MY HEALTH
MY DATA

Edwin Morley-Fletcher, Lynkeus

H2020-ICT-18-2016 - Big data PPP: privacy-preserving big data technologies
Grant agreement no: 732907 - EC Budget 3.455.190,00
Duration: 1st November 2016 – 31 October 2019

MHMD Peculiarities and Mission

- **Biomedical**

  Issues of data subjects' privacy and data security represent a crucial challenge in the biomedical sector, more than in other industries

- **Privacy and Security**

  This makes it the ideal field to build and test new models of privacy and data protection, and the technologies that encode them

- **Blockchain and Personal Data Accounts**

  MHMD aims at changing the existing scenario by introducing a distributed, peer-to-peer architecture, based on Blockchain and Personal Data Accounts.

- **New mechanisms of trust and value-based relationships**

  MHMD is developing new mechanisms of trust and of direct, value-based relationships between people, hospitals, research centres, and businesses, in what is going to be the first open biomedical information network centred on the connection between organisations and the individual.

MHMD ambitions to:

- **Profile and classify** sensitive data based on their informational and economic value
- Assess the most suitable and robust **de-identification** and **encryption** technologies needed to secure different types of information
- Allow having **advanced analytics** running on anonymised or pseudonymised data
- Evaluate the overall security of MHMD multi-modular architecture by testing it through dedicated **self-hacking** simulations and **public hacking challenges**
- Analyse **users' behavioural patterns** alongside **ethical and cultural orientations**, to identify hidden dynamics in the interactions between humans and complex information services
- Improve the design of **data-driven platforms**
- Foster the development of an **information marketplace**, in which both individuals and clinical institutions will be able to exert control on their health data and leverage their value

MHMD Assumptions

- **It is now possible to reverse Ronald Coase's Transaction Costs**
- **What Internet did to transaction costs regarding information, blockchain can do regarding trust**
- **What is needed for health data is a Distributed Empowerment system**
- **Based on a portfolio of Smart Contracts**
  - Smart contracts are the executable pieces of code, stored on the blockchain for future execution, which bind people and transactions to specific actions and outcomes.
  - They require no further direct human involvement after the smart contract has been made a part of the distributed ledger, which is what makes these contracts "smart", or autonomous.
- **It is highly worthwhile to analyse such a system within the EU GDPR, checking its applicability as an operational Infostructure**

  Where data transactions are informed and controlled by the principles of:
  - Lawfulness, fairness, transparency, purpose and storage limitation, data minimization, accuracy, security, accountability,
  - Satisfying data subjects' requests such as the right to modify, erase, be forgotten, donate data, withdraw consent, or even access a copy of his/her data
- **Can the blockchain ensure compliance with the GDPR requirements, yet making this happen seamlessly and efficiently, at scale?**

MHMD Participants

- **5 SMEs:**
  Lynkeus (Italy) [Coordinator], Digi.Me (UK), HW Communications (UK), Gnúbila (France), SBA Research (Austria)
- **4 Clinical partners:**
  Deutsches Herzzentrum Berlin (Germany), Ospedale Pediatrico Bambino Gesù (Italy), Queen Mary University London (UK), University College London (UK)
- **4 Research centres and Academia:**
  Athena Research (Greece), Consiglio Nazionale delle Ricerche (Italy), HES-SO (Switzerland), Universitatea Transilvania din Brasov (Romania)
- **1 Legal consultancy:**
  NCTM (Belgium-Italy)
- **1 Industry:**
  SIEMENS Healthcare (Germany)

Strategically Relying on Four Leading Hospitals

- Following the example of routine data inflow by the OPBG PCDR, and the interoperability system established in Cardioproof and MD-Paedigree
- Taking into account the less restricted data processing allowed by the GDPR when it is aimed at scientific research, and the proviso that the data protection legislation does not apply to anonymous/duly anonymised data
- Guaranteeing that all health and personal data will:
  - Be duly anonymised before been uploaded on MHMD Infostructure
  - Be processed, should the use of partial anonymisation techniques be indicated for the intended use of data, on the ground of a Dynamic Consent provided by the data subjects.
- Exploring different open data implementation approaches
- Evaluating, to the extent permitted by national and European regulations, solutions providing some concrete acknowledgment of data value

MHMD Kick-off Meeting – Rome, 7-8 November, 2016

Two layers of data flow

- **A semi-automated data profiling and cleaning engine that:**
  - Ensures and assesses data quality
  - Guarantees the most appropriate de-identification or encryption mechanism, according to each type of data or modality

- **A privacy preserving and security layer that combines:**
  - A privacy preserving data publishing engine (providing anonymisation tools)
  - A privacy preserving complex data flow execution engine (i.e., differential privacy, SMPC, homomorphic encryption)

The joint goal is to allow:

- Classifying medical data and correspondent security and privacy provisions in each category
- Assessing relevance, sensitivity, risk for the individual and practical value
- Selecting the most appropriate security and privacy preserving technique in each case

Key MHMD User Entitlements

- **Aggregate personal data from disparate sources:**
  Social media accounts, clinical data repositories, personal drives, wearable devices, etc., in a single, user-owned account (PDA).
- **Assign data access rights**
  Within an efficient workflow, based on stakeholders' permissions and addressing simple questions:
  - Type of data requested
  - Intended use
  - Data that will be retained
  - Data that will be shared with 3rd parties and intended use
  - Implementation of the Right to be forgotten.
- **Stay informed of, and enquiry on, relevant data transactions after access has been granted**
- **Be able to revoke data access rights, or extend them**
- **Be able to receive requests from stakeholders for data access permissions**.
  Requests may also include incentives offered by stakeholders in exchange for data
- **Define post-mortem usage or donation of personal data**

Blockchain: no recourse to Trusted Third Party

- **Applying the blockchain approach to health data guarantees secure access from anywhere on any device**
- **The Blockchain ledger is the secure, non-editable record where:**
  - All transactions are confirmed by the network as entries forming blocks of transactions
  - The whole network monitors the legitimacy of each transaction, guaranteeing a distributed control system
- **Each stakeholder can enact anonymous transactions through the ledger:**
  - Employing public key encryption for identifying owners in the ledger, recording one half of the public key pair
  - Only the person or istitution holding the corresponding private key can decide what happens next to their data
- **Each stakeholder is equipped with a 'wallet' containing:**
  - An encrypted identifier
  - His/her Dynamic Consent
  - His/her data access policy file

Dynamic Consent

- **Dynamic Consent allows to extend traditional consents, combining them into a user workflow in which patients may or may not allow access to their data based on a range of key parameters:**
  - What will data be used for
  - What will be done with the data
  - What data will be retained
  - What data will be shared with 3rd parties and for what purpose
  - How will the right to be forgotten be implemented
  - Define post-mortem usage or donation of personal data.

Dynamic Consent Functionalities

- **Wrapped Information (WI) making the consent policies cryptographically bound:**
  Packages of information are self-enforceable with regard to consensual access, implicit data transformation, time-triggered functionalities (consent expiry/self-destruct, re-consent request triggers, etc.)

- **Dynamic and Enforceable Policies (DEP)**
  By which information access and management are controlled by a hierarchy of semantically defined policies, with managed control of precedence and conflict resolution, enabling the initial definition of smart contracts.

- **Compliance Oversight and Audit (COA)**
  An automated oversight checking that policies are electronically enforced and assuring through the blockchain that transactions are integral.

Challenging MHMD Privacy & Security

Checking the ability of avoiding privacy & security breaches by having recourse to:

- **Privacy preserving data processing API**
  Creating the required abstraction between privacy and security preservation & data analytics being applied to the data
- **Penetration testing and vulnerability assessment**
  on MHMD Federated Infostructure
- **Watermarking & fingerprinting data sets**
  To identify data leaks and attribute the source of the leak
- **Active self-hacking**
- **Making use of synthetic but realistic datasets attributed to virtual patients**

Contacts:

emf@lynkeus.com

Website:

http://www.myhealthmydata.eu/