be looked at to ensure users have the same level of protection and access to compensation whether they use traditional or AI-enabled technology. [79]

Data Protection, Big Data and AI

Since May 2018, the *General Data Protection Regulation* (GDPR),[80] is applicable in the EU. This legislation aims at providing a common set of data protection rules for all companies operating in the EU, regardless of where they are based. The GDPR deals with both data security and privacy. The GDPR provides more rights to citizens and tries to ensure that people are better informed about the use of their personal data. It also clarifies the responsibilities when using data and entities using personal data. For more information, please see our guide to the GDPR and how it affects patients and patient organisations.[81]

While the GDPR is an improvement on the previous Directive in various respects, patients' organisations should monitor several areas in implementation to ensure patients' rights are respected and to advocate for patient empowerment. In particular, and as stated in EPF's position on Data Protection, of our key concerns is to ensure that individual rights which apply to patients –access to one's personal data, transparent information about processing, and the right to be forgotten or to erase data – are effectively implemented, with patient friendly information and transparent processes.[82]

EPF also calls for more cooperation between Member States on minimum security requirements to ensure an equivalent level of protection of personal data shared by patients across the European Union and to facilitate cross-border healthcare and research.

---

[77] Connectivity can in itself pose a safety risk (a device connected to the Internet may be hacked) but also indirectly (a device that loses connectivity may malfunction).

[78] Some AI-based products may "learn" and improve their own performance over time with less or no human oversight, thus making it more difficult or even impossible to understand how algorithmic decisions have been reached. The report recommends that algorithms should be made sufficiently transparent to enable trace back in case decisions need to be reviewed.

[79] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19.2.2020, https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf

[80] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679

[81] EPF, The new EU Regulation on the protection of personal data: what does it mean for patients? – A Guide for patients and patients' organisations (2016), https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf

[82] https://www.eu-patient.eu/whatwedo/Policy/Data-Protection/

With the rise of AI, the projected growth of global data volume figures[83] and the new European digital strategy, the existing European data protection provisions could undergo a revision process. As foresee by the Article 97 of the GDPR,[84] the Commission shall submit a report by May 2020 on the evaluation and review of the Regulation. This public report, to be submitted to the European Parliament and to the Council, could represent a starting point to adapt the GPDR and take into account revision needs already considered within the abovementioned Data Strategy and Artificial Intelligence White Paper.

Of particular interest for the patients community is, for instance, the reference made in the Data Strategy Communication **on enhancing the portability right**[85] for individuals regulated under Article 20 of the GDPR, therefore giving them more control over who can access and use machine-generated data.[86] The Strategy also focusses on the importance of data protection for the development of stronger data infrastructures and technologies, such as cloud infrastructures and services.

The promotion of the development of sectorial Common European Data Spaces, in particular the European Health Data Space, also calls for adjustments and more tailored data protection frameworks due to the specificity of challenges related to specific domains of public interest. In this respect, the Data Strategy clearly mentions the **establishment of a Code of Conduct** for processing of personal data in health sector, in accordance with Article 40 of GDPR.[87] Addressing use and data protection fragmentation within and between Members States is also considered as a crucial element of a successful development of a European Health Data Space.

Data protection is also crucial when addressing the rise of AI as a core element of digitalisation. The 2020 White Paper, while pointing out the existence of ad-hoc rules already included in the EU data protection legislation,[88] also mention the need for monitoring current legislation application in view of AI adoption. In particular, the Commission stresses the importance of examining whether AI systems pose additional risks for fundamental rights, including data and privacy protection and non-discrimination.

The **COVID-19 emergency**, finally, added a new layer of complexity to data protection in Europe, tackled by the European Commission with dedicated guidance on the development of new apps that support the fight against coronavirus.[89] The guidance aims to offer the necessary framework to guarantee sufficient protection of personal data and limitation of intrusiveness, ensuring effectiveness and compliance of such tools even in times of crisis. Commenting on the guidance, Commissioner for Justice, Didier Reynders, said: "The use of mobile phone apps have the potential to really help in the fight against coronavirus […] At the same time, we are talking about very sensitive data being collected on the health of our citizens, which we are duty-bound to protect."

---

[83] IDC, 'The Digitization of the World From Edge to Core'(2018) https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

[84] https://gdpr.eu/article-97-commission-reports/

[85] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Art. 20, GDPR: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided

[86] European Commission, A European strategy for Data, COM (2020) 66 final, pag. 20.

[87] https://gdpr.eu/article-40-proper-application-of-the-regulation/

[88] E.g. Art. 13(2)(f) GDPR: controllers must, at the time when the personal data are obtained, provide the data subjects with further information necessary to ensure fair and transparent processing about the existence of automated decision-making and certain additional information.

[89] European Commission, Communication - Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, 2020/C 124 I/01, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN

Conclusions

Given the priority accorded to digitalization as an overall EU policy including in health, EPF as a cross-disease umbrella patient organisation is regularly asked to contribute a to patient perspective to various initiatives. Likewise, our member organisations whether working in a disease focus or at national level, are invited to participate in debates and policy discussions around digital health. It is therefore crucial that the patient community continues to be actively engaged in this fast-moving area of EU health policy.

Capacity-building is critical. Public health systems, from policy makers to researchers and healthcare staff to have the needed skills and knowledge to govern and use AI for the benefit of society. Civil society organisations, including patient organisations, also need capacity-building in this area in order to participate meaningfully in public debates related to AI and other emerging technologies.

In addition to capacity building, however, patients' involvement in shaping the future of digital health in Europe needs to be facilitated by more inclusive governance models that enable effective participation and interest representation in all stages. The unique experience that patients can bring in both developing technological solutions (research and innovation process) but also in related policy debates (e.g. on ethics) is fundamental to ensure balanced policies and innovation.

Empowering individuals is crucial. Only through clear and dedicated information and education opportunities, patients can better understand and exercise their rights while exploiting the full benefits of the digitalisation of care. Empowerment and inclusion are vital to guard against exacerbating health inequalities and deepening the digital divide in society. Digital health, data, and AI, can prove challenging for the general population, and lack of empowerment could exacerbate inequalities and hinder individuals from accessing services or exercise their rights. Health literacy will be a critical strategy for patients and for society in general to enhance equity and rights.

With the rapid rise of AI and to exploit its potential positive impact on healthcare, existing regulatory frameworks should be revised, adapted, or complemented to better address the benefits and risks related to artificial intelligence. In particular, it will be important to ensure that high-risk AI applications in healthcare are well defined and subject to an adequate regulatory framework to fully ensure their safety and transparency.

The future development of the European Health Data Space should be also subject to particular attention and a sector specific approach, inclusive of patients' views and build on the key elements outlined in the Data Strategy, including: sector-specific legislative or non-legislative measures, dedicated code of conduct for processing of personal data in health sector, adequate infrastructures and capacity-building, support further development of EHRs at European level.

Definitions of key terms

This section draws on a glossary developed in the context of Digital Health Europe and gives a definition of various terms that have been used in this briefing paper.[90] Please note that these may not be exactly the same definitions that are used by the reports cited in this paper.

Anonymisation	IMI Code of Practice: Process of removing all elements allowing the identification of an individual person (i.e., of rendering data anonymous). ISO/TS 25237:2008: process that removes the association between the identifying data set and the data subject. UK Information Commissioner's Office: process of rendering data into a form which does not identify individuals and where identification is not likely to take place. See also: *Pseudonymisation*.
Anonymised data	IMI Code of Practice: Data which was identifiable when collected but which are not identifiable anymore (have been rendered anonymous). Anonymous data are no longer personal data. UK Information Commissioner's Office: data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place.
Artificial Intelligence	European Commission and AI HLEG - "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)."
Consent	ISO/TS 14265:2011: any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.
Data Controller (or Controller)	IMI Code of Practice: The natural or legal person, or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data.[91]
Data Donation	Data donation research is research in which people voluntarily contribute their own personal data that was generated for a different purpose to a collective dataset.[92]

---

[90] Please note the glossary below was last updated on 12/12/2019. For updates please refer to the Digital Health Europe website: https://digitalhealtheurope.eu/resources/glossary.html

[91] In a clinical trial, the organisation(s) responsible for the trial is usually considered being the controller (for collaborative projects, see EDPS "Opinion related to the clinical study in the frame of the research project PROTECT WP4", issued on 29 November 2012)

[92] https://theoryandpractice.citizenscienceassociation.org/articles/10.5334/cstp.178/

Data Governance	Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.[93]
Data Processor (or Processor)	IMI Code of Practice: The natural or legal person, or any other body, which processes personal data on behalf of the controller.
Data Protection	ISO TS 25237: 2008: technical and social regimen for negotiating, managing, and ensuring informational privacy, confidentiality, and security.
Data Sharing	UK Information Commissioner's Office: the disclosure of data from one or more organisations to a third-party organisation or organisations, or the sharing of data between different parts of an organisation.
Explicit Consent	ISO 18308:2010: permission that is freely and directly given, expressed either viva voice or in writing.
Genetic Data	IMI Code of Practice: All personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.[94] This Code considers only genetic data rich enough to identify a data subject.
Health Data	Under the GDPR, health data is defined as "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*".
Implied Consent	ISO: informational consent that is freely and directly given, indicated by an action or an inaction rather than a formal verbal or written indication of agreement on the part of the data subject.
Medical Data	IMI Code of Practice: Any data concerning patients or study participants health, collected within the context of health care or clinical trials (e.g., name, address, living conditions, health data, life style habits, social security number, image data…).[95]
Person Identification	ISO/TS 25237:2008: process for establishing an association between an information object and a physical person.
Personal Data	IMI Code of Practice: Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Also commonly referred to as Personally Identifiable Information or PII[96].
Privacy	ISO/IEC 2382-8: freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.
Processing*	IMI Code of Practice: Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaption or alteration, retrieval, consultation, use disclosure

---

[93] http://www.datagovernance.com/defining-data-governance/
[94] As defined in Article 4 para (10) of "General Data Protection Regulation"
[95] Unless otherwise specified, medical data refers to individual subject data and not aggregated subject data.
[96] Many guidelines use the term Personally Identifiable Information or PII

	by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Pseudonym	ISO/TS 25237:2008: personal identifier that is different from normally used personal identifiers. Note 1: This may be either derived from the normally used personal identifier in a reversible or irreversible way, or alternatively be totally unrelated. Note 2: Pseudonym is usually restricted to mean an identifier that does not allow the derivation of the normal personal identifier. Such pseudonymous information is thus functionally anonymous.
Pseudonymisation	IMI Code of Practice: Process of removing all elements allowing the identification of an individual person, except the key(s) allowing linking the data to the person. Such key shall be randomly generated and subject to technical and organisational measures to prevent its unauthorised use. ISO/TS 25237:2008: particular type of anonymization that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.
Pseudonymised Data	IMI Code of Practice: Personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution. The only difference between pseudonymised and anonymised data is that in the latter case there exists no key to link data to the data subject.
Re-Identification	IMI Code of Practice: The process of linking de-identified data to the study participant. UK Information Commissioner's Office: process of analysing data or combining it with other data with the result that individuals become identifiable.
Research	IMI Code of Practice: Any scientific research project including clinical trials and fundamental research, aiming at gaining scientific knowledge in the health sector.
Secondary Use of Data (or Data Re-Use)	IMI Code of Practice: Processing of already existing medical data for a purpose different from the purpose for which they have been initially collected.[97] ISO: any legitimate use of a health care record other than for the purpose of supporting the direct delivery of health care services to the subject of care.

---

[97] E.g., medical data collected to conduct a clinical trial on breast cancer used to run a study aiming to identify new biomarkers, but which was not planned in the consent form.