the digital health society
enabled by ECHAlliance

iHD

# Proposing a common basis for health data access across Europe

2021 RECOMMENDATIONS BASED ON CALLS TO ACTION ON HEALTH DATA ECOSYSTEMS

# Round Table 3

# Proposing a common basis for health data access across Europe.

# Working groups based on Calls to Action on Health Data Ecosystems

This report presents the findings of a multi-stakeholder round table consultation, in the form of consensus papers from three Working Groups to examine **the acceptance criteria for societal trust in the use of health data and a recipe for trustworthy digital health: standards, architecture and value.**

The three Working Groups were developed and convened by DHS and i~HD neutrally and independently from the event sponsors, Johnson & Johnson and Microsoft. A total of 50 participants, distributed evenly amongst the Working Groups from EU and international institutions, national governments, industry, academia, hospital management, healthcare professionals, regulators, and patient representatives.

These topics take a deeper dive on three of our 7 2020 Calls to Actions on Health Data Ecosystems, specifically Action 4 (Demonstrate benefits to society from data access, use and reuse), Action 5 (Adopt a risk stratification approach), and Action 6 (Build trustworthy

## CALLS TO ACTION

1 **Raise the digital, literacy & skills of all stakeholders**

2 **Generate and value trustworthy Real World Evidence**

3 **Accelerate interoperability across Europe and globally**

4 **Demonstrate benefits to society from data access, use and reuse**

5 **Adopt a risk stratification approach**

6 **Build a trustworthy framework for data access and use**

7 **Adopt a transformational approach to health data**

framework for data access and use). Consensus papers were developed and agreed through a combination of online meetings, email discussion and shared document editing.

**Working Group 1** considered how nominated health data access decision-making bodies, such as data permit authorities, should best define rules for data access and provide public transparency about data access requests, decisions they make, actual uses of data that occur, any audits of use that they undertake, and the benefits of making good use of health data. The group composed illustrative lists in each of these areas that might be used to frame the development of specific decision rules and be used for communication with the public. It proposed a series of recommended actions for data permit authorities to ensure adequate consultation and transparency.

**Working Group 2** looked at how best to promote the development and adoption of a European multi-stakeholder Compact regarding responsible data use, transparency, accountability and communication. A Compact was proposed as a kind of "soft law" that would be quicker to develop and agree, and more easily updated in the face of technology changes, than a Code of Conduct. The working group considered how a Compact might be developed in a transparent and inclusive way, how it might be promoted to the organisations that need to endorse it, to the public who need to be assured by it and be enforced (possibly with sanctions) to win public confidence and trust.

Working Groups 1 and 2 also both touched on the topic of data reciprocity – a quid pro quo for data access. This is a complex and controversial topic, and both Groups recommended that this subject needs much more multi-stakeholder consultation to develop good and ethically acceptable candidate reciprocity models.

**Working Group 3** looked at the experience over the three years since the GDPR came into force, including the problems of varying interpretation regarding its application to health data reuse. The Working Group examined the possible opportunities for more proportionate data protection risk management that the Data Governance Act and AI Regulation may introduce, alongside the GDPR. Like the other two Groups, this Group also emphasised that health data be used for research that is safe, equitable and for the public good. They considered the different risks and therefore the different levels of data protection that may be needed for research that may involve the analysis of, but not direct access to, subject level data. They also explored key areas of risk management, considering traditional approaches and the learning to date of GDPR's implications.

**All three Working Groups proposed action, consultation and further investigation to advance the trustworthy uses of health data.**

Further Call to Actions will be developed in the next series of roundtables centred on 'Scaling up the availability and reusability of big health data' which will take place in the autumn of 2021.

## WORKING GROUP 1

### TRANSPARENCY AND TRUSTWORTHY DECISION MAKING

## WORKING GROUP 2

### SOCIETAL COMPACT AND RETURNING VALUE FROM DATA USE

## WORKING GROUP 3

### RISK AND REWARD:

DATA PROTECTION FOR NAVIGATING EVOLVING RISK REQUIREMENTS TO REALISE THE BENEFITS OF HEALTH DATA INNOVATION

CALL TO ACTION 6

BUILD A TRUSTWORTHY FRAMEWORK FOR DATA ACCESS AND USE

WORKING GROUP 1

# TRANSPARENCY AND TRUSTWORTHY DECISION MAKING

# Context

There is increasingly a great interest for building on the transformational value of using big data for decision making. The importance and value of accessing large-scale real-world data was seen particularly during the COVID-19 pandemic.  Accessing health data is more complex than in other industry sectors and the diversity of data hinders their use. Harmonizing data access via the European Health Data Space (EHDS) is an important enabler for creating a digital single market and growing societal confidence in data use.

An increasing number of bodies are being established to make data access decisions on behalf of one or more data sources in response to diverse public/private body requests. This includes some Data Permit Authorities being established at a national (Member State) level, such as the trailblazing FINDATA. Such bodies are progressively replacing localised decision-making at regional, registry, cohort or healthcare provider level, which has proved to be complex to administer and complex for data recipients and has given rise to varying decisions for the same type of request.

This Working Group has considered how these dedicated (and usually statutory) health data access decision-making bodies should best define their rules for data access and how they provide public transparency about data access requests, decisions they make, actual uses of data that occur, any audits of use that they undertake and any sanctions they impose, and the benefits of making good use of health data.

This paper brings together several areas on which Working Group members feel it would be valuable to stimulate further multi-stakeholder Europe-wide consultations and consensus building, offering these sections and their lists as starting points for those consultations.

This includes:

1. **Guiding principles for data access decision making bodies**
2. **Types of data use and reuse, transparency and societal value**
    - **Illustrative (non-binding) lists of data reuse purposes that would normally be supported, and not supported**
    - **Criteria for, and categories of, organisation that would usually gain data access at different levels of detail**
    - **Example scenarios illustrating a quid pro quo for data access, showing the value for patients and society**
    - **Information that should be published to support transparency**
3. **Specific issues on which it is recommended to invest in public awareness and engagement**
4. **Implications for the EHDS**

# 1 Guiding principles for data access decision making bodies

The formation of data access decision making bodies, e.g. Data Permit Authorities (DPAs) like FINDATA, that make overarching decisions on behalf of multiple healthcare organisations within a regional country is, in general, welcomed provided that these bodies operate according to trustworthy and transparent principles that are created through open consultation and multi stakeholder engagement. Consistency across Europe will, however, only exist if the majority or all Member States have such bodies or equivalent mechanisms, with harmonised administrative and permission processes including data protection and ethics decisions. This need for consistency applies equally to physical data sharing situations in which data sets are transferred between parties, to remote data access facilities such as data safe havens where the researcher travels to the data, and federated architectures that support distributed querying. Similar decision-making rules can be applied to each of these types of data access.

These bodies need to have systems and processes to provide governance across the data reuse landscape, at times enabling individuals to be made aware of research in which their data has been used, but in all cases providing assurance (ensuring trustworthiness) about multiple possible learning health system, research and innovation uses (for societal good) made using health data.

It is suggested that all data access decision-making bodies across Europe, especially DPAs, should align on a set of principles by which they will establish and operate decision-making rules and provide transparency to the public about decisions they have made and their outcomes.

In addition, data access decision-making bodies should contribute, at national and European levels, to the development and promotion of good models of data altruism (as defined in the Data Governance Act). These models will facilitate consistent and trusted adoption of the Data Governance Act.

The proposed guiding principles and recommended actions arising from these principles are presented on the next page.

## Defining data access policies and rules

**Ensure that the policies and rules developed for data access decision making adequately reflect public preferences and optimally balance differing public viewpoints**

**Be transparent, to all stakeholders and to the public, about the principles and rules that will be applied when evaluating data access requests**

**Specify and publish the data processing conduct expected from all data users, including how this will be monitored and enforced**

### Recommended actions

Consult with the public to agree the societal benefits that health data users should be required to target, and how population and personal preferences for data reuse should be reflected through policies, rules and decisions.

Include a diversity of public strata so that the inputs from the public properly reflect and cater for the diversity of patient and public views across Europe.

Consult with key stakeholders and the wider public on proposed policies and rules for granting access to health data.

Publish the membership of data access decision-making committees.

Involve patients and citizens in decision making bodies (e.g. on boards and committees)

## Making data access decisions

**Provide public information about the uses being made of health data, to a meaningful but practical level of granularity and specificity**

**Be as transparent as is legally permissible about declined data access requests, data breaches or infringements of policies and codes of conduct, and how these have been handled**

### Recommended actions

Publish illustrative examples of the uses of health data that are likely to be supported, and those are unlikely to be supported.

Require the intended benefit of data use to be stated with each data request.

Define binding terms and conditions required of data users, potentially subject to audit, such as only using data for the agreed purposes, by the approved organisations and adopting agreed standards for data protection and security, being transparent about the outcomes.

Encourage data providers to adopt equitable and transparent processes for making data available to other organisations.

## Publicising the outcomes of health data access

**Inform all stakeholders, especially the public, about the societal benefits intended and later achieved through each granted data access request**

**Periodically review the effectiveness and successful outcomes from implementing the data access policies and rules, and revise them to improve the trustworthy value from health data for society**

### Recommended actions

Publish an inventory of data access requests received, accepted, declined and of any investigations into data breaches or misconduct.

Publish the benefits that have been enabled through granting data access, and any lessons learned about reusing health data in a trustworthy way.

As part of transparency, promote (or require) the publication of research findings and other outcomes (whilst not requiring the disclosure of confidential information).

Publish illustrative examples of how different kinds of organisation have created societal value from health data.

Consult with stakeholders including the public on proposed revisions to data access rules, on the basis of experience gained, new innovation opportunities or new regulations.

2

# Types of data use and reuse, transparency and societal value

## Illustrative (non-binding) lists of data reuse purposes that would normally be supported, and not supported

It is unlikely that a comprehensive list of data use and reuse purposes can be enumerated that would cater for all possible request scenarios and future innovations. However, the illustrative list below of example high-level uses that would normally be supported, subject to more detailed scrutiny by the data access body on a case by case basis, is considered to be a useful resource to support public awareness and to build confidence in the kinds of data uses that are considered likely to yield societal benefit.

### Improving the care to individuals through health data use and reuse

- Health status monitoring
- Continuity of care (including the patient and caregivers)
- Care pathway tracking, clinical workflow management
- Real-time feedback and guidance to patients and clinicians
- Personalised medicine delivery
- Disease interception, prevention and wellness
- Real world outcomes
- Comparing data with a reference population

### Population health uses of health data

- Quantify disease diversity and unmet treatment needs
- Public health surveillance
- Public health strategy
- Health services and resource planning
- Quality and safety monitoring
- Care pathway optimisation
- Pharmacovigilance, safety signal detection and validation
- Post-market surveillance of medical and in vitro devices
- Evidence to underpin value based health care models
- Medical device research and innovation, including algorithm refinement
- Outcomes of pharmaceuticals, vaccines, medical devices, and diagnostics
- Outcomes management and value-based healthcare pilots

### Research uses of health data

- Epidemiology and observational research studies
- Disease understanding, disease burden, unmet need and stratification
- Outcomes research, comparative effectiveness research
- Predictive analytics and identify patient sub-groups that respond better to certain treatment
- Digital innovation: devices, sensors, apps (including understanding patient's experience and PROs)
- AI development conforming to the new AI Regulation
- Quantify deeply stratified populations, for targeted therapies and personalised medicine
- Biomarker discovery and validation
- Diagnostics development
- Accelerate the conduct of clinical trials
- New treatment indication areas
- Adaptive trials and licensing
- Patient characterization and optimal treatment sequencing
- Testing and improving outcome sets
- Assessing the feasibility of planned research and implementation

The following list of **example purposes that would not normally be supported** is proposed here, also for potential publication for public awareness and assurance, although individual cases might arise where a request under one of these categories is considered to have sufficient societal value and societal safeguards to be appropriate.

## Examples of purposes for which health data should not be used

**Research uses of data that would require but have failed to achieve ethical approval**

**AI development that would not be permissible in the EU**

**Weapons development and research, including development of biological weapons (but OK for research into treatments following biological attack)**

**Drugs for use in capital punishment, interrogation or torture**

**Eugenics**

**Political projects where there is party political gain motivating the research**

**Discrimination and profiling of persons**

- using data to develop profiles intended for marketing, service access or financial purposes
  - e.g. the exclusion of guarantees from insurance contracts and the modification of insurance contributions or premiums of an individual or group of individuals presenting the same risk
- (but OK to carry out population profiling to target appropriate therapies and to assess health risks)

**Marketing or endorsement of an existing product**

- the promotion of products towards health professionals or health establishments, or towards patients or the public
- (but OK to conduct usability testing of devices, uncover unmet treatment needs)

**Research where the sole outcome is a financial interest**

**Research which would be deemed illegal in the EU**

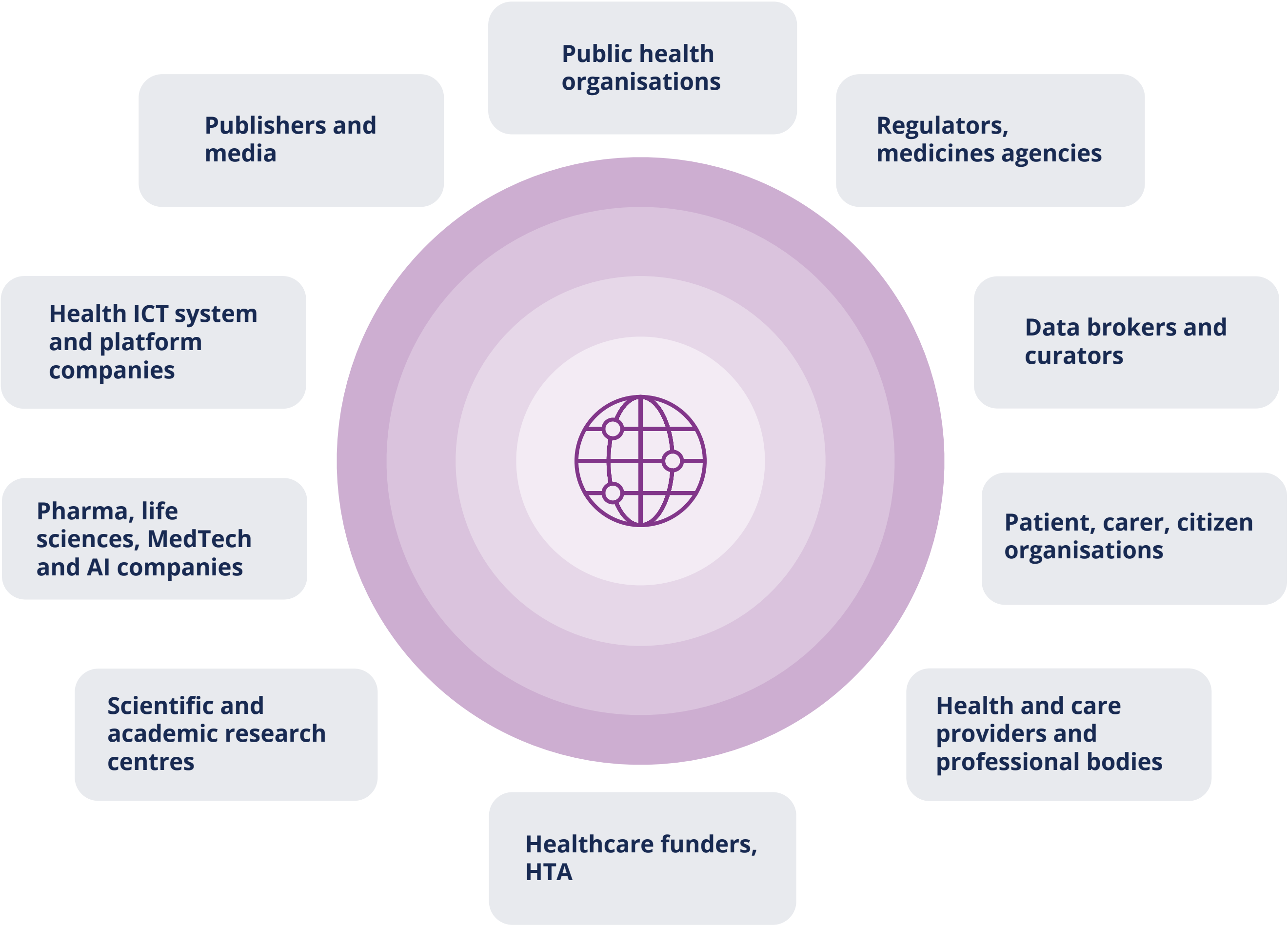
**Business models that build on selling or reselling the accessed data**

## Criteria for, and categories of, organisation that would usually gain data access at different levels of detail

It is recommended that, rather than pre-determining the categories of organisation that will normally be approved to gain access to health data, DPAs collaborate to define criteria that will normally be used to determine the suitability of a requesting organisation, over and above the purpose for which data access is requested. Such criteria might include whether the organisation undertakes knowledge discovery as part of its scope, its commitment to adhere to the terms and conditions for data use that are set, its willingness to co-operate with inspections and audits, and takes into account any pre-existing track record of acceptable or unacceptable data use or governance.

The Working Group was not in a position to elaborate on these ideas in the time available.

However, they felt it may also be helpful to list examples of organisations that are usually expected to meet such criteria. This list of high-level categories of organisation is proposed here as a resource for public awareness and assurance but can also only be illustrative. It should not be assumed that any organisation fitting to one of these classification headings will automatically have its request approved, nor that an organisation that does not naturally fit onto one of these categories would automatically be refused data access. It should be noted that this list does not include access by individuals to their own health data, the right to which is stipulated by the GDPR and is not normally part of the scope of data access decision making bodies.



**Public health organisations**

**Regulators, medicines agencies**

**Data brokers and curators**

**Patient, carer, citizen organisations**

**Health and care providers and professional bodies**

**Healthcare funders, HTA**

**Scientific and academic research centres**

**Pharma, life sciences, MedTech and AI companies**

**Health ICT system and platform companies**

**Publishers and media**

## Example scenarios illustrating a quid pro quo for data access, showing the value for patients and society

The following are examples of possible ways in which organisations conducting research might offer a quid pro quo towards the organisations providing data or data access, to health data infrastructure operating costs or more broadly to society. These are intended to stimulate discussion and the expansion of examples through wider stakeholder consultation. It is not assumed that any or all of these would be put into practice without much more detailed analysis of the value propositions and how the corresponding value of the quid pro quo would be quantified and approved.

It should be noted that none of these examples involve directly paying for the data. This is considered by the working group to be too controversial and complex to utilise as a kind of quid pro. Anxieties have been expressed in the past in consumer surveys about the concept of health systems "selling data".

**Contributing health (or other data relevant to health) for others to use, by acting as a data provider for data assets they hold and are willing to share with others**

**Contributing financially to the direct costs incurred by personnel preparing and providing a dataset to which they have been granted access**

**Contributing financially to the cost of data curation or a data access infrastructure, from which they might benefit, but without any privileged priority or permission**

**Making an in-kind contribution through the provision of data, staff expertise, computing resources and other items such as software in a pre-competitive way that enables wider well-protected access to good quality health data, to multiple users and for multiple purposes of which they would benefit without preference**

**The contribution of data cleaning, cross-mapping, natural language processing or bio-sample analysis results, given back to the data provider in order to enrich the data sets for subsequent use by any other approved organisation**

## Information that should be published to support transparency

As an elaboration of some of the principles that relate to demonstrating transparency, it is suggested that decision-making bodies, especially DAPs, should openly publish the following information about decisions that they have made and what has happened regarding health data uses that they have permitted. They may wish to consider publishing the following transparency information.

Given the potential for a very large number of data access requests to be handled by a decision-making body, potentially operating at a national level, and a very large number of data sources that may be involved in servicing any single request, a scalable solution needs to be found for collating this information, preferably in as automated a way as possible. This may itself require research and piloting.

- **Category of organisation (actual organisation name?) making the data access request**
- **Purpose (or category of purpose) for making use of the data (for example utilising the list presented in Section 2, but taking commercial sensitivity into account)**
- **Intended format of the end result (knowledge, product, service…)**
- **The societal benefit of that end result**
- **Intended method for societal access to the benefit (open publication, licensed knowledge, licensed software, licensed medicinal product…)**
- **If any data, data enrichment or other quid pro quo is being offered**
- **Country or countries in which processing will take place**
- **Whether anonymised or pseudonymised or identifiable data is needed**
- **Data access decision**
- **Approximate date when results are anticipated, and later links to the publication or other accessible outputs (e.g. reports)**
- **Any follow-up information (changes, concerns, investigations, termination…)**

# 3

# Specific issues on which it is recommended to invest in public awareness and engagement

The establishment of new data access decision-making bodies such as national DAPs, and their adoption of new principles and rules that inevitably will widen health data access and its reuse, should be accompanied by raising public awareness and engaging in public dialogue about the following issues and areas of assurance, in addition to work that clarifies the scope and content of the principles outlined above.

It is also important, for transparency, that information is published on what makes data access decision making bodies themselves trustworthy, who is represented on them and how their decisions are made. It is important for bodies to demonstrate that patients are at the heart of this discussion (whether it is on data being used for enhancing patient care or for research). It is important that public engagement also addresses the public perceptions and misperceptions about health data "ownership".

**The need for data on large numbers of people, often with and without a condition so that some of them can act as control patients, in order to enable high-quality research.**

**Education about information (cyber) security safeguards and how to support organisations to comply with data protection legislation, obligations and state of art practices.**

**The practical challenges with providing individuals, European scale (current population ~470 million), with personalised feedback on how their health data have been used across the multiple uses across Europe..**

# 4 Implications for the EHDS

The work to design the EHDS, including stakeholder consultations and the development of legal, policy and governance instruments, will stimulate consensus on principles and good practices that could be adopted or adapted by many Member State data reuse initiatives, and cross-border initiatives in specific disease areas or amongst particular communities. They should therefore be developed with that wider applicability in mind.

Some countries, notably Finland and Portugal, have already developed national rule books, and are gaining experience in their use. The EC should consult these rule books and with their authors, in order to help develop its own set of rules for enabling data access appropriately via the EHDS.

Priority should be given to establishing minimum essential principles, practices and permission criteria that can quickly be agreed and widely endorsed, although more detailed instruments will take longer to produce.

In addition to data access rules, there needs to be greater uniformity and conformity by Member States in implementing an interoperable solution to data collaboration in the EU, which the EHDS can accelerate.

Research and pilots should be encouraged that give citizens greater transparency and input on how their own data has been used by different organisations and for different purposes. This may be possible even if the data had been made anonymous by indicating the research uses of datasets in which the individual is likely to have been included. The European momentum behind the EHDS is an excellent opportunity to investigate different ways of providing this transparency information back to the public, and to find an achievable balance between technical feasibility and meaningful transparency.

CALL TO ACTION 4

DEMONSTRATE BENEFITS TO SOCIETY FROM DATA ACCESS, USE AND REUSE

WORKING GROUP 2

# SOCIETAL COMPACT AND RETURNING VALUE FROM DATA USE

# Context

An increasing number of bodies are being established to make data access decisions on behalf of one or more data sources, in response to diverse public/private body requests. Codes of Conduct are being advocated as a possible solution to securing health data access at scale. However, the ones relating to GDPR are designed to facilitate compliance with privacy laws, not to facilitate access to and use of health data for the benefit of society in general, thus not responding to the aim of this WG.

The preparation and the processes to pass laws takes considerable time. Formal Codes of Conduct based on legislation, such as the GDPR, take too long and are not flexible enough. In contrast, the speed of change in technologies is very fast, outpacing the ability of legal systems to regulate. So "soft law", like a Compact, has the ability to adapt quicker to this pace of change and therefore provide greater protection against the latest technology innovations.

This Working Group explored:

- **How best to promote the development and adoption of a European multi-stakeholder Compact regarding responsible data use, transparency, accountability and communication?**
- **What inclusive mechanisms might be adopted to hold open public consultation when developing the terms of such a Compact?**
- **How could a well-designed Compact be promoted to organisations that need to endorse it, to the public who need to be assured by it and be enforced (possibly with sanctions) to win public confidence and trust?**
- **A Compact can also include the notion of reciprocity. What might be candidate transactional models for in-kind or in cash return for data access, and to whom should the return be distributed or given to?**

[1] *https://echalliance.com/calls-to-action-on-health-data-ecosystems-recommendations-from-multi-stakeholder-round-tables/*

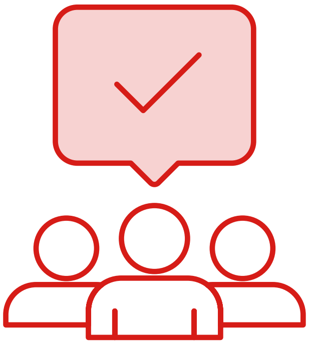
# 1 What is a Social Compact?

A Compact or social contract is a voluntary agreement between a range of multi stakeholders to cooperate together to achieve social benefits[2]. The essential ingredient in a Compact is the concept that an individual or organisation "gives" for the common good of society. There might be different models for this value exchange but they need to be fair respecting the need for potentially proportional society benefits. The value might be economic but could include wider social, academic and research benefits or any combination. A Social Compact whose purpose is delivering societal benefits was supported by the WG and this is consistent with data access altruism. A Compact could promote a "Data Culture for Society" extending the concept behind "Data Saves Lives"[3].

A Compact could essentially be an agreement between the stakeholders for access to health data on terms contained in the Compact to be used for analysis, research and innovation to improve health and care services, outcomes and policy development, as well as creating new services, drugs and devices. These stakeholders should extend beyond simply one industry or industries in general and include public, private and voluntary sectors.

Also, several Compacts could be developed based on specific health sectors or conditions and/or geographic areas (regions or countries) or for specific purposes (health research). Sections 3-5 and 7 create a checklist for the design of Health Compacts. In this way multiple Compacts can be created using the Checklist to assist coherence and mitigate conflicts or overlaps between Compacts. Mapping Codes of Conduct and Compacts would assist with avoiding duplication and overlaps. An illustrative diagram is included in the Annex in Section 8 and more work would be required to complete the mapping.

Notwithstanding the possibility of creating multiple Compacts (for different health sectors, for example) the Working Group was drawn to the concept of a single cross border international compact to champion health data as a societal benefit and the principle of data dignity (see Guiding Principles below). The challenge with a single Compact is the need to respect the wishes of individuals who may have different preferences for different uses cases or for organisations to access their data. We believe the Compact is able to address these issues by providing a broad framework with schedules or rules for specific use cases and classes of data.



[2] https://iep.utm.edu/soc-cont/

[3] https://datasaveslives.eu/

2

# Content of a Compact?

The exact scope would be developed by the stakeholders involved but should include:

- **Specific social benefit and purpose (e.g. improve research into breast cancer)**
- **What use of health data**
- **Access terms to the health data**
- **Adherence and monitoring arrangements**
- **Governance arrangements and structure**
- **Annual reporting of the activities of the Compact, societal benefits achieved and compliance with the Guiding Principles.**

# 3 Guiding Principles for any Compact

- Open, transparent, responsible, inclusive and accountable use of Health data

- Aims must include using health data to improve the health, care and wellbeing of citizens and contribute to improving health and care inequalities.

- Fair and equitable value exchange between signatories respecting the requirement for society and common benefits from individual and organisation giving access/data altruism

- If an organisation receives commercial value through having data access and using the derived knowledge as part of its development of provision of an innovation, this benefit should be reflected back in some way, with the possibility that it is reflected back through the pricing of that innovation.

- Compliance with all national and European laws e.g. GDPR and ethics to ensure data privacy, good data management and governance

- Data Dignity. This involves three key tenets:

  » While the majority view was that data itself should not be monetised (with some exceptions) meaning access to health data is not charged at a profit but on a cost recovery basis (innovation and solutions developed from it can be charged at a profit), this may depend on the type of health data. In fact, it was noted that a) industry is already sometimes paying a profit element to access health data and b) Working Group 1 came to a different view ("It should be noted none of the above examples involve paying directly for the data. This is considered by the Working Group to be too controversial and complex to utilise as a kind of quid pro quo. Anxieties have been expressed in the past

**consumer surveys about the concept of health systems “selling data)” There might be situations in which paying for data is reasonable and fair, and in other situations proves not to be acceptable or workable. This illustrates this subject is extremely complex as not all health data is the same so more in depth investigation is required before concluded positions could be advocated.**

- » **Clarity of purpose and transparency about how health data will be used and**
- » **Human Centric and respect for the health data subject so they agree how their data is used. The use of health data must be centred around the wishes of the people who provided the health data.**

- **Promoting a “Data culture for Society” building upon the Data Saves Lives initiative.**
- **Using data to increase evidence-based decision making in healthcare and to increase the quality, transparency (traceability, explainability and interpretability) of machine learning and AI.**
- **Compliance and use of FAIR guiding principles for scientific data management**
- **Promote interoperability and mutual reciprocity**
- **Regular transparent communication by and to signatories on the use of health data, the social benefits realised, and lessons learned.**

The  Compact Principles  are consistent with the approach taken by the Principles for a human-centric, thriving and balanced data economy (Access, Share, Act, Trust, Innovate and Learn) published by the Finnish Presidency of the Council of the European Union 2019[5].

Both data quality and avoiding data bias are important for the effective use of health data. In particular, ensuring that data is representative of populations or population samples is essential to maintaining citizen trust.

Monitoring the compliance with the Principles will be very important particularly operationalising Data Dignity. The involvement of industry is central to delivering societal benefit and who will monitor and be responsible for data governance needs to be clear and effective.

A number of Codes of Conduct are being development currently and many of the Guiding Principles could be adopted by these Codes.

[4] https://www.go-fair.org/ or https://www.fair4health.eu/

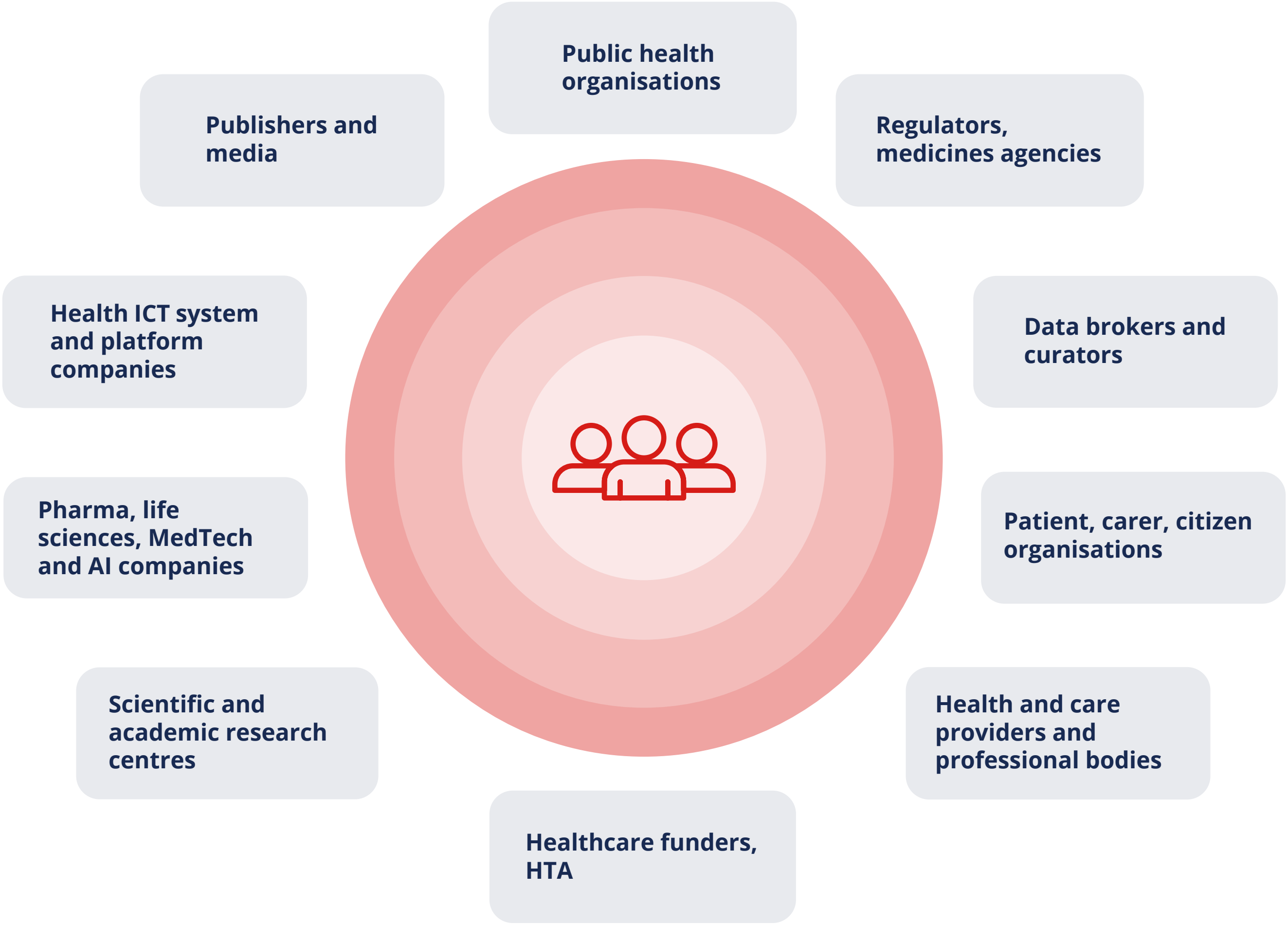
[5] https://api.hankeikkuna.fi/asiakirjat/2d0f4123-e651-4874-960d-5cc3fac319b6/1f6b3855-fc1d-4ea6-8636-0b8d4a1d6519/RAPORTTI_20191123084411.pdf

4

# Possible types of stakeholders who could be signatories to a Social Compact?

The principle is that any organisation or individual who wishes to become a party to a Compact is eligible to do so. The wider the organisations involved, the greater the scope of the Compact and ability to facilitate access to health data at scale. Accordingly, a Compact should not be limited to EU Member States or Europe and stakeholder groups with a remit beyond Europe would be desirable. The list below is not intended to be exhaustive.

Scalability is important. Organisations can take considerable time to sign up to new initiatives whereas individuals may move much faster and champion Compacts. The Working Group considers that adopting a twin channel approach of both organisations and individuals being able to sign has advantages, especially as, in the future, consumer generated data has the potential to be the most important source of health data.



**Public health organisations**

**Regulators, medicines agencies**

**Data brokers and curators**

**Patient, carer, citizen organisations**

**Health and care providers and professional bodies**

**Healthcare funders, HTA**

**Scientific and academic research centres**

**Pharma, life sciences, MedTech and AI companies**

**Health ICT system and platform companies**

**Publishers and media**

# 5

# Public Consultation to develop scope, guiding principles, governance and decision-making rules.

The engagement of citizens who are truly representative of Members States is very important. To date a number of surveys have been undertaken, e.g. EURORDIS Rare Patients Barometer in 2018[6] or DigitalHealth Europe project survey to citizens in 2020[7], but these to date are not large enough or inclusive enough of society. This will be challenging given the cultural differences and different levels of trust in Member States but this is precisely why this information is essential to build meaningful and effective Compacts for health data use, which could in turn support the establishment of a European Health Data Space. We need a deeper understanding of public expectations for the fair use of health data.

The survey must not leave anyone behind; so should deploy a variety of established tools such as written and online surveys, citizen juries, town hall meetings and social media campaigns. Any survey needs to be designed by experts in public consultation and communication and the results should be used to refine the concept of a Health Compact and the checklist we have proposed.

[6] https://www.eurordis.org/publication/rare-disease-patients-participation-research

[7] https://digitalhealtheurope.eu/results-and-publications/consultation-paper-citizen-controlled-health-data-sharing-governance/

# 6

# Returning value from Data Use

A. current challenge is the commercial market for health data. Some industry organisations argue that raw data has no value, while health organisations defend that it has a substantial value and without it industry has nothing to work on. These are the two extreme views.

Industry has deployed a range of incentives to both develop and pilot innovations and the examples below lists various types of in-kind support. They are only a few examples of many possible ways in which commercial organisations conducting research, or academically funded research bodies with provisions in a grant to contribute to data access, might offer a quid pro quo towards the organisations and individuals providing data or data access. These are intended to stimulate discussion and the expansion of examples through wider stakeholder consultation. It is not assumed that any or all of these would be put into practice without much more detailed analysis of the value propositions and how the corresponding value of the quid pro quo would be quantified and approved.

It was recognised that value exchange has to be fair to both sides so for industry the data access needs to be timely and the data has to be quality data. Any reward model must also be fair respecting the need for proportional society benefits and data dignity. Further work is needed to define societal benefit and fair value exchange taking into account the opinions, preferences and values of all stakeholders including citizens, healthcare providers, research bodies and industry. Moreover, value and societal benefit are abstract concepts that vary between individuals, organisations, sectors and societies. It is therefore acknowledged that attributing value to data sources, particularly where multiple data sources are used, is not straightforward. Further work on defining societal benefit and parameters for fair value exchange work would assist the possible development of a range of value sharing models for data access.

Options for returning value from data access and use could include:

**Payments to health provider organisations or health systems. A fee to access data sets covering the cost to provide that information (e.g. collecting, storing, extracting and anonymising). Cost recovery calculations should be transparent, not including any element of profit by the data source/provider. Exactly what these costs might be, and how they are calculated, needs further work[8].**

[8] *Charging for recovery costs on a time incurred basis is not without challenges e.g. the person who first requests pays considerably more than subsequent people requesting the same data.*

**Cost recovery models for data access might price out smaller companies, academic and research organisations. Proportional subscription models combined with recovery costs (as used in Finland where there are four components for charging[9]) and reduced rates for smaller companies, academic and research organisations (or grants to them) should be investigated further.**

**Contributing financially to the cost of data curation or a data access infrastructure, which they would be a possible beneficiary of data access, but without any privileged priority or permission.**

**Contributing financially to the direct costs incurred by personnel preparing and providing a dataset to which they have been granted access.**

**Making an in-kind contribution through the provision of their own data, staff expertise, computing resources are rather items such as software in a pre-competitive way that enables wider well protected access to good quality health data, to multiple users and for multiple purposes of which they would benefit without preference.**

**Contributing to data cleaning, cross-mapping, natural language processing or returning biosample analysis results back to the data provider in order to enrich the data sets for subsequent use by any other approved organisation.**

**Acting as a data provider for data assets they hold and are willing to share with others.**

[9] https://findata.fi/en/pricing/

Payments to individuals, especially in relation to consumer generated data, could be justified. However, in relation to Compacts, individual payments run counter to the concept of social or societal benefits.

It is sometimes proposed that organisations, whether public or private, which utilise data should pay the data provider (such as a healthcare organisation or health system or registry) or the data subject (a model sometimes utilised by app developers) for their data. Such models are both complex and somewhat contentious, mainly because the utilisation of datasets is usually part of a long and multi-faceted research and innovation pipeline within which it is extremely difficult to quantify the impact of any one element. It is therefore very difficult to ascertain what business value any particular data set has over other data sets that might have been accessed instead, or not accessing any equivalent data but using other strategies or ways to simulate the relevant knowledge.

It is also difficult to determine how any potential business value should then be translated into some financial return via the pricing or availability of the subsequently-created innovation. A further challenge for data curated by an organisation on behalf of its data subjects, such as a healthcare organisation on behalf of its patients, would be to apportion any “return” between the provider and the patients. These are complicated quantification issues and much more work would be needed to determine specific scenarios in which models of this kind might be considered or piloted, if indeed they are viable at all, other than at the SME direct-to-customer level as at present.

7

# How should a well-designed Compact be promoted to win public confidence and trust?

- The recommended public consultation would provide invaluable information and evidence to promote a well-designed Compact. Key requirements will be to promote trust, confidence, transparency and accountability.

- The promotion should be multi channelled and include all the stakeholders identified in Section 4. Many of these stakeholders have substantial communities they would be able to promote a Compact to.

- Engaging and receiving support from patient, disease and care groups and wider civil society groups would be important to gaining momentum, speed and wide citizen support which in turn would encourage industry backing. If it was possible to gain the same support from regulators, health and  care providers and funders, health and care professional bodies and trade associations that would be desirable.

- The multi channelled (e.g. written, social media, town hall meetings etc) approach needs to be professionally designed by communication experts but should provide information and the benefits clearly and simply which all citizens are easily able to understand avoiding the health and data sector jargon.

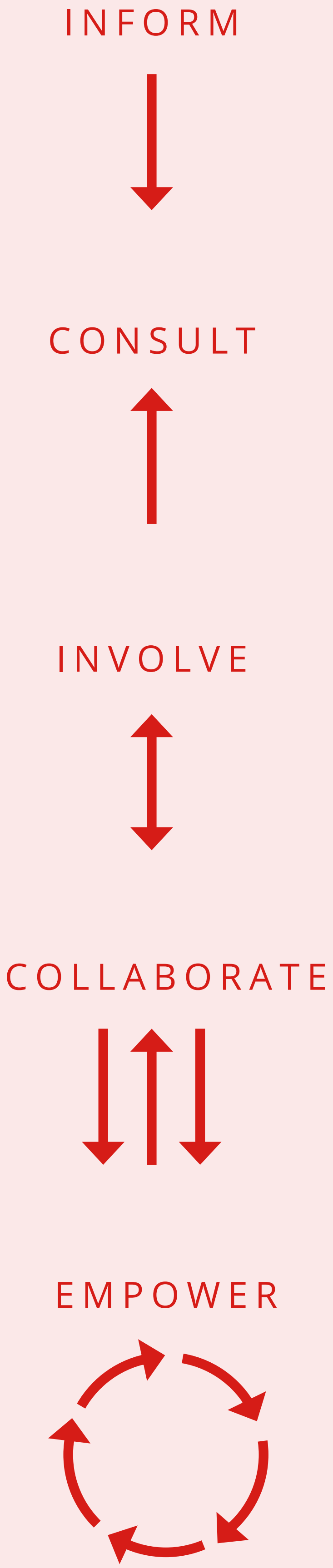
- The communication must be inclusive leaving no citizens behind (avoiding digital exclusion)

- Sponsorship from industry, data initiatives, charities or other not for profit organisations for the development of a Compact itself and its promotion would facilitate the development of well-designed and trusted Compacts. This could allow advertising campaigns to promote a Compact and citizen sign up.

The scale of the communication required to design, promote and set up a Compact is not underestimated but the scale of the task is itself dwarfed by the potential societal benefits from creating Data Dignity and a Data Culture for Society.

A number of organisations have confirmed they would help promote the concept of a Compact including SITRA and TEHDAS.

The diagram opposite is taken from Ada Lovelace Institute. A spectrum of public participation (Foundations of Fairness Where next for health data partnerships).



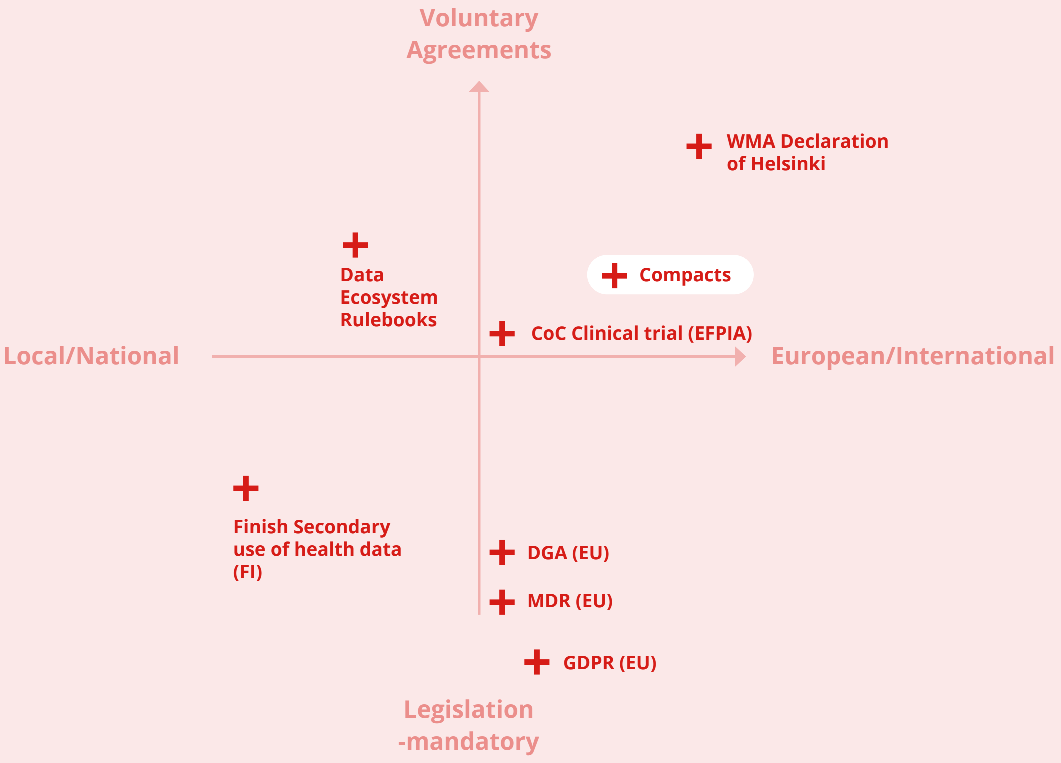
# 8 Implications for the EHDS

The importance of Citizen trust has been acknowledged by both Member States and the European Commission if digital health services are to realise their potential and the European Health Data Space to succeed. The concept of EHDS extends beyond just citizens and the data ecosystem must be inclusive of all stakeholders (as we illustrated in Section 4). The diagram in Section 8 illustrates there is a long way to travel to empower Europe citizens and realise the potential of health data.

A Compact, which aligns with the EU solidarity principle, using extensive consultation to develop the outline we have proposed (design, scope, principles, returning value and promotion) provides an opportunity to create a European health data ecosystem for the health and wellbeing benefit of its citizens, drive the Digital Single market and facilitate innovation and economic prosperity.

ANNEX HEALTH DATA:

## An illustrative mapping of hard and soft laws.



KEY

**DGA**
Data Governance Act

**MDR**
Medical Device Regulation

**GDPR**

**CoC**
Code of Compact

**AIA**
Artificial Intelligence Act

CALL TO ACTION 5

## ADOPT A RISK STRATIFICATION APPROACH

WORKING GROUP 3

# RISK AND REWARD: DATA PROTECTION FOR NAVIGATING EVOLVING RISK REQUIREMENTS TO REALISE THE BENEFITS OF HEALTH DATA INNOVATION

# Context

Working Group 3 of the Roundtable Discussions focussed on the management of risk for health data driven innovation activities. **The need for striking the balance between managing the risks of these initiatives without stifling innovation and opportunity has never been more pressing.** After just over three years of implementing the General Data Protection Regulation (GDPR), the health data reuse community finds itself reflecting on the experience and how it manages risk to citizens' data.

This reflection has been prompted by the need to consider the advent of new European regulations in the form of the Data Governance Act and the first draft of the Artificial Intelligence Regulation, both of which will need to be interpreted and adhered to alongside GDPR. Working Group 3 conducted two round table discussions to explore key areas of risk management, considering traditional approaches and the learning to date of GDPR's implications. This gave rise to the identification of key themes that establish the positions within this paper.

In exploring risk management and implications for future proofing the encouragement of innovation and reaping rewards from research and data reuse for public good we reflected on the following questions:

**Are we getting risk management right across Europe?**

**Have we interpreted GDPR in the most future proof, consistent and nimble way?**

**How do we meet the new challenges and honour holistic approaches in managing risks?**

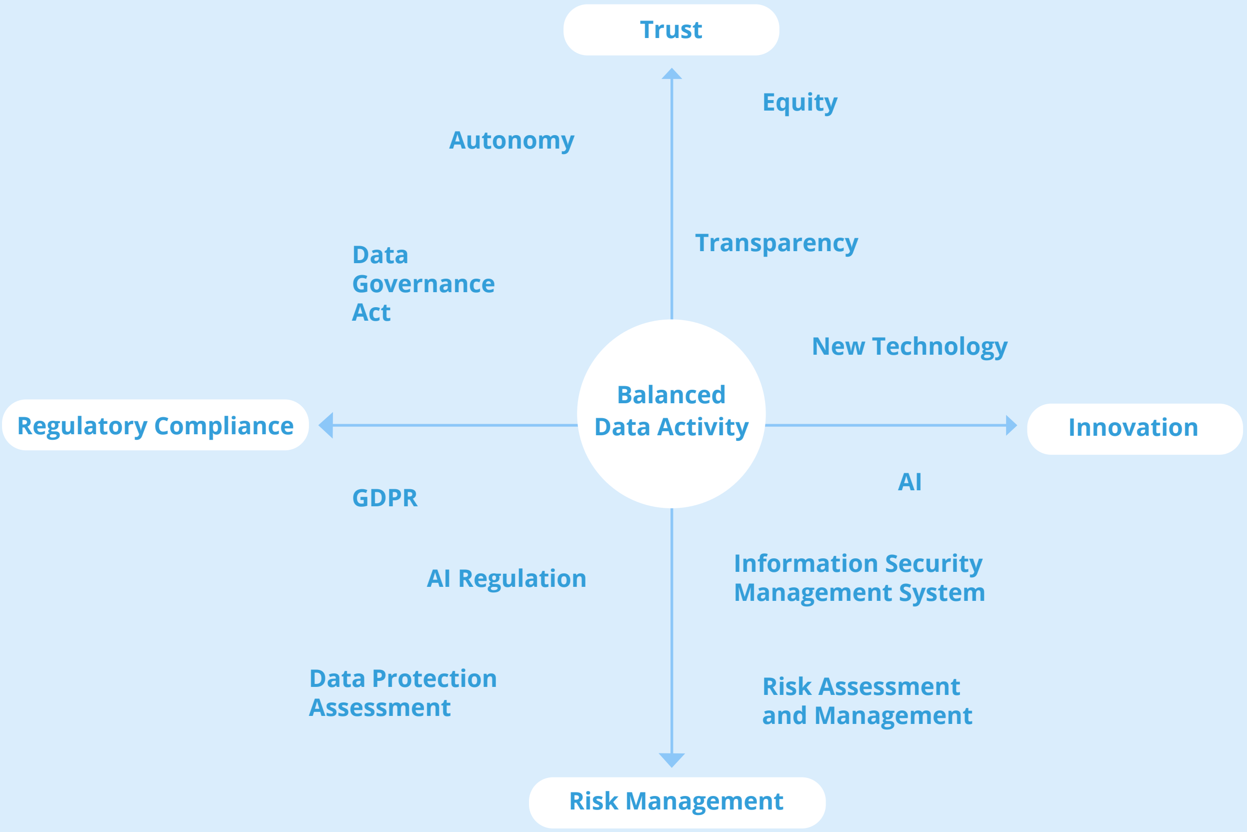
**What do we need to do to enjoy benefits and maintain trust without stifling innovation?**

The exploration of these questions gave rise to the following key themes that we explore in this paper:

1. **How well are we managing risk after three years of GDPR and how can the Data Governance Act and AI Regs help?**
2. **Clarity on data handling, its purposes and protections – what does the use entail, what are the benefits and trade-offs and why are they important?**
3. **Data Lifecycle Assurance, trade-offs and value tensions: what enables data to flow within reasonable expectation?**
4. **Robust Intermediaries and governance facilitating trust – are they the mechanism to assure risk management?**

The European Data Protection Board in its ruling on the Data Governance Act is prioritising a one-to-one relationship between data subjects and their personal data, but the emerging and inevitable trusted intermediary model conflicts with this approach. Additionally, regarding AI the sheer velocity and volume of data flows stretches GDPR. Working Group 3 concluded that a holistic, transparent and measured risk management approach will allow a trusted data ecosystem to emerge.

DIAGRAM



# 1 How well are we managing risk after three years of GDPR and how can the Data Governance Act and AI Regs help?

The regulatory space will continue to evolve, more so in the coming three to five years. **An honest and critical reflection of how the health data innovation community manages risk is pressing** to ensure that innovation is not stifled by uncertain and inconsistent interpretations of law and that the new regulatory frameworks can be best leveraged to help manage risk holistically and drive innovation. **Risk management has a more technical than regulatory basis but viewpoints are pointing towards linking both regulatory requirement with technical implementation of risk assessment and management.**

Reflecting on the GDPR experience has cast light on how risk owners in research and innovation manage risks to data assets and data subjects, as well as the tools and the procedures in place to do so. In parallel **GDPR has also led to much wider discussion and consideration from data subjects themselves,** both because of data breaches and scandals, as well as **a growing interest and in some cases concerns around how their personal data is used and the benefits that may be possible.**

What is clear however is that the relatively short period of GDPR implementation has given rise to a series of varying interpretations of law which in turn have added complexity for risk managing health data reuse. **With the arrival of new laws key questions arise around how risk management can balance the mitigation against harms with the benefits that research and innovation through the use and reuse of health data can bring.** In exploring this area we refer to the Assessment of EU Member States' rules on health data in the light of GDPR[1] which can help the innovation community to reflect on what we have learned after three years of GDPR interpretation.

Across Europe interpretation of GDPR can vary on a number of key areas. **The anonymity of data is a one example of where there are differences in interpretation around whether a data set is too detailed to be reliably considered anonymous,** or whether a set should be considered anonymous where there may be a linking table between the data set and the identity of the data subjects where it might be considered Pseudonymised and therefore fully under the protections of GDPR. **Where anonymity cannot be justified this causes a risk management oversight in terms of process and procedure for handling data and has significant implications for not only conducting innovation with**

[1] https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf

**data but also the trust that innovators and citizens will have in the work.**

Another **significant area of variation is the selection of Legal Basis for data processing and Special Category data processing justifications.** In the area of health research for public benefit, some jurisdictions advise using Public Task for conducting Scientific Research for Public Authorities like hospitals and academic institutes, whilst advising Legitimate Interest and Scientific Research for industrial and Third Sector institutions. Other jurisdictions advise and sometimes require relying on GDPR Consent.

Furthermore the **Data Protection by Design and Default paradigm introduced by GDPR provides a common basis to honour Privacy by Design and adopt tooling to achieve this in the form of the Data Protection Impact Assessment.** Within this paradigm alone **there is variation both within and across jurisdictions as to when Privacy by Design should be applied and under what circumstances to run an Impact Assessment.** Where Risk management is concerned these are key tools for developing a risk assessment and mitigation approach and injecting it into the design and development of research and innovation products, particularly for security, accountability and accuracy of data handling. **In looking to establish a common approach for accessing and using data across Europe, a clearer position on when and how to risk assess is essential to providing trustworthy practices.**

Working Group 3 reflected that legal interpretation can vary, where two lawyers may easily give a different interpretation of law. **GDPR at least by design and intention is supposed to make very clear across all parties what the particulars are but there can still be different interpretations.** In thinking about risk management that is meaningful and applicable, this must be seen as a benefit and not a detriment. **How can Europe get the best out of this variation?** It is crucial to remember that it is not necessarily to do with GDPR but how local jurisdictions interpret their own laws, where GDPR is about building a firm harmonisation framework across states.

GDPR is also only starting its fourth year of application. The first time risk assessment for GDPR compliance is conducted for any given activity it is important to work with legal experts to map out compliance risks. This provides learning, experience and precedent where the next time risk management occurs it is much easier with the experience and knowledge and it is not as problematic or complex to manage GDPR requirements.

**It is therefore essential to capture that experience and harness the learning outcomes, especially as new data innovations are becoming possible with Artificial Intelligence and Data Altruism, for instance.** This is also the case for recording and sharing variations in interpretation, which will help the research and innovation community navigate local jurisdiction requirements and provide a much more nuanced and applicable risk management approach across jurisdictions. As an example **the ability to describe pseudonymised data as it is differently understood across different countries will provide Europe a basis for comparison and the means start to navigate optimal risk management strategies.** Additionally a comprehensive list of risk mitigation strategies could form part of this resource. **The articulation of risk, protections, data use purposes and data processing approaches is crucial as a basis for collegiate working, risk management and demonstrating trustworthiness and transparency.**

# 2 Clarity on data handling, its purposes and protections – what does the use entail, what are the benefits and trade-offs and why are they important?

Working Group 3 reflected on the how the regulatory and risk management profiles change and become more complex when reuse of health data is concerned. We considered the distinction between primary use for care purposes and secondary use for research and innovation. With regards the mitigation against harm, **separate processes are needed to ensure that research is safe, equitable and for a public good (i.e. ethical) and where data is shared outside of the context of acquisition, i.e. the health care setting,** the more technical information risk management and compliance requirements start to require additional assurances over and above the primary uses of health and other personal data to provide care and run a health care service.

**The traditional distinction between primary and secondary uses of health data may not however be sustainable and is arguably neither representative of what happens in health care practice or conducive to protecting rights, reaping benefits or improving health expediently.** If we are to fully realise the potential of the European Health Data Space and ensure our efforts to risk manage do not in themselves cause harm, we must look more closely at the experience on the ground. From the hospitals' perspective at least, there have been some lessons learned from GDPR and national legislation around secondary use. **There is a balance between availability and privacy and the needs of the patient to receive the best care possible, where there is an imperative to be able to change practice for their best interests.** This has been especially clear during the COVID pandemic. **A balance must therefore be struck between the care imperative, privacy and confidentiality where clinical and care colleagues need to be able to work nimbly to achieve the best care outcomes possible.**

On the one hand therefore there appears to be a tension between identifying purpose and use of data which, if handled over-cautiously, will apply a much more rigorous and sometimes excessive risk management profile. This profile focuses both in terms of mitigating against individual harm directly and via a breach of security or confidentiality. In certain cases these risks remain in the gift of care services to manage because the purposes are to support innovative care for individuals rather than research to drive innovation more generally.

On the other hand **there are nuanced points around what data use purposes relate to, whom they will benefit and the justifications for access in the first place. This relates to being able to use standard wording to describe those purposes using a common dictionary and set of terms to articulate**

**what the uses are, who they involve, who they benefit, whether they are for individual benefit for their care and / or wider public and why they are important.** This must include clear terms as to the nature of the purpose, i.e. whether it is for direct care or wider research, and clarify the need for identifiable or anonymous data, where it should be clear when linking back to the individuals is necessary via pseudonymisation and why this is important.

Data consumers may need to use anonymous, pseudonymised or identifiable data, where this will determine the risk assessment requirements. In terms of mitigating against risks, different protection measures can be considered and their uses justified. **In the case of identifiability risks, homomorphic encryption and differential privacy, for example, can potentially offer a robust assurance to the extent that even industrial partners would be able to make use of the data sets to produce outputs of value and offset anxieties around wide access beyond the care setting. It is important to consider that new technologies can already offer strong risk management and assurance safeguards, and investment should therefore be encouraged to support further development of these new technologies.**

By being clear from the outset using common, unambiguous terms, risk owners can be more confident in ensuring they are pursuing the best risk management framework without unduly slowing certain purposes. This also gives a firm foundation to articulate to data subjects and the wider citizenry what exactly is happening with their data, how it is being used, what their options are and how they and their data can be protected, as Working Group 1 is exploring.

This is an important focus because **assurance about where the data will be going and how it will be handled is very powerful, especially in demonstrating trustworthiness. This is why trust frameworks and contextuality is important – protocols are moving away from Electronic Healthcare Record specific contexts to wider, trusted contexts that include trusted frameworks, processes, infrastructures and partners.** We have different trust frameworks using different ethical and interoperability frameworks where roles are changing. There will be more and more evolution of this that now includes cross border examples and risk management will need to be able to work from a well articulated understanding of these changes to allow for trusted interventions and outputs.

For example we are seeing how new cases like with COVID-19 and vaccine passports are testing traditional models and in clear need of a paradigm shift. It demonstrates how an individual will share some of their health data across countries and how they are the primary sharer of that information themselves. The trust framework level operates on the national and interoperability between nations. More discussion around the roles within these trusted paradigms and how these work across borders moving forward is needed.

Risk managing the European Heath Data Space model will need to consider tried and tested approaches such as the Danish example. Data are being aggregated across Denmark and whilst there is some fragmentation across access and availability of data there is a data authority that monitors this aggregation of data and its use. **Being able to clearly articulate the risk strategies, purposes and the ramifications will provide assurance to patients and the public that their data is being protected, will ensure data users are confident that they are working within regulated bounds and will help all stakeholders feel assured that the outputs of the work are reliable and equitable.**

3

# Data Lifecycle Assurance, trade offs and value tensions: what enables data to flow within reasonable expectation?

Anticipating a range of access needs in terms of granularity is essential but must be explicit. **Not every research purpose will need subject level access but anticipating the future the scope needs to be that broad.** Some of those needs are there now and others will emerge in the future. How do you manage risk in a regulatory framework where new products have a benefit risk balance that must be struck – is there a similar paradigm here and how do the trusted frameworks considerations which are very promising fit? **The goal of this position paper is to look to advising at a national level as well where there may be limitations on resource to actively risk manage in line with all legal and wider regulatory requirements.**

The draft AI Regulation reminds us of how we have a different kind of discussion between private sector and others and how there are trade-offs like in the aforementioned case of the COVID pandemic, and we are also seeing it elsewhere in healthcare. This stems primarily from the assessment of the context that the AI will be deployed in and competent authority assurance that safety can be assured alongside and beyond the GDPR requirements.

For example Microsoft are trying to operationalise their ethical principles into standards their engineers can work with. They cannot work with "be fair" or "be ethical" where they need to be more operationalised. They believe that focus on why the tool is being developed, who is working on it, who will benefit and who will either not benefit or be at a disadvantage. A case in point is the development of tools enhanced by facial recognition technology to support blind and visually impaired people.

There is a value tension between the privacy of other people who are subjected to facial recognition and the accessibility and utility of the tool. The tool gives the participants using it a new and rich enhancement where they can start to recognise people they know with the features functionality made possible by facial recognition, but **GDPR raises points around the use of facial recognition, privacy and personal data where there may be potential compliance implications, especially for rights and freedoms, given that facial recognition in operation. In short one person benefits and another could be at a disadvantage but how one might apply the value judgments needs an understanding of how GDPR principles may be compromised if risk is not carefully understood.**

The health data innovation community is now at a turning point to consider this more closely.

> The static approach to the data subject and how we manage risk can hinder a more holistic approach that encourages shared learning and pragmatic application.

Hindsight can help the community to think about how Europe might have redrafted GDPR given what is becoming apparent about the possibilities of AI and features such as facial recognition. **Caution is warranted not to differentiate too much how we risk manage for GDPR, the Data Governance Act and AI otherwise we may lose out a more holistic approach to risk management that aligns more with the socio technical issues and approaches.**

**We must reflect: was GDPR not drafted to be holistic?** Has its holism been undermined because of a siloed interpretation, with the development of too rigidly specific an understanding of its interpretation across sectors and disciplines concerns have been addressed independently as opposed to jointly? The focus is on the data subject and there are bases that isolate this including public task and legitimate interest but starting from this perspective it tries to build a system that is unbiased, fair and privacy enhancing.

The European Data Protection Board position on GDPR and ruling on trying to maintain a one-to-one relationship between the data subjects and their data vies with the announcement of the Data Governance Act, where the Board was not entirely certain about the Trusted Intermediary model. Yet it seems this model is inevitable - all citizens rely on these intermediaries to manage their data and services. Another challenge posed by AI is that GDPR principles can apply but the sheer velocity and volume of the use of data stretches those principles. The reality of how data flows throws into uncertainty calls for purist visions of the data protection principles and prompt some reflection. How do we accept that reality, especially with the role of intermediaries, and realise a holistic and measured risk management approach that fosters the trusted ecosystem paradigm?

# 4 Robust Intermediaries and governance facilitating trust – are they the mechanism to assure risk management ?

The roundtable discussions explored the need to leverage the new paradigm of the Trusted Intermediary as defined by the Data Governance Act. **To fully appreciate a holistic and representative risk management approach that serves to protect data subjects, data custodians and service providers, the health data driven innovation community will need to agree and support a new, inclusive risk management and reward realisation paradigm that can likely be captured by the concept of a Trusted Research Ecosystem.**

This new paradigm will likely represent trusted platforms or intermediaries of people, processes, infrastructure and transparency about which parties may benefit from current and novel data uses, and which parties may receive no benefit despite contributing to the benefit of others where they themselves may potentially be disadvantaged. To frame a risk management paradigm we can draw on the 5 Safes[2] as proposed by Ritchie, which promote:

- **safe projects – access needs to be for a valid statistical purpose**
- **safe people – researchers can be trusted to use data appropriately and follow procedures**
- **safe data – the data itself are inherently non-disclosive**
- **safe settings – the technical controls surrounding access prevent the unauthorised removal of data**
- **safe outputs – the statistical results produced do not contain any disclosive results**

These will likely evolve to promote a balance between protecting the individual's relationship with their data as keenly defended by the European Data Protection Board and marrying this with the need to apply inclusive models for trust delegation and more inclusive scopes for consent as championed by those intermediaries. At the very least this should promote both a better understanding of what might be reasonably expected around data (re)use as well as allowing for a more holistic and consistent position with regards data altruism.

[2] https://link.springer.com/article/10.1057/elmr.2008.73

**However it must be noted that whilst the 5 Safes represent a basis on which to develop a risk management infrastructure, they are not that infrastructure per se. They will need to be enhanced by intelligence on the scope and variety of regulatory interpretation and its variation across jurisdiction, a common set of terms for describing data use and protections, and safe and reliable assurances of the functioning of the risk management processes for any given data use.**

Conversely, placing the alignment of regulatory requirement with the technical process focus of risk management raises practical issues. **The reality is that risk includes oversight of not only data and its use, but also of liability, indemnity and risk to multiple parties (the data providers, the data users, data subjects and sponsors of the initiatives). Would a Trusted Intermediary be able to offer the assurances to cover these kinds of risks or would there need to be some form of delegation with regards risk management?** In any event, the goal here is to ensure that trustworthiness around data use can be established to meet the expectations of all stakeholders.

**At the same time a practical approach to ensure that the marriage of regulatory compliance and risk management must foster expediency in the processes for identifying and managing those risks and ensure they do not hinder reasonable data use and innovation.**

# Contributors list

| Name | Organisation |
|---|---|
| Transparency and trustworthy decision making | |
| Dipak Kalra (Co-Lead) | The European Institute for Innovation through Health Data |
| Jaana Sinipuro (Co-Lead) | Sitra |
| Ain Aaviksoo | GuardTime Health |
| George Crooks | Digital Health & Care Innovation Centre, Scotland |
| Gianluca Diana | Microsoft |
| Tala Haddad | French Health Data Hub |
| Nigel Hughes | Janssen |
| Richard Milne | Wellcome Genome Campus and University of Cambridge |
| Liesbet Peeters | Multiple Sclerosis Data Alliance and Hasselt University |
| Enkeleida Nikai | Janssen |
| Tanja Stamm | University of Vienna |
| Zoi Kolitsi | The European Institute for Innovation through Health Data |
| Working Group on Societal Compact and returning value from data Use | |
| Bleddyn Rees (Co-Lead) | Digital Health Society |
| Angela Bradshaw (Co-Lead) | Alzheimer Europe |
| Carina Dantas (Co-Lead) | European Connected Health Alliance |
| Catherine Chronaki | HL7 Europe |
| Adrian Jones | NICE UK/ NHS England |
| Sara Boltman | Butterfly Data |
| Elena Bonfiglioli | Microsoft |
| Markus Kalliola | SITRA & TEHDS |
| Thomas Ganslandt | University of Heidelberg |
| Petra Wilson | Health Connect Partners |
| Steve Broomhall | Johnson & Johnson |
| Andrew Warrington | Microsoft |
| Dr. Michael Short | UK Department for International Trade |
| Clayton Hamilton | World Health Organisation |
| Veronica Zilli | Johnson & Johnson |
| Working Group on Risk and Reward: Data Protection for navigating evolving risk requirements to realise the benefits of health data innovation | |
| Brendan Barnes | European Federation of Pharmaceutical Industries & Associationsw |
| Daniel Corredera | Johnson & Johnson |
| Rachel Dunscombe (Co-Lead) | Tektology & Digital Health Society |
| Hani Eskandar | Microsoft |
| Tomas Gornik | Better Care Health IT expert, co-chair of openEHR |
| Pekka Kahri | Helsinki University Hospital |
| Jesper Kjær | Danish Medicines Agency |
| Licinio Kustra- Mano | DG Sante |
| Cornelia Kutterer | Microsoft |
| Nathan Lea (Co-Lead) | i~HD |
| Nikolas Mastellos | Cerner |
| Michael Strübin | MedTechEurope |

the digital health society
enabled by ECHAlliance

i~HD

# Common basis for health data access across Europe

2021 RECOMMENDATIONS BASED ON CALLS TO ACTION ON HEALTH DATA ECOSYSTEMS

THIS INITIATIVE IS SUPPORTED BY

Johnson & Johnson

Microsoft