Mirko De Maldè – Lynkeus (Project Coordinator)
Nicola Bergonzi - Ospedale Pediatrico Bambino Gesù

eHealth Week 2017 – Malta - May 11th
EC Commissioner Vytenis Andriukaitis has stressed the importance of “patient empowerment and patient-centred care”

HIMSS’s CEO Stephen Lieber talked about “Health data usage and sharing issues”
The big data revolution in healthcare

• With its 150 exabytes of stored data worldwide per year, Healthcare is a bright example of “data explosion” phenomenon.
mHealth mIoT

• Within 2020 – 40% of IoT technologies will be healthcare-related
• This will be the basis of the “Internet of Medical Thing” (IoMT), or medical Internet of Thing (mIoT)
Key figures

5.6 billion dollars/year spent in the US to protect healthcare data

27.8/67.7 millions of medical records breached since 2009

The problem in figures

Black market prices 10x higher for medical records in respect to other industries

More than 193 million personal records open to fraud and identity theft in 2015

Mirko De Maldè
A new civil right to personal health data ownership

“[We shall overcome] the old, paternalistic model in medicine in which the data is generated and owned by doctors and hospitals”...

“Patients should be the owners of their own medical data. It’s an entitlement and civil right that should be recognized”.

The New York Times

The Opinion Pages | OP-ED CONTRIBUTORS

The Health Data Conundrum

By KATHRYN HAUN and ERIC J. TOPOL  JAN. 2, 2017
• This will also apply to patient, who is “the single most unused person in health care”.
• Thanks to mIoT, smartphone, and Personal Data Account, a new era of healthcare democratisation will start.
The General Data Protection Regulation

• **Data access**: “A data subject should have the right of access to personal data which have been collected concerning him or her”

• **Right to data portability**: receive personal data in a structured, commonly used, machine-readable and interoperable format”
The GDPR and the Patients’ consent

• Freely given, informed, and specific
• Easily readable, and in plain language
• Data Controller will have to demonstrate consent
MHMD goals

• CITIZENS’ EMPOWERMENT
  (PDA, dynamic consent, smart contracts)

• DATA PRIVACY AND SECURITY
  (blockchain, de-identification, encryption)

• DATA VALUE ENHANCEMENT
  (blockchain, big data analytics for pseudo/anonymised data)
MyHealthMyData – Basic Facts

- Grant agreement no: 732907 - EC Budget 3.455.190,00
- Duration: 1st November 2016 – 31 October 2019
- Consortium:
  - 5 SMEs:
    Lynkeus (Italy) [Coordinator], Digi.Me (UK), HW Communications (UK), Gnúbila (France), SBA Research (Austria)
  - 4 Clinical partners:
    Ospedale Pediatrico Bambino Gesù (Italy), Deutsches Herzzentrum Berlin (Germany), 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:
    Panetta&Associati (Italy)
  - 1 Industry:
    SIEMENS Healthcare (Germany)
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 key innovations (1)

**DYNAMIC CONSENT**
A dynamic consent interface will allow users to grant, deny or revoke consent to data access for different uses according to their preferences.

**PERSONAL DATA ACCOUNTS**
Personal storage clouds will enable individuals to access their data from any technological device through the blockchain and employ them for personal use.
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.
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 on the basic of user-defined consent**

- **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**
MHMD key innovations (2)

**BLOCKCHAIN**
The data platform will rely on the blockchain system, a digital ledger where data is trimmed in hash-based language code and data transactions are visible to the entire network of stakeholders, minimizing any possibility of fraudulent usage.

**SMART CONTRACTS**
Self-executing contractual states, based on the formalisation of contractual relations in digital form, will automate the execution of peer-to-peer transactions under user-defined conditions.
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 institution 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.
MHMD key innovations (3)

MULTILEVEL DE-IDENTIFICATION AND ENCRYPTION TECHNOLOGIES
Multi-party secure computation and homomorphic encryption techniques will be employed for encoding and de-associating sensible data from the owners’ identity, still allowing the application of advanced analytics on pseudonymised or anonymised data.

BIG DATA ANALYTICS
The project will explore the feasibility of applications leveraging the value of large clinical datasets, particularly advanced data analytics, medical annotation retrieval engines and patient-specific models for physiological prediction.
A long story of EU-funded research

From FP6...

Sim-e-Child

MD-PAEDIGREE

Passing through FP7...

CARDIOPROOF

To H2020
MHMD and the strategic role of the 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 being uploaded on MHMD Infostucture
  - 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 regulation, solutions providing some concrete acknowledgment of data value
OPBG’s role in MHMD

• OPBG represents the largest clinical center involved in the study.
• OPBG will oversee the implementation of the tools for individuals’ rights implementation for personal data ownership and control.
• OPBG will make sure that the developed tools are in line with the standards ethical requirements and relevant regulations
• OPBG will also test and validate the final platform, assessing its usability in data management, exchange, research activities and patient relationship.
Contacts:
info@myhealthmydata.eu

Website:
http://www.myhealthmydata.eu/