digital enlightenment forum

Towards a European Ecosystem for Healthcare Data

Brussels, BE

25 October 2017

Workshop Report

Contents

Introduction

As Europe is undergoing foundational changes in healthcare, there is a need to orient developments towards value-based, outcome-based and patient-centred care. The Digital Enlightenment Forum (DigEnlight) conference on Trusted Data Management in Healthcare in June 2016 highlighted how personal health data promises to revolutionise healthcare, bringing personal health data under individuals' control for their own benefit and that of society as a whole.

In the meantime, there has been progress on several fronts. The European Innovation Partnership on Active and Healthy Aging conference in December 2016 stressed the need for user-generated, data-driven economic models, citizen empowerment, and the need for organisation and change management models. In early 2017, the European Commission set up a Task Force that will work across portfolios on developing concrete proposals to harness the potential of data and technology in order to deliver better health and care conditions in Europe. It will examine incentives and obstacles to achieve secure exchange of health data across the EU. Whilst a Commission Expert Panel on effective ways of investing in health underlined that disruptive innovations must also respect values of universality, equity and solidarity while delivering high quality, effective and safe health services[1]. The European Commission is preparing a Communication on eHealth. The Estonian Presidency has taken several initiatives to drive forward the agenda of a 'digital health society', addressed by health ministers in July 2017, in a forthcoming declaration and Presidency Conference. One outcome is the Digital Health Society Tallinn Declaration[2].

Building on its earlier work and broad network in the area, DigEnlight organised this workshop in Brussels to address future needs and requirements in facilitating and coordinating European healthcare data management in a privacy-preserving and trustworthy manner.

The meeting brought together policy makers, technology experts and industry representatives in view of making concrete recommendations on how to meet specific challenges inherent in emerging policy, technology and application issues. They discussed the state of play, the main obstacles and proposed policies and technology solutions to ensure trust in a privacy-respecting data environment for patients, professionals and other actors in a transparent and auditable healthcare environment.

Presentations from the meeting are available from the DigEnlight website.[3]

Welcome

Welcoming everyone to the meeting, **George Metakides, President of DigEnlight**, explained that this was a follow up to the event in Amsterdam in June 2016, which was organised in collaboration with DG Connect and Philips (NL). Healthcare data has been frantically accumulated – we might even say 'hoarded' – by diverse categories of collectors: governments at all levels, health organisations, research organisations, insurance companies, pharma, and internet oligarchs. In short, we are seeing a goldrush. Significantly, ordinary citizens also collect data in a systematic way and are trying to put it to some use.

As in Amsterdam, there are two basic questions to address: firstly, is this health data being used effectively so as to create value? secondly, is this being done with appropriate privacy safeguards? If the answers to these questions were "yes", then there would be no need for a further workshop. In reality, the road is strewn with challenges – technical, organisational, policy, regulatory, etc. – which makes health providers reluctant to use these data streams and solutions. There is an urgent need for upskilling and to create awareness of consequences both positive and negative. Rolling forward the European ecosystem in healthcare data will not be smooth and will not be short: the workshop, hopefully, would start to provide some answers.

[1] https://ec.europa.eu/health/expert_panel/sites/expertpanel/files/012_disruptive_innovation_en.pdf

[2] https://www.eu2017.ee/news/insights/digital-health-society-declaration

[3] https://digitalenlightenment.org/event/workshop-towards-european-ecosystem-health-care-data

Keynote Address

Despina Spanou, Director, Directorate H - Digital Society, Trust & Cybersecurity, DG CONNECT

Ms Spanou welcomed this DigEnlight Workshop, which followed similar events organised by the Commission earlier in the week relating to implementation of the GDPR and the eHealth Stakeholders Group. All were extremely timely in view of the Commission’s work in preparing a Communication on eHealth which is due to be adopted before the end of 2017.

All segments in our society can benefit significantly from digital innovation; health is no exception. For example, supporting healthy lifestyles with mobile health leads to reduction in non-communicable diseases. This not only adds years to life expectancy, but improves health status in those extra years. Accessible, affordable and high-quality health care are important foundations of Europe's social model. But preserving these values in the future will rely on: our capacity to embrace digital innovation; our ability to pool investments and expertise across borders to advance medical science and personalised medicine; and most importantly our greatest asset: empowered citizens.

Digital health and care transformation was addressed as part of the Digital Single Market mid-term review (adopted 10 May 2017). The DSM proposals aim to ensure that the digitisation in health and care will benefit EU citizens, providing them with better treatment, prevention and early diagnosis of diseases, and to deliver more sustainable health and care systems across the Union. The Review identified three priority areas for policy actions:

1) **Enabling citizens´ secure cross-border access to health data**: Citizens in Europe have the right to access their health data and yet, in practice, this is often not the case. Most citizens don't have electronic access to data about their own health, which is often scattered in different places and untraceable. This limits the potential in making us better managers of our health and our medical conditions.
2) **Development of a world-class data infrastructure to advance research and personalised medicine**: There is an enormous potential in using health data to advance medical research and personalised medicine. However, integration of big data faces many problems related to cross-border, technical and semantical interoperability and standards.
3) **Support widespread adoption of digital health tools for citizen empowerment**. It is important to promote a true European market for digital products and services on health and care that empower citizens and overcome the fragmentation that our innovators (start-ups and SMEs) often face when trying to scale up across borders.

In all these aspects digital technologies, together with data exchange and analysis, play a central role. Data has become an essential resource for growth, jobs and societal progress and smart use of it can be a source of decisive competitive advantage. The Commission provides funding for research and innovation and for the establishment of important digital infrastructures that can support these ambitions for decades to come. But funding is not enough. Other enabling conditions are required to stimulate data exchange towards better health outcomes, from prevention to cure.

Health data is highly sensitive and therefore trust and security are essential for scaling up the use of digital innovations in health. Recent surveys indicate that many citizens are willing to share their health data, especially with their doctors or for research purposes, but that is on the condition that confidentiality is guaranteed. European legislation on data protection has been revised to reinforce those guarantees, especially when it comes to health data. It is up to those responsible for the enforcement of that legislation to ensure that privacy is protected effectively.

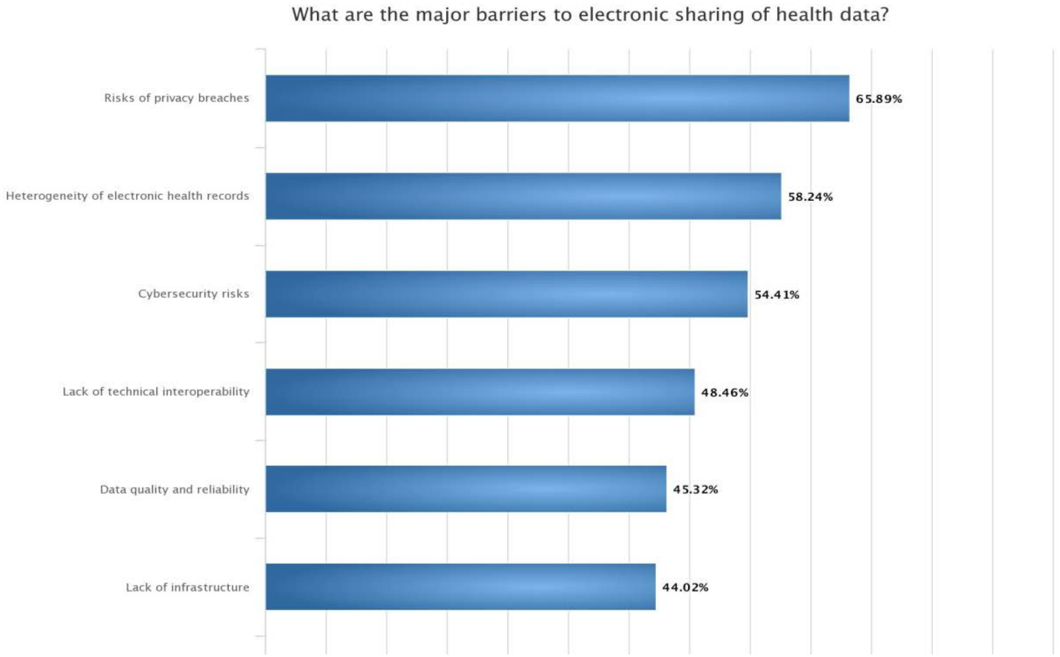
In preparation for the forthcoming Communication on Digital Transformation of Health and Care in the Digital Single Market an open consultation was organised that received more than 1400 contributions. The messages were clear:

- More than 90% of respondents agree that citizens should be able to manage their own health data;

- More than 80% think that sharing health data can help improve treatment, diagnosis and prevention of diseases;
- More than 60% agree that it would be useful to further develop infrastructure to pool health data and resources securely across the EU;
- Most respondents don't have access to digital health services at the moment. Of those who do not, two out of three would like to have it;
- More than 80% agree that citizen feedback to healthcare providers and professionals is essential to improve services.

When asked what the EU should do to overcome barriers to access and sharing of data, the top four actions were: develop **standards** for data quality and reliability; **standardise** electronic health records; propose **health-related cybersecurity standards**; and support **interoperability** with open exchange formats and interfaces.

Figure 1: Barriers to Electronic Sharing of Health Data



Source: European Commission

In conclusion, Ms Spanou said that we must start defining tomorrow's health and care in Europe. Digital technologies and data are transforming our society and the healthcare sector is no exception. Digital health solutions have already shown many benefits but still have much to offer in Europe and beyond, both to healthcare systems and to people. This will depend to a very large extent on a better use of data and empowered citizens that trust digital solutions. The question is not if this transformation will take place but how, where, and who will benefit from it. The Commission's ambition is to harness the power of health data and digital innovation to ensure that Europe will remain the global leader in delivering tomorrow's personalised healthcare.

In answering questions from the audience, the issue of the role of the EU versus Member States dominated. Ms Spanou stressed that healthcare remains a competence of the Member States and the Commission is not proposing anything that would affect the functioning of national healthcare systems. The focus is on investing in an interoperable system to increase the benefits of what is done at national level. We are not starting from scratch here: some countries are already well advanced but even here hospitals are often still poor at sharing data. Where investments are made, it should be on the basis of standards and interoperability.

GDPR and Health Care Data Management

Jos Dumortier, TimeLex (Belgium)

Health-related issues in the GDPR

The General Data Protection Regulation (GDPR) represents a major shift in the EU's approach to the regulation of personal data and has major implications for the health sector.

Patients have had right of access to their data for many years under EU and national laws. The GDPR extends these rights and introduces a new approach to what is already available. In the Netherlands, for example, an app is available that enables users to choose from a list of major companies and generates an email to request right of access. Most likely, companies will develop similar processes, or 'templates', in order to respond in the way that the new law requires.

The law provides clarifications on what constitutes health data, including new definitions of 'biometric data' and 'genetic data'. Prohibition to process remains the basic principle but there is a list of ten exemptions (e.g. explicit consent, public interest, provision of health or social care, …). Article 9.4 states that: "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health".

'Consent' is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. Processing of health data without consent is prohibited except for the stated list of exemptions and authorised secondary use.

Access rights have been strengthened, such that data subjects now have the right to access data concerning their health, for example their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided (recital 63). Profiling of data subjects is expressly prohibited (Article 22) and privacy impact assessments are mandatory for high-risk processing of personal data (e.g. large scale processing of health data).

The GDPR introduces several new measures in relation to security. As soon as a controller becomes aware that a personal data breach has occurred, he would be obliged to notify this breach to the supervisory authority. The individuals whose personal data could be adversely affected by the breach would also have to be notified in order to allow them to take the necessary precautions. Controllers have a general obligation to ensure appropriate technical and organisational measures are in place to ensure the protection of the rights of data subjects, but still having regard to the state of the art and the cost of implementation. Codes of conduct are encouraged under the Regulation and may include measures to ensure the security of processing. Codes may be specified by regulators, but also by associations or other groups of controllers. Companies may be held to keep binding promises in these codes. Finally, certificates such as data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors are encouraged.

Secondary use of health data

The re-use of health data for research purposes was the focus of intense debate while the Regulation was being negotiated. The Commission's original proposal required the consent of the data subject, which could be withdrawn at any time. The research lobby argued that this was impractical and drew attention to the substantial benefits for society from being able to use big data in health-related research.

The compromise negotiated under the GDPR states that personal data collected for legitimate purposes may be reused for scientific research purposes provided there are appropriate safeguards, in accordance with the GDPR, for the rights and freedoms of the data subject. Responsibility for providing those safeguards shifts from the Member States to the data controllers, which could be harmonised in future through codes and standards. The new data protection law in Germany specifies a list of possible 'appropriate safeguards': these include audit trails, awareness raising, pseudonymisation, and encryption. The possibility of dynamic consent is also being researched under projects such as EnCoRE.[4]

Cross-border exchange of health data in the EU

Health is a competence of the Member States and EU competences in this sector are quite limited. The main framework for EU efforts in this domain is the eHealth Network (eHN), which is being supported by the "Joint Action to Support the eHealth Network" (JASEHN) launched in 2015.[5]

Cross-border exchange of health data raises many legal issues. What should be the legal basis? (informed consent?); who should have access?; where does liability lie?; as well as other issues such as patient rights, minors, therapeutic exception, duration of storage, etc. Each Member State deals with these issues differently and matters become even more complex where cross-border exchanges are involved.

JAseHN was tasked to create a multilateral agreement for cross-border exchange of health data and the final text was adopted by the eHN in its May 2017 meeting. The agreement provides for Cross-Border eHealth Information Services (CBeHIS), focusing initially on patient summaries and e-prescription. Requests will be processed via National Contact Points for eHealth (NCPeH) and for these purposes 'healthcare' excludes public health. Various aspects of the implementation and governance are being finalised.

Asked whether data portability applied to the health domain, Mr Dumortier said the provisions of the GDPR on this issue were clearly applicable, but it does not appear to be a major issue in the health sector at present. In response to another query about codes of conduct for secondary use of data in healthcare, Mr Dumortier explained that these were still under development.

Privacy Preserving Processing of Health Data within the EU

Chair: Reinhard Posch, CIO, University of Graz, Austria

Wessel Kraaij (**University of Leiden/TNO, Netherlands**) described infrastructures for secure data analytics. Digital technology promises to redefine health and care in the EU, opening the way to value-based healthcare and more personalised health management. Data is integral to this vision: combining the right data may lead to important new insights. But at present data storage is fragmented and the GDPR limits the extent to which different data sets may be combined. The challenges are, firstly, to provide a trusted environment where individuals are able to control data access and sharing; and secondly to support secure and legal data analytics for combined datasets.

At present, data is partitioned in various ways (horizontally, vertically) and is then anonymized and/or pseudonymized for research purposes. But the more personal data is combined, the easier it is to re-identify a profile and the more difficult the anonymization process becomes. For example, personal well-being data (Fitbit, smartphone apps) are quite personal and could lead to re-identification using external data. Personal data may seem innocent, but can lead to valuable insights. Meanwhile, regulations regarding data processing and storage are becoming more strict, with data leaks leading to substantial fines and professionals reluctant to use big data approaches.

A citizen-driven healthcare economy could be the game-changer here. Citizens together form a Cooperative and a Community. The cooperative delivers a health data platform and governance structure that enables individuals to collect their data (medical and lifestyle). It also provides services for members and delivers services to customers. Data is controlled by citizens and patients themselves, who rely on their cooperative for support. MIDATA (see below) and PRANA (a project relating to childhood development), both in the Netherlands, are examples of this approach.[6]

[4] www.hpl.hp.com/breweb/encoreproject/

[5] http://jasehn.eu/

[6] www.pranadata.nl

Johan van Soest (**Maastricht University Medical Centre, Netherlands**) set out what he saw as prerequisites for a privacy-preserving data economy. Personal health data should be reusable and captured at source. Data should be machine interpretable and distributed, and federated data analysis approaches should be followed. Personal health data should be used responsibly within an open ecosystem and with incentives (pay backs) for data providers.

At present, the barriers to sharing data are not so much technical as ethical, political, and administrative. One solution is to share the algorithm instead of the data: in other words, to distribute it to every centre where it is needed, so allowing the data to be kept at the source where it is easier to maintain control. This is the approach followed by Personal Health Train, a Dutch collaboration of multiple universities and (technical) institutes.[7] Experience to date has shown that the results from such an approach generally converge and produce the same results as if the analysis was done centrally. Keeping data at the source gives different possibilities in handling and securing the data.

Finally, FAIR is a set of guiding principles for scientific data management and stewardship, specifying that services should be Findable, Accessible, Interoperable, and Reusable. These, too, provide a cornerstone of the infrastructure picture: we need to rely on FAIR data descriptions if we can't "see" the actual data when transporting algorithms.

David Chadwick (**University of Kent, UK**) described mobile patient access to hospital information based on work with the National Health Service in the UK. The system relies on verifiable credentials (VCs), potentially long-lived electronic credentials that the user stores under his/her control and uses as he/she wishes in order to access electronic resources. They contain certified identity attributes and authorisation tokens.

Most websites today are not able to verify a user's identity attributes: they either trust the user, or do not offer the online service. Furthermore, today's federated identity management infrastructures have a number of limitations that VCs address. For example, identity providers (IdPs) are the centre of the identity eco-system and know too much about the user's movements, as they issue short lived credentials for each service provider (SPs) (i.e. they can track the user). IdPs have to trust SPs to keep users' attributes private, which they may not trust them to do, while SPs may require users' attributes from multiple authorities or attributes that IdPs are not willing to assert A strong authentication system known as FIDO (Fast Identity Online), originally developed by the FIDO Alliance, has been adapted through the addition of identification and authorisation features that conform to the W3C verifiable credentials model. The University of Kent has used this solution to support an NHS use case that allows for transfer of VCs from the latest smart devices. It allows a patient to book or cancel a hospital appointment or order a repeat prescription online without needing a username or password. Instead the user authenticates to the smartphone using a fingerprint, and the phone using public key cryptography to send identity assertions to the hospital.

In summary, virtual credentials are privacy protecting: they give the user full control of their identity while the SP only obtains the attributes needed for authorisation and that the user consents to reveal. There is no globally unique correlating handle and the IdP does not know which SP the user is visiting. They protect against identity theft, are very easy to use, and in the limited user trials were unanimously liked by patients.

In his presentation, entitled Ethical Industrialisation of Personal Information, **Luk Vervenne** (**Synergetics, Belgium**) looked at how to mainstream ethical considerations in the personal health economy. Enterprises are being forced to become more user centric and the GDPR provides further impetus in that direction. A digital transformation that embraces ethics requires a new data utility infrastructure, or 'personal data store' (PDS), as a form of public good.

A PDS enables the user to be the custodian of personal data and empowers them as a stakeholder within the health data ecosystem. It enables a separation of functions between data (utility) and services (ecosystem). Within a data utility, all PDSs are part of a single end-to-end trust assured data

[7] See YouTube video at http://tinyurl.com/y9dcpao2

lake. Ownership of data is replaced by access–usage–delete rights. PDSs would be much more efficient and lower cost, especially if based in the cloud, making them attractive for SMEs; they could also automate GDPR-compliance. Their widespread use would, finally, allow the (ethical) re-use of personal data on an industrial scale and help to democratise access to analytics for individuals and SMEs, meaning it would no longer be the preserve of large corporates.

Regional or domain players could play a key role in providing these new data utilities. They would allow data and services to be separated. At one level would be an underlying data utility, comprising an end-to-end trust assured environment and cloud-based PDS. This would use a GDPR-compliant techno-legal-contractual trust framework to provide a level playing-field for organisational personal data management at scale. On top of this utility layer would sit many free or commercial ecosystem business models based on APIs.

Bian Yang (**NTNU, Norway**) spoke on "Enhancing Trust in e-Health by Secure and Privacy-Preserving Identity Management". Data is key to all in eHealth and is central to a 'Health 3.0' approach based on patient-centred data management. Essential factors here are that: a) the patient's full health data profile is accessible; b) the patient decides how and with whom the data is shared; and c) privacy is configured around the patient.

Approaches to privacy-preserving identity management in healthcare include:

1) Identity Proofing: Selective disclosure and certification of identity attributes; and anonymous attribute proofing / ownership verification.
2) Identity Authentication: Federated identities and Single-Sign-On (SSO); user-centric (e.g., OpenID, FIDO, GOV.UK Verify, etc.); and self-sovereignty identities.
3) Data Outsourcing for Analysis: embracing issues such as de-identification for data analytics; and re-identification (GDPR's right to access, portability, and be forgotten).

Research is needed in areas such as: privacy-preserving biometrics (renewability, irreversibility, unlinkability); privacy-preserving attributes proofing (selective disclosure, selective property/value proofing, and anonymous ownership verification); and distributed ledger technology for trusted platforms that enable subjects to identify themselves and trade their data for profit.

In the panel discussion, it was queried how society at large, and not just large corporates, could benefit from the huge value in aggregated data. Mr Vervenne explained that various forms of analytics could be used. Typically, analytics are performed next to the data, but analytics-as-a-service is an emerging market with many opportunities for SMEs. Open source solutions are also available. Mr Vervenne noted that the UK is passing a law that would make it illegal to seek identities from anonymised data and the EU should follow.

Several of the presentations had referred to homomorphic encryption and the panel was asked to comment on the maturity of this technology. Mr Kraaij said that in the case he had presented its use was relatively limited: the technology does not scale at present. It is used in a research context only and is not generally available for citizens, to which Mr Vervenne agreed.

Petra Wilson stressed that 'data ownership' is a difficult concept. It is not allowed for under English law and also is not mentioned in the GDPR. When working with data we acquire IP in the results, but have no rights in the data per se. Focusing on rights and governance is a far safer approach, Ms Wilson argued.

Building a Healthcare Data Ecosystem

Chair: Miguel Gonzalez-Sancho-Bodero, HoU EC/CNECT

Manuel Perez Perez (**ATOS, Spain**) noted that big data and cloud are two of the trends that are defining the emerging digital transformation in healthcare. The provision of big data capabilities using cloud delivery models shows a huge potential for a new era of combined applications that will bring cost savings and competitive advantage. Data-Analytics-as-a-Service (DAaaS) represents an approach to an extensible platform that can provide cloud-based analytical capabilities over a variety of industries, including healthcare.

Performing analytics in the cloud presents many challenges and requires the basic analytic workflow to be customised in various ways. In addition, real time processing requires different features than non-real time environments. These aspects are being explored in detail in CrowdHealth, a Horizon 2020 project studying Data Analytics as a Service.[8] CrowdHealth aims to deliver a secure ICT platform to collect and aggregate high volumes of health data from multiple information sources in Europe. It also proposes the evolution of patient health records (PHR) towards holistic health records (HHRs), enriched to become "Social HHRs" to capture the clinical, social and human factors.

Ernst Hafen (**ETH Zürich, Switzerland**) provided an update on MIDATA, a personal health data management cooperative that has already received significant publicity within the European healthcare community. MIDATA promotes a citizen-controlled approach to data access. It enables users to gather all of their different health-relevant and other personal data in one secure place. They can then decide to share data with friends or physicians or to participate in research by providing access to subsets of their data. In this way, users contribute to the development of new treatments for their own health.

MIDATA promotes trust at many levels. Cooperatives are owned by citizens and not-for-profit. The code is open source and is made available to partners agreeing to MIDATA's ethical and governance principles. Governance is transparent and a high emphasis is placed on security aspects, such as data encryption. It also offers a platform for innovation in healthcare.

The first use cases are being implemented at sites across Switzerland, including applications related to obesity, leukaemia, type-2 diabetes, multiple sclerosis and allergies. By working with European partners, MIDATA has the potential to democratise the personal data economy, providing an alternative approach to that offered by large corporates.

Catherine Chronaki (**HL7 Foundation, Belgium**) addressed the role of standards as an infrastructure for innovation in the data economy, and the role of the eStandards project in developing a roadmap for sustainable and collaborative standards development.

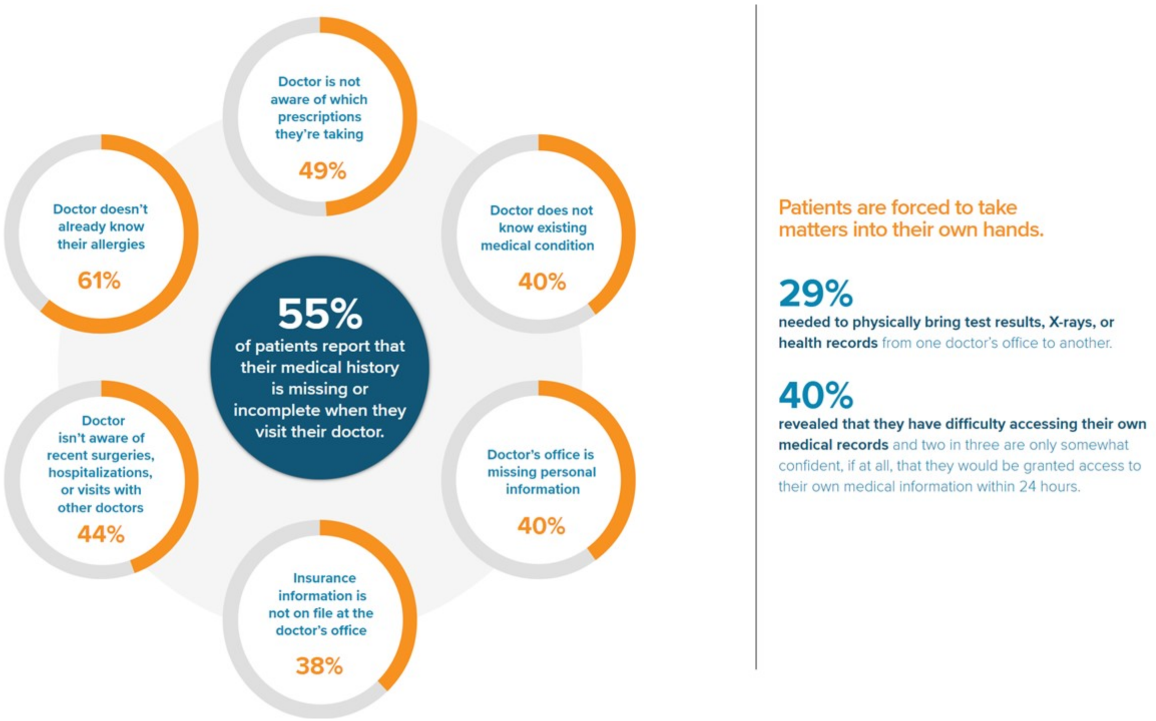
eStandards can unlock the transformative power of data. Today, we are moving from systems of record (e.g. simple documentation systems, such as EHRs), to systems of innovation that are able to unlock data and user experiences. As the speed of change increases, there is demand for more flexible governance. The adoption of eHealth at scale calls for cooperation among organisations developing standards and specifications, joining policy makers to address key challenges. The eStandards project aims to bridge this gap by promoting high quality widely-adopted standards that advance cost-effective sustainable interoperability. The project addresses three key aspects of digital for improving trust and flow in healthcare: co-creation – to make it real by using standards; governance – to make it scale for large-scale deployment; and alignment – to make it flourish in a sustainable way.

Patient summaries – dashboards that collect all personal health information together in one place – are being used as an example. The aim is to develop a specification for an International Patient Summary (IPS) that focuses on a minimal and non-exhaustive set of information that is specialty-agnostic and condition-independent, but still clinically relevant. This would be used, for example, to

[8] www.crowdhealth.eu

provide support for cross-border or cross-jurisdictional emergency and unplanned care. Practitioners need to join forces to make digital health happen: patient summaries could be a useful starting point.

Figure 2: Patient Experiences in Accessing Their Medical History[9]



Joan Guanyabens (**SalusCoop, Spain**) described Salus.coop, a Catalonian initiative for personal health data similar to MIDATA.[10] Salus started one year ago to explore a citizen-driven model of collaborative governance and management of health data. This model should enable citizens to share their health data to accelerate research and innovation in healthcare, thus maximizing social and collective benefits. It envisages a scenario where data providers – individuals, apps, and public/private health centres – will transmit their data users, who would be either private companies, aiming to provide personalised services, or researchers in the public or private sectors. The Salus cooperative will mediate these transactions, with citizens acting as both data donors and administrators.

A feasibility study undertaken in Barcelona in 2016 helped to identify the perceived benefits of the approach and also barriers, both for citizens and among agents. Most importantly, it highlighted that such an approach requires systemic change at many levels. Data is no longer scarce but abundant; management has to shift from the individual to the collective, while delivery channels move from intermediaries to being direct. Knowledge becomes symmetrical rather than asymmetrical, publications are integral rather than selective, and the number of actors involved increases many fold. Finally, innovation shifts from products to processes. An ethical code for this 'health data commons' is now being planned, including principles for data governance, and two pilots are being implemented focusing on noise pollution and breast cancer.

Claus Nielsen (**DFG Foundation, Denmark**) recounted his personal experiences and those of family members in dealing with the healthcare system in Denmark. This prompted him to form the Data for Good (DFG) Foundation as a not-for-profit foundation and a public health project that aims to allow citizens the right to control their own personal data. In other words, we need "smart health". Smart health is about offering the right products, interventions and services to the right people at the right time in the right context. This sounds easy but is difficult in practice because of cultural

[9] http://surescripts.com/connectedpatient/default.html, quoted by Ms Chronaki.

[10] www.saluscoop.org

differences. DFG is working to break down these barriers and create a fair market for personal healthcare data.

During the discussion, the panel was asked whether the cooperative model was being portrayed in opposition to the ‘winner takes all’ approach and whether, with their inherent instability and lack of overall control, cooperatives were being set up to fail. Mr Hafen responded that neither proposition was true. Rather than taking away from traditional models, cooperatives create a parallel economy under the control of the citizen. We need a data economy where people have many options open to them in how they ‘spend’ their data, as in the financial sector. There will be room for many different models and by empowering citizens cooperatives will have a big role to play. Mr Nielsen agreed. DFG has been set up as a foundation so as to be able to donate back to society in an ethical way; similarly with MIDATA. These could provide a model for Europe that runs alongside Facebook and other providers. Asked about the potential for Salus, Mr Guanyabens explained that the concept of Salus coin was being considered as a cryptocurrency to use within the ecosystem. This is only an idea at present: it could be implemented through blockchain.

Pan-European Coordination and Policy

Chair: Paul Timmers, independent digital economy & society advisor

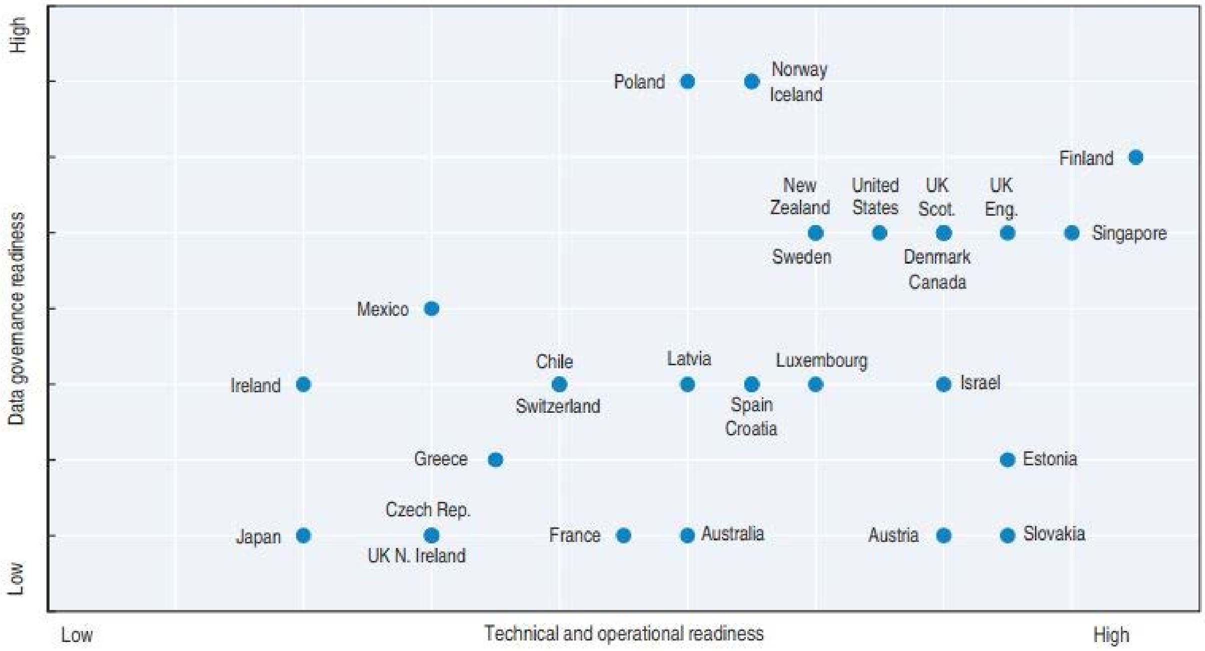
Sonja Marjanovic (**RAND Europe, Belgium**) argued that the benefits of health data fall into three categories. Firstly, it may be used for research and innovation, such as to explore new avenues for research or improve the quality of research outcomes. Secondly, data may be used for pharmacovigilance and public health, including enhanced emergency preparedness. Thirdly, data feeds into healthcare delivery and health systems more widely by improving quality and delivering operational and efficiency benefits.

Collaboration and coordination, public acceptability, data protection regulations, data quality and interoperability, and workforce capacity are all important building blocks for supportive health data ecosystems. In terms of regulation, the GDPR is paving the way towards a clearer framework but many challenges remain. Workforce capacity is often overlooked, yet it will be essential to equip workers with the skills and competencies to engage with, interpret, communicate and act on health data. This can be tackled through educational curricula and CPD. Empowerment is also needed for patients and the public, researchers and regulatory bodies.

Effy Vayena (**ETH Zürich, Switzerland**) looked at how ethics are central to the digital health debate. We used to think of health data as coming from standard, well defined sources, even if the related ethical issues were not all solved. The range of sources is growing and is facilitated by technical and policy capabilities that also have ethical aspects, and are relevant to growing numbers of stakeholders. Meanwhile, approaches and readiness vary across the developed countries (see figure). In short, the health data ecosystem is becoming ever more complicated, creating tensions at many levels.

The path from raw data generation to demonstrated health benefits has to overcome various hurdles, most of which are well known: data access, data protection, evidence, accountability, and trust all come into the frame. Trust affects all actors, institution to institution as well as individual users. Among other issues, Prof. Vayena emphasized the principle of data fairness: i.e. data that can be used for research purposes and research results should be made available for further research use to advance the common good of scientific knowledge.

Figure 3: Health Data Readiness in OECD Countries



Source: OECD

The debate here often gets stuck on the issue of access. We have to move on to consider how the benefits should/will be shared: a more positive approach will shift the mindset.

Petra Wilson (**Health Connect Platform, Belgium**) stressed that eHealth is a journey, not a destination. At present, the European eHealth ecosystem journey has some missing links. It requires 'fuel' (more data), 'ignition' (better interoperability), and 'regulation' (better governance). Without proper accreditation for providers and services, we will undermine trust. Without proper governance rules, we will end up in court. Without legal requirements for standards and interoperability, we will misunderstand the message and cause harm. Without properly adjusted legal rules, we will lose the good will of clinical partners. And by failing to create new rules and new procedures we will miss a panoply of opportunities to provide better, safer and more accessible care. Member States appear to be frightened by the implications of the GDPR and are arguing for slower implementation: we cannot afford to let that happen.

Lars Rohwer (**Siemens Healthineers, Belgium**) described Siemens' activities in the healthcare sector. The company has a broad portfolio in diagnostic imaging, as well as lab automation and assays. It has around 45k employees in 75 countries and revenues of about €13bn with €1bn reinvested into research and development. Under an announced IPO, in 2018 these health-related activities will be spun out from Siemens AG as a new separate business, Siemens Healthineers.

Siemens has around 600k medical devices installed at sites around the world that generate vast amounts of data, much of which is not used today. Healthineers will focus on helping customers extract value from this data. There are other opportunities, too, such as creating digital twins of real-world devices for practitioners to experiment on. The efficiency of pacemakers, for example, is highly sensitive to where they are positioned on the heart. Being able to experiment with a digital twin allows the surgeon to model the performance before applying on the patient.

Lars Rohwer emphasized that close collaboration between policy makers and stakeholders from academia, healthcare, patients and industry is key when it comes to regulating digital health. Firstly, since not only regulations are evolving but also the portfolio of digital solutions, it is important to prevent "unintended side effects" on potential beneficial solutions in healthcare by regulatory initiatives on digital in other sectors since those initiatives typically have horizontal, cross-sectoral implications. Secondly, "shoot first and ask later" approaches are a well-known phenomenon of disruptive digital businesses, and are especially inappropriate when it comes to the health and care of people. Close collaboration would also support mature and responsible going-to-market approaches and ensure the provision of meaningful digital innovations in healthcare.

Magda Rosenmöller (**IESE Business School/EIT Health, Spain**) outlined the activities of the new EIT Health, where big data is a strategic focus. EIT Health is one of the Knowledge Innovation Communities (KICs) set up by the European Institute of Innovation & Technology (EIT). Like all KICs, it integrates three pillars: education, innovation, and support for start-ups and entrepreneurs. These services are provided by a strong partnership of committed, experienced and highly competent partners in academia, industry (pharma, medtech, ICT, large and small), research centres, testing labs, incubators and accelerators.

EIT Health summer schools and short courses have been organised, including an Executive Masterclass in Healthcare Informatics; SensUs, a novel training programme on sensors for healthcare; and FHME, a programme to understand the competencies of future healthcare managers. Other activities include participation in GENiE, the Global Educators Network in Health Care Innovation Education; and StarShip, a fellowship programme for healthcare innovators. From a policy perspective, EIT Health Think Tank is looking at barriers to innovation that need to be overcome in order to tackle the future burden of chronic diseases on healthcare systems and their sustainability.

In the discussion, Prof. Vayena was asked how ethics could apply to an ecosystem. She saw it as being a governance issue, applied through oversight that is systemic across the ecosystem. This requires us to rethink certain frameworks.

Ms Wilson commented that there are interesting examples of people learning from other sectors and apps, for example cities using an asthmatics tool for environmental monitoring. At present these are isolated examples and too much is spent on pilots that do not achieve anything (‘pilotitus’): we need to join up existing examples of good practice wherever they are found. Mr Timmers quoted similar examples from the energy sector, where data from consumer devices is being collected for energy management purposes.

The field of health data research and policy is highly dynamic and there is a need for further reflection, thematic learning and evaluation to better understand how to create and connect receptive places, to inform future interventions and to identify transferable lessons. Scale up and sustainability should be high on the priority agenda.

Conclusions

The workshop highlighted recent developments and progress on various fronts in relation to a European ecosystem for healthcare. At policy level, the DSM Mid-term Review and developments under the Estonian Presidency have put the issue of digital health firmly on the policy agenda. The forthcoming Communication on Digital Transformation of Health and Care is sure to stimulate further debate.

Key points from the workshop presentations and related discussions included the following:

1) **The GDPR has significant implications for the health sector and will spur innovation:** Implementation of the GDPR is fast approaching and promises to bring a major change in culture relating to personal data in Europe. The specific implications for the health and care sector are not fully clear as yet. What is clear, however, is that the GDPR will be a spur to innovation and for this reason alone Europe cannot afford to ease off on implementation.
2) **New privacy-protecting approaches to the processing of personal data:** New identification and authorisation technologies, such as verifiable credentials, overcome the limitations of current systems, giving users full control over the disclosure of their health and other data. Such technologies allow a privacy-by-design approach, where privacy is configured by and around the user.
3) **Separation of data and services promises significant business opportunities for Europe**: Data and services are emerging as separate elements of the health data ecosystem, each with its

own needs and requirements. Data will increasingly become a utility that runs over an end-to-end trust-assured cloud-based infrastructure. The business value will be in apps and services (e.g. data-analytics-as-a-service) provided by corporates, start-ups and SMEs. Both aspects represent significant business opportunities for Europe. The vision is for users to have the same level of choice in storing and transacting their health and other personal data as they have at the moment in the financial sector.

4) **Exploiting experience in citizen-driven health data initiatives:** Europe has growing experience with citizen-driven health data initiatives, such as DFG, MIDATA, PRANA and Salus.coop that follow various models. There is a need to network and share experiences between these initiatives, as well as to better define their relationship to other actors (e.g. companies and publicly-held databases) in building health data ecosystems.
5) **Efforts on standards and interoperability must reflect user requirements and needs:** Standards can unlock the transformative power of data and are key to the EU's three policy priorities: secure cross-border access; world-class data infrastructure; and citizen empowerment. Use cases, such as the International Patient Summary, will help ensure that efforts in relation to standardisation and interoperability reflect the requirements on the ground; it is essential that practitioners play an active role in their development.
6) **Building workforce capacity for health data**: As digital health becomes a reality, a major effort in skills and training will be required. The health and care workforce across the board needs to be upskilled, not only in relation to the technical innovations but in the legal and regulatory aspects as well. The EIT is leading the way here and more needs to be done to scale up the training effort and mainstream the lessons from these initial experiences.
7) **An ecosystem approach to ethics**: Ethics is central to the digital health debate. We have to explore how to apply ethics within a health data landscape that is evolving rapidly and becoming ever more complex. Rather than focusing on the ethics of access, we should move the debate on to consider how the benefits should/will be shared within an ecosystem approach.