REPORT	3 JUNE 2022
SECRETARIAT/ SDM	CPME 2022/023 FINAL

European Doctors (CPME) represent national medical associations across Europe. We are committed to contributing the medical profession's point of view to EU and European policy-making through pro-active cooperation on a wide range of health and healthcare related issues.

Challenges of health data in Europe- Are we preparing?

Building trust – Enabling Science

#ProtectHealthData

On 6 April 2022, the Conseil National de l'Ordre des Médecins (CNOM) and the Standing Committee of European Doctors (CPME) held a joint event entitled 'Challenges of health data in Europe – Are we preparing?'. The event was hosted within the context of the French Presidency of the Council of the European Union and was intended to contribute to the inclusion of digital health in an ethical framework through the application of the European principles for ethics in digital health.[1]

Dr Patrick Bouet, CNOM President and Dr Christiaan Keijzer, CPME President co-hosted and co-opened the event. Dr Patrick Bouet noted that every country has been impacted by the increasing opportunities and challenges relating to the use of health data. In Europe data has been used for a long time and should continue to be used for the public good. Dr Christiaan Keijzer stated that sharing health data would help with the prevention of diseases, patient-centered healthcare, and improved treatment alternatives if done ethically and lawfully. Any data exchange needed to be built and maintained on the basis of trust and would be rejected otherwise.

Mr Dominique Pon, French Ministerial eHealth Delegation, opened the floor with a statement on eHealth data, its use and interpretation. He noted that health data sharing needed to be patient-centred, respecting patient autonomy and medical confidentiality. As part of the digital health strategy, the French Presidency had a double objective: first, ensure that the ethical dimension for

[1] <https://presidence-francaise.consilium.europa.eu/media/zp2jt3up/european-ethical-principles-for-digital-health_fr_eng.pdf> and <https://presidence-francaise.consilium.europa.eu/media/mw3b3zjq/european-ethical-principles-for-digital-health-introduction_vdef_revue-002.pdf>.

health data processing was respected; second, develop the digital single market. He further noted that the French digital roadmap was based on three principles - ethics, sovereignty, and transparency - and that ethics would be at the forefront of their efforts. Ethics consisted of four other principles: do good (beneficence), do no harm (nonmaleficence), autonomy, and justice. These principles were at the heart of the framework. With regards to sovereignty, Mr Pon mentioned that there was a need to oversee the platforms where health data was currently being exchanged, in order to control their destiny. He said that *"these platforms should be made by us*." Since 3 February 2022, *"Mon espace sante"* had been provided to all citizens in France, where citizens could store their health data in a safe way and share it with healthcare professionals, respecting personal data protection and ensuring data integrity. This way citizens would be active in relation to their own care. The platform also had a secure messaging system where the patient could discuss with the doctor. He concluded by referring to the European Health Data Space (EHDS) and that ethics would be a main pillar therein.

Dr Jacqueline Rossant-Lumbroso, CPME Vice President moderated the panel discussion. The main highlights were the following:

Mr Gérard Raymond, France Assos Santé President, gave an overview of his perspective on the exchange of health data in France, the role that doctors should have, whether patients would be open to health care data exchange and how patient trust could be built. He noted that France had a healthy democracy where patients were entitled to help, assess, and have an active voice about their healthcare system. He welcomed the French eHealth strategy that was now becoming an EU strategy. Four principles needed to be respected in order to build patients' trust: ethics, transparency, humanism and solidarity. It was important that patients were reassured and that they trusted how their data was being stored and used. He mentioned that the tools made available in the eHealth framework needed to bring added value, to improve patient health as well as relationships between healthcare professionals and patients. The health space in this digital health platform – *the "Mon espace santé"* - did this since everyone had their own storage site where they could access their data. He stated that patients were becoming real managers of their data and that they needed to be convinced that health data stored and collected in an anonymous way could help improve the healthcare system. However, the challenge was to win the patient's trust. He noted that patients were active partners in the creation of this digital framework and that people need to be convinced that these tools were for everyone's benefit and that it could help enhance patient-doctor relationship, and patient-research relationship in healthcare. In order to build patient trust, Mr Ramond noted that it was important to listen to patients more effectively and that physicians need to be open to what patients were saying. If patients felt free to exchange ideas, then they would be more inclined to exchange data. To build trust it could be useful to focus on people with chronic diseases such as diabetes or heart diseases, for a pilot study to show the advantages of these processing health data and expand the model to other patients in a second step.

Ms Jessy Pollux, CNOM Data Protection Officer (DPO), explained why CNOM had a DPO and the challenges that DPOs faced daily. CNOM collected data, had health databases, and therefore needed to comply with regulations on data protection, which necessitate a DPO. DPOs provide

independent advice that help managers make the right decision, respecting the data subject rights, and to be coherent from a legal, technical, and organisational point of view. According to Ms Pollux, DPOs have a crucial role in the safe exchange of data, such as securing doctor's digital identity. DPOs would face many challenges. First, for Ms Pollux, the DPO needed to reconcile three different actors and interests: the Medical Council while carrying out its public role, doctors, and patients. Second, DPOs must follow the ever-increasing legislative requirements to keep up with procedures and processes. There were many new French and European laws to ensure safe data usage in the past years. Sometimes there were too many which caused for more constraints than advantages. Third, there were cyber threats every minute – health data was very valuable for cyber criminals.

Mr Markus Kalliola, Project director from the Finnish Innovation Fund Sitra, gave an overview about how Finland was facing health data sharing, what measures had been taken, and the TEHDAS activities. Mr Kalliola noted that Finland had taken multiple measures to ensure data sharing, which could be divided in primary and secondary use of health data. For primary use, Finland had a central patient archive where patients could see their own health data and prescriptions. For secondary data, meaning using health data for purposes other than the primary reason for which they were originally collected, Finland had a novel set up. A new act had been passed in the parliament called the Findata. This organisation collected data, pseudonymized it and provided permits to data users under certain conditions. Researchers who applied for this data could access it from a secure environment. Once the research was concluded, the data they received was removed from the secure environment. People in Finland can opt-out from Findata, but many did not do this, as the Finish citizens trusted the government.

Mr Kalliola, also informed about the Joint Action Towards the European Health Data Space (TEHDAS). This was an action funded by Member States and the European Commission to support them in building the EHDS and developing principles for the cross border secondary use of health data. A regulation on the EHDS was expected early next month. Mr. Kalliola believed that the impact for doctors on the secondary use of data would be limited, although for the primary use of data the impact would be high.

Dr Ignacio Alamillo-Domingo, Spanish Medical Council digital transformation director, provided an overview of the main risks for doctors and the healthcare sector infrastructure. He also explained what consisted of self-sovereign identity (SSI), why it was needed and how would it work. Mr Alamillo-Domingo informed that the SSI was a new way to manage identity giving individuals control of their digital identities. He highlighted four main risks in digital health. The first risk was about identity theft of doctors or patients, as there was no assurance that a medical doctor or a patient was indeed a medical doctor or patient, which would have a possible impact on prescriptions. The second risk was about legal validity and recognition of medical documents (e.g prescriptions, certificates) as platforms were adopting different types of electronic signatures. Documents would need to be qualified in terms of admissibility. The third risk was about not being able to connect to patients' records across borders. Several agreements and circles of trust were needed. The fourth risk was about the legal position of being a data controller of patient data. Medical doctors were liable for ensuring that there were security measures in place by platforms where patient data is held or

exchanged. There was a need for solutions to all these risks, otherwise it was too risky to add doctors to these platforms and conduct medical acts. For Dr Alamillo-Domingo, the SSI would help and it would be equivalent to a national identity card. It would be possible to prove one's identity via an electronic card which would be stored in mobile phones. A legislative proposal had been launched by the European Commission called the "eIDAS Regulation" or the digital identity act.[2] From a medical perspective, physicians would be able to show their identity when accessing digital health data in another Member State and would be able to access to it directly.

Recommendations

In order to be prepared for the digitalisation of healthcare in Europe, Mr Raymond recommended that the relevant actors discussed together these issues and expressed their concerns. Ms Pollux proposed that medical associations continue to invest in digital education. Mr Kalliola noted that voluntary cooperation between Member States was no longer sufficient and there was a need to focus on permanent structures embedded in law. Dr Alamillo-Domingo believed that the role of medical associations should be to provide secure systems to doctors. Moreover, professional associations should bear the responsibility of proving the identity and qualification of a medical doctor. Doctors should have a usable qualified identity in their digital wallet. Mr Pon noted that digital health needed to be built step by step. Digital tools were not just tools but an environment. There was a need to understand the magnitude of digital health and to think about it together. Otherwise, big data companies would take over, and that would not guarantee a safe Europe.

Discussion

A debate followed about whether patients could potentially sell their health data and whether doctors should share their data for research or policy-making purposes, and in doing so if they should receive monetary compensation, academic credits, or a symbolic reference. Mr Raymond considered that data belonged to an individual rather than to a doctor. If data was given to doctors, then it was their responsibility to hold on to this data. If data had been processed and made anonymised, then it was important that patients were kept up to date about the research that was being conducted. Selling data, in his view, was not ethical. Mr Kalliola noted that Finland did not allow for health data to be sold, although that there was a cost/fee for accessing to health data. Dr Alamillo-Domingo mentioned that doctors had started using digital platforms, which had their own way of storing data. It was important to make sure that these platforms did not allow health data to be sold. Ms Pollux added that sooner or later health data will be resold either by the doctor, by the patient or by platforms. It is important to anticipate this because currently entities already give their health data via connected objects (connected watch, smartphone etc.). In fact, platforms had data that they could exploit.

A question was raised by Mr Rudolf Reibel (Head of Brussels Office of the German Medical Association) regarding the secondary use of data. He mentioned that there was a large agreement

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.

that scientific research could be linked to product development, service development, and commercial services. He questioned how it could be ensured that the purpose served the public interest and not the data user. Mr Kalliola stated that this had caused a lot of debate. In Finland, they defined the purpose in their legal act, which included research and innovation. Private and public companies were able to pseudonymise data if they did scientific research. In their legal act, they do not define who can access this data, but rather the purpose of the data.

A discussion was also held after Ms Sarada Das (CPME Deputy Secretary General) questioned who would bear the costs for the digital transition in small medical clinics / practices, adjusting to the electronic health record or the health data spaces. In France, the social security bore the cost. In Norway, small practices, GPs and doctors working in private clinics had paid a great deal to access these systems which had been imposed on them. As a result, doctors avoided connecting to these platforms as they were very complex, and the time spent to process data therein was not accounted for. Dr Christiaan Keijzer (CPME President) and Dr Jacques de Haller (CPME Past-President) believed that these systems should be financed at a European level in order to prevent different systems and different types of financing. Mr Kalliola noted that the Data Governance Act recognises that financial and administrative costs are to arise, foreseeing fees related to the processing of requests for the re-use of data. The costs to data users and sharing providers were to be counterbalanced by the value emanating from broader access and use of data, as well as with the market uptake of novel services.

Conclusion

Closing remarks were provided by Dr Ray Walley, CPME Vice-President, and Dr Patrick Bouet, CNOM President. Dr Walley stated that the discussion considered various national viewpoints, the EU added-value, some practical advice for physicians, national medical associations, and the government. He noted that the healthcare sector needed to evolve and adapt. With the impending Artificial Intelligence Act and the future Regulation on European Health Data Space, a new language was being created. Therefore, it was important to get the legislation right. Dr Bouet concluded by noting that all speakers and participants had unanimously agreed with the theory. There was no one expressing a different view on health data management in the public interest. The governance responsibility relied on decision makers to create digital tools that were used appropriately. Governments needed to play a role and soon as. There were several operators in the market which needed to be regulated.

***