image: KTSDESIGN /SCIENCE PHOTO LIBRARY / Getty Images

Rocco Panetta Managing Partner
r.panetta@panetta.net

Lorenzo Cristofaro Senior Associate
l.cristofaro@panetta.net

P&A | Panetta & Associati, Rome

A closer look at the EU-funded My Health My Data project

The EU-funded project My Health My Data ('MHMD') looks to introduce a new way of sharing medical information and empowering their primary owner, the patient, using encryption solutions and the blockchain. Here, Rocco Panetta and Lorenzo Cristofaro of P&A | Panetta & Associati, who have been involved in the MHMD project since its initial proposal to the European Commission, explain the aims and value of the MHMD project.

While the deadline for the General Data Protection Regulation ('GDPR' - Regulation 2016/679) is looming in all EU Member States, the European eHealth sector is expecting new technological upheavals, involving both private and institutional players, which should accelerate growth and trigger true innovation.

The EU-funded My Health My Data ('MHMD') project stands at the very centre of this change and aims to revolutionise healthcare from within, by making patients and individuals more aware of the real value of their health data, by means of a secure and distributed technological ecosystem. The very essence of MHMD is built on one of the main pillars of EU data protection law, the principle of *habeas data*, which grants individuals the right to take back control of their personal data, with crucial consequences from a legal, social and economic point of view.

The project has been conceived, from the outset, with a view to changing the way sensitive data are shared, making use of an innovative distributed model of smart contracts that enforces consent mechanisms and peer-to-peer data transactions between public and private healthcare providers and patients. The ultimate goal is to transform the data access and control rights that individuals are vested with under applicable law into a straightforward innovation enabler for both the public and private clinical sectors, in order to foster medical and scientific research while setting novel security benchmarks, especially in light of the forthcoming GDPR. The current state of the art of EU digital healthcare shows a myriad of isolated, locally hosted and unsafe medical data repositories which are often subject to violations and data breaches, caused by both internal issues and outside threats (i.e. WannaCry and the like).

In this context, patients and individuals are understandably discouraged from giving their consent to the processing of their data for further medical research purposes, as in most cases they are not (put) in the position of having a clear understanding of who is using their data, for what purposes and, most importantly, what measures have been implemented to safeguard this information.

The MHMD project aims to change this scenario, enhancing the value of data subjects' consent and granting them effective and ongoing control of their data flows through personal accounts operating on a dynamic multi-platform basis.

By gathering clinical records from all medical stakeholders (hospitals, research centres and businesses) and wellness data via a specific mobile app, featuring privacy-by-design, while boosting patients' continuous monitoring of their data flows, the project reflects the switch of paradigm provided by the disintermediation of healthcare services through advanced technology and big data analytics.

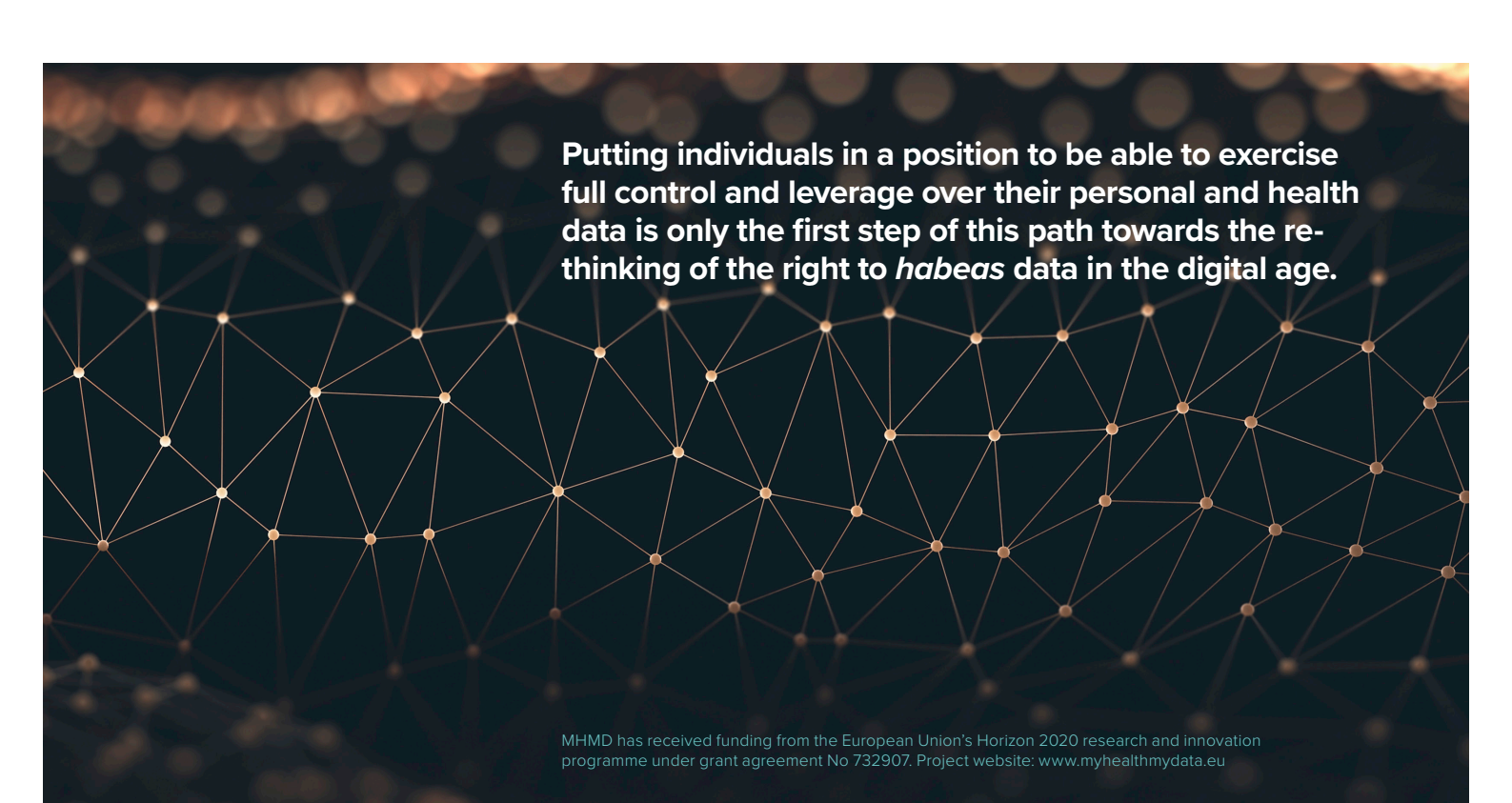Patient related data will be classified based on their nature and scientific value, so that the most suitable and robust de-identification and encryption measures can be applied, which still allows advanced knowledge discovery through analytics and deep learning applications running on a growing amount of anonymised or pseudonymised data.

To achieve such goals whilst complying with the GDPR, the project has been built on four main operational pillars, aimed at ensuring that all pivotal requirements of the regulation will be properly implemented: dynamic consent, personal data accounts ('PDAs'), smart contracts and encryption techniques, all embedded in a blockchain-based network.

Within this architecture, information relating to the distributed storage of health data are trimmed in a hash-based language code ensuring the highest security standards.

The most advanced encryption techniques (some of which are currently being examined at international level) will be deployed throughout the entire infrastructure, such as secure multi-party computation, homomorphic encryption and PEP - polymorphic encryption and pseudonymisation - in order to secure all the information running on the blockchain.

Data flows will be continuously validated by the entire network of blockchain users, avoiding any possibility of fraudulent usage, while also reducing the risk of data breaches or losses. Smart contracts will also play a crucial role in the project, as they are the best tool, on

Putting individuals in a position to be able to exercise full control and leverage over their personal and health data is only the first step of this path towards the re-thinking of the right to *habeas* data in the digital age.

account of their self-executing nature, for automatically regulating data flows between data subjects and stakeholders, in such a way as to create a pan-EU (and then, hopefully, an international) network of healthcare data for research purposes. As in real life transactions, rights and obligations built into the smart contracts will be binding among all the parties operating within the MHMD environment and connected to each data subject's true expression of will.

Individuals will be put in a position to modulate, by means of a granular consent interface embedded within their personal data account, the permits - then enforced by smart contracts - for accessing and processing their data by each stakeholder, whether a research centre, a healthcare facility, a business or other organisation.

In this way, patients will finally be able to fully leverage the value of their personal data, for instance, turning to different healthcare professionals for second opinions in a much smoother way, or finding patients with similar conditions and contacting them when they receive permission; similarly they may decide to share their health information on a monthly basis with their local hospital and not with their personal physician, or provide information for research purposes to biomedical centres and universities, and so on.

A straightforward probative, secure, open and decentralised technological framework will be created which will enable patients to securely share their personal and medical information with third parties, whilst keeping full and ongoing control over any first or further-compatible processing carried out by the various stakeholders joining the project, all bound by the strong security policies governing the blockchain and the relevant data exchanges.

The overall security of the project's multi-modular architecture will be tested repeatedly through dedicated self-hacking simulations and public hacking challenges, performed on synthetic data sets.

Consistent with the novel benchmark set by the GDPR, the whole project has been designed in such a way as to fulfil, also in the light of a specific data protection impact assessment, the requirements of privacy-by-design and by-default. This means, in reality, that all measures and safeguards will be put in place as necessary to ensure the implementation of the key principles set forth by the GDPR and, particularly to avoid the collection (and processing) of personal data which are not reasonably essential to achieve the intended research purposes.

In addition, the whole distributed infrastructure and the processes underpinning its functioning are being developed by a joint technical/legal team, in order to ensure that all the rights provided for by the GDPR can be easily exercised at any moment by the data subjects, as long as (some of) these rights are not likely to render impossible or seriously impair the achievement of the objectives of the research (e.g. the right to erasure). The concrete application of so many disruptive technological innovations is obviously proving to be more than challenging. Nonetheless, thanks to in-depth analysis of the current and forthcoming regulatory framework and the involvement of a wide team of multi-disciplinary experts, the project - also as a bench mark - is increasingly attracting the interest of both institutions and market players and is already building, step by step, a brand new European eHealth and biomedical research ecosystem.

Disintermediation of digital personal medicine and the Internet of Things are in the spotlight, as are distributed ledger systems: that is why the MHMD intends to bring the discussion to a new level, by fostering the use of blockchain and patient-centric technologies, in order to provide a new basis for digital disruption in the scientific research and healthcare sector.

Putting individuals in a position to be able to exercise full control and leverage over their personal and health data is only the first step towards the re-thinking of the right to *habeas* data in the digital age.

The ultimate goal of the MHMD is to help the development and consolidation of the first health distributed data marketplace in the EU, based on common rules, fairness, transparency, robust security standards, openness and full and substantial interoperability criteria.