03: CASE STUDIES
From actual to future services: promises and value of the MyData model

Helsinki, August 31 2017
Imagine a world where...
MyHealthMyData (MHMD) is an H2020 EU-funded research project developing an European platform for sharing and exchanging PERSONAL HEALTH DATA among clinical institutions, individuals, research centres and industry for medical care, research and business purposes.
MHMD at a glance

- **Duration** November 1, 2016 – October 31, 2019
- **Funding** € 3,456,190
- **Consortium**

  5 SMEs
  
  4 Clinical partners
  
  4 Research centres and Academia
  
  1 Legal consultancy
  
  1 Industry
MHMD mission

CITIZENS’ EMPOWERMENT
Grant individuals ownership and control of their personal health data

DATA PRIVACY AND SECURITY
Ensure the strongest privacy protection and health data security

DATA VALUE ENHANCEMENT
Leverage the value of large biomedical datasets for medical care, research and business
How will MHMD do that?

"Gears" (CC BY-SA 2.0) by AJC1

"Gears" (CC BY-ND 2.0) by Charlie Gross Photography
(1) BLOCKCHAIN
Providing certified information

A secure, non-editable digital ledger 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

Applying the blockchain approach to health data guarantees secure access from anywhere on any device
(2) SMART CONTRACTS

Encoding regulation and implementing it at the speed of light

Self-executing contractual states, based on the formalisation of contractual relations in digital form, that automate the execution of peer-to-peer transactions under user-defined conditions.

Regulate data transactions on the blockchain
- in compliance with the incoming GDPR regulation
- allowing to set use conditions and consent options for different stakeholders and purposes.
(3) PERSONAL DATA ACCOUNTS
Individual data ownership and control

Personal storage clouds enabling individuals to access their data from any technological device through the blockchain and employ them for personal use.

Aggregate personal data from disparate sources (social media accounts, clinical data repositories, personal drives, wearable devices, etc.), in a single, user-owned account.
(4) MULTILEVEL DE-IDENTIFICATION AND ENCRYPTION TECHNOLOGIES

i.e. Multi-party secure computation, homomorphic encryption

- Profile and classify sensitive data
- Identify most suitable de-identification and encryption techniques

Encode and de-associate sensible data from the owners’ identity, still allowing the application of advanced analytics
(5) PENETRATION AND RE-IDENTIFICATION CHALLENGE

Checking the ability of avoiding privacy & security breaches

- Active self-hacking (1) and public hacking (2) simulations

- Testing external re-identification possibilities on
  1) synthetic datasets attributed to virtual patients
  2) patients consenting to being used as test-basis

"Hacked..." (CC BY-NC-ND 2.0) by Christine Krizsa
(6) DATA CATALOGUE

Finding specific data of interest

- Organise datasets so to provide a database overview from outside
- Allow researchers to find what kind of data most suits their needs

http://maxpixel.freegreatpicture.com/photo-29398
The project will explore the feasibility of

1. advanced data analytics for similarity search, data exploration and patient stratification (*DeepReasoner*)
2. personalized physiological models for clinical decision support
3. machine learning algorithms for knowledge discovery
4. data value estimation models

on **DE-IDENTIFIED AND ENCRYPTED DATA**
Our vision...