Key Considerations

for the European Health Data Space

Introduction: Consent-free data usage will divide society and creates a conflict relative to GDPR

The EHDS Proposal has the objective of enabling **primary and secondary use of electronic health data** in a safe environment across the European Union. There is no doubt about the necessity of the EHDS Regulation as such. However, there is big disagreement on how to accomplish its objectives.

The discussion centers around the legal basis for the secondary use of electronic health data. While the Commission proposal provides for overriding the patient consent, there are strong voices requesting patient participation in the form of an opt-in or opt-out solution. The Commission's proposal foresees orchestrating secondary use of electronic health data through governmental bodies. This poses ethical, technical, legal, and political challenges.

The patients' right to self-determination is a cornerstone of European values. Further, the permanent anonymization of image data might be technically impossible and there is currently no infrastructure that could harness the potential of all data available in terms of collecting, curating, structuring and processing health data that is at hand.

Ultimately, the acceptance of the EHDS by the European citizens will be of utmost importance as the division of society is progressing. Simply overriding patient consent is not a viable solution because this approach violates the citizens' fundamental rights by generally subordinating them to the public interest in health data sharing. Currently, there is no compromise in sight on the debate that ranges from overriding consent, or solutions for opting-in or opting-out.

Broad universal meta-consent: Co-existence of consent-free, opt-in, and opt-out

We propose the implementation of a universal consent as already announced in the DGA, in the form of a broad meta-consent that would be given only once, centrally stored, and universally applicable for all use of patient data until changed or revoked (like an organ donor card). Such consent could define, in a quite granular matrix, who would be granted the right to use what type of data for what clinical use case and through what access means. The complexity can be mitigated by clustering practical use scenarios, rendering the consent patient friendly, informed and specific. The concern of bias through limited participation of patients can be mitigated by complementing the approach through a defined set of consent-free datatypes, and establishing a control group for calibration.

Scope of regulation limited to nationwide systematically captured health data

To address the heterogeneity of the various health systems, digital structures, and public sentiment of all member states, the scope of the data that fall under this regulation should in any case be limited to data categories where the majority of such data is captured consent-free based on a specific national law. For example, in Germany, this would be the rather limited data from an implant or cancer registry, and other areas where data capture is paid for by the health care system. Explicitly excluded should be data acquired as part of a privately funded multicenter trial, registries as well as scientific organizations. The need to share data without scientific recognition or financial compensation would otherwise destroy any incentive to engage in extra efforts for the collection of advanced or very detailed data not captured in the ordinary course of care.

GDPR-"Privacy by design" calls for distributed functions rather than central government bodies

The current proposals suggest central national bodies are the sole option for orchestrating data exchange, based on the idea of scaling models successfully in rather homogenous and centrally organized countries like Finland. Yet, the proposals neglect that not all countries have the same health care systems, IT structures, and most importantly relationship to or understanding of the role of governments in relation to its citizens. As the financial sector exemplifies, banking is accepted as safe even without being part of a state banking system – similarly, the public will gain trust in the private healthcare sector bodies as well. Due to a growing divide between some groups in society and their concerns in this regard, some alternatives should be carefully considered:

- The USA has demonstrated that data sharing and secondary use can work well without a central instance;
- European multinational organizations may be more robust in their political independence, like the EMA (as a model for European trust center for assigning pseudonyms);
- Distributed functions and storage concepts as opposed to putting all into one body (in the current proposal the trust center, data collection, and access approval are all performed by the same governmental institution);
- Political independence of such bodies should be ensured, comparable to central banks or notified bodies; and
- Data processing by companies that create user profiles should be banned.

Allow alternative pathways of secondary data use besides the EHDS

The full potential of data can only be leveraged if industry can also gain access to health data for purposes beyond academic and fundamental research. Governments should not form the sole pathway of connecting data holders with data users as long as standards are met. Options could include a standardized universal consent form (as proposed above), a template for approval of a use case through a private entity access committee, and a data security standard that could be audited and certified. A non-centralized framework should be open to private bodies at each process step to foster innovation and entrepreneurship through competition. From the perspective of resilience and technical sovereignty, Europe needs innovation not only in the use of data, but also

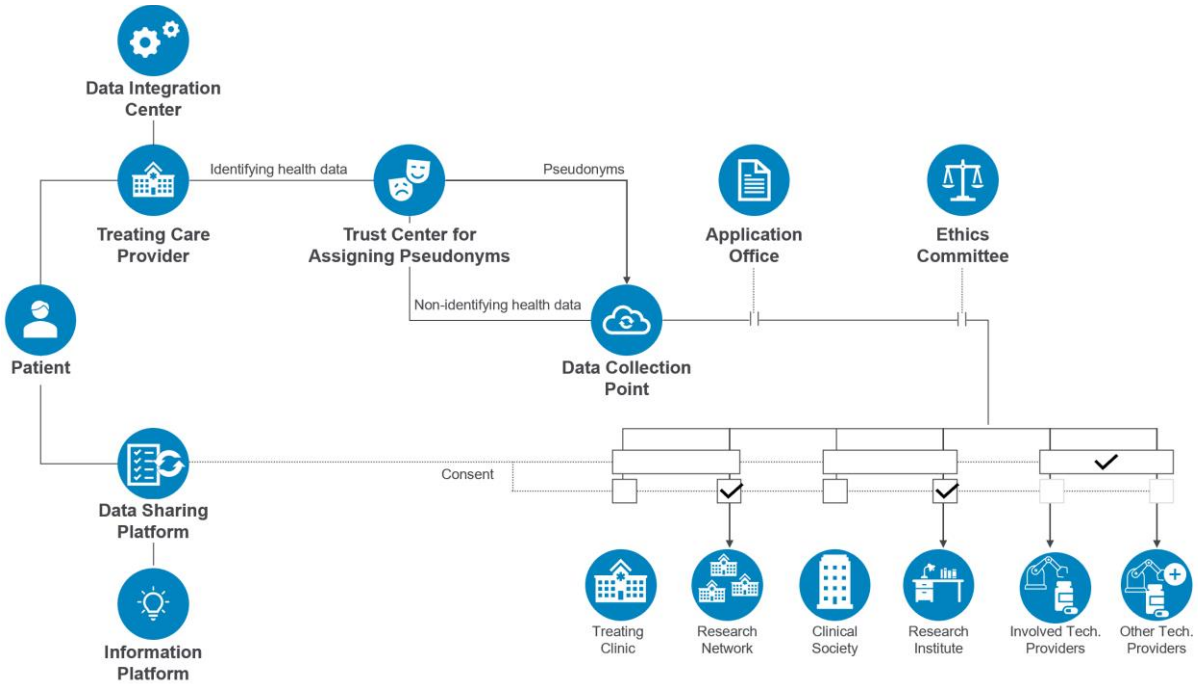
in the infrastructure to collect, store, manage, process, curate, and share such data for primary and secondary use.

Invest in structured data captured through validated processes

Data often exists in silos. Even in Israel, it is often locked inside a specific health system. The USA for example has implemented the information blocking rule of the 21st century Cures Act to allow portability of data, and Israel is implementing a similar regulation. This requires data to follow a certain technical format (i.e., HL7 FHIR), and semantic formats (LOINC, SNOMED-CT). The EU should use the "meaningful use" criteria in the USA as a benchmark, but should go further: In order to increase the value of data, clinical notes, doctors' letters, and diagnostic reports should be replaced through standardized, structured data captured in a clearly defined process, significantly increasing the value of data in primary and secondary use. Structured reports that contain standardized, quantitative information and are geared to the needs of the recipients of the reports, ensure the quality level of the reporting and guarantee traceability as well as the possibility of future support by assistance systems and artificial intelligence.

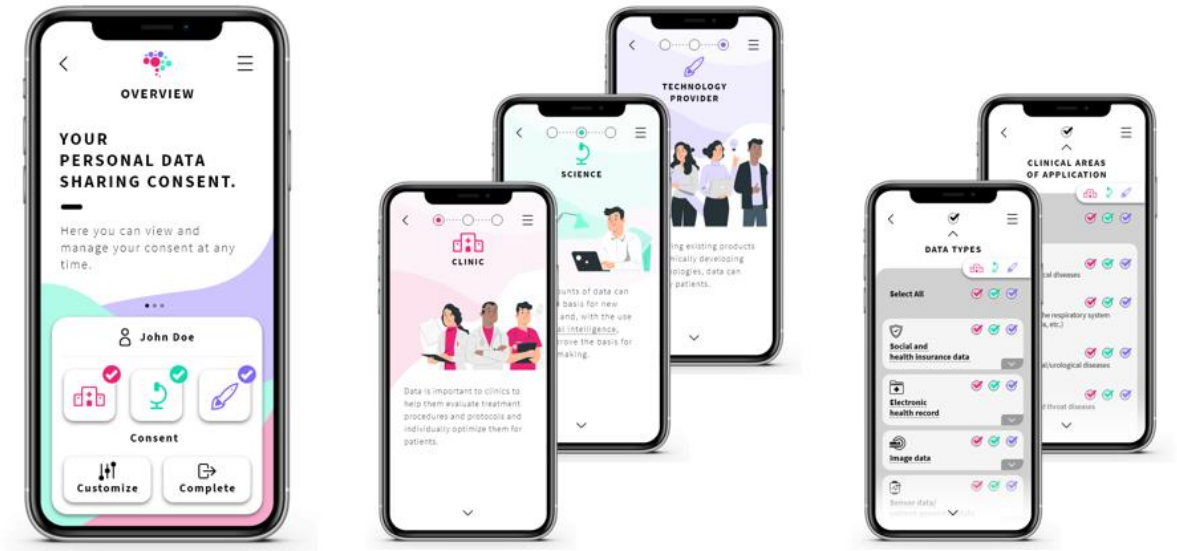
Harmonize regulations to provide a pathway to approval for AI applications

The future of healthcare will be data driven and will rely on the latest generation of AI. However, the current regulations are not harmonized to facilitate products treating patients: While the Data Act and EHDS Regulation proposals aim at producing better data, the AI Act Proposal requires 100% of data to be validated. This hurdle cannot be mastered with data from unknown sources. And finally, there is no defined process for AI-based applications in the Medical Device Regulation (MDR), originating in 2014 (before AI was even a topic). Thus, there should be experimentation clauses, making the EU the place to develop, validate and deploy AI applications as long as there are final checks and alternative validations.



Broad Universal Meta-Consent

Patient consent is a multi-dimensional problem: Different use cases can be mapped in a matrix that defines who can use what data for what purposes, and how. In this way, both consent-free, consent-based opt-in or opt-out processing, as well as processing prohibitions can be represented and change over time.



DIMENSIONS OF DATA CONSENT MATRIX

1. **Users**

Clinic

Data is important to clinics to help them evaluate treatment procedures and protocols and individually optimize them for patients.

☐ Treating Clinic
☐ Research Network

Science

Large amounts of data can create the basis for new therapies and, with the use of artificial intelligence, it can improve the basis for decision-making.

☐ Clinical Specialty Society
☐ Other Research Institutes

Technology Provider

By improving existing products and dynamically developing new technologies, data can help many patients.

☐ Technology provider of involved technology
☐ Other technology providers

2. **Data types,** for example social and health insurance data, image data, sensor data and biomaterials.
3. **Clinical application fields,** for example, diseases of the respiratory system, dermatological diseases or cardiovascular diseases.
4. **Consent to be contacted,** for example on additional findings, results of relevant studies, but also inquiries regarding extended consent.