



**MY HEALTH
MY DATA**

Edwin Morley-Fletcher, Lynkeus

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

- **GDPR**

The coming into effect of the General Data Protection Regulation (GDPR) provides a unique opportunity for precisely defining in what cases will MHMD deal with pseudonymised data (requiring consent) and in which cases will it be possible to have recourse to anonymised data, and what will it mean to adopt a “qualified anonymisation” approach.

- **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, Personal Data Accounts, and Smart Contracts**

MHMD is going to introduce a distributed, peer-to-peer architecture, based on Blockchain, Personal Data Accounts, and Smart Contracts.

- **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, aiming to establish the first open biomedical information network centred on the connection between organisations and the individual.

Background: A long term anticipatory strategy

LYNKEUS . Munich 2003

Erich Reinhardt (CEO, Healthcare Sector of Siemens)

PRIDDE (Paediatric Radiological Image Database-guided Diagnosis Excellence)



Health-e-Child (2006-2010)



Biomedical knowledge repository and communication conduit for the future



CaseReasoner



(2010-2012)



Model-driven Prediction and Simulation in Paediatric Cardiology



CARDIOPROOF (2013-2016)



Proof of Concept of Model-based Cardiovascular Prediction



AVICENNA (2013-2015)



A Strategy for In Silico Clinical Trials



SILICARDIO (2017 ??)

in-SILico trials for CARDIOvascular devices



MD-PAEDIGREE (2013-2017)



Model-Driven European Paediatric Digital Repository

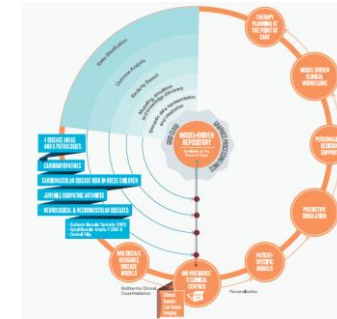


**MY HEALTH
MY DATA**

(2016-2019)



Privacy, Security, Blockchain



Background: An Innovation Community



ICT08 (Lyon, Health-e-Child Best Exhibition Award) - ICT10 (Brussels) - ICT13 (MD-Paedigree Best Exhibition Award; Networking Session on *Big Data in Healthcare*) - ICT15 (Networking Session on *Enhanced Consent: a vision for Patient Data Protection and Data Management*)



Virtual Physiological Human Conferences (Trondheim, 2014 – Amsterdam, 2016)



CHOC Children's Heart Institute, Anthony C. Chang: *Pediatrics 2040: Trends and Innovations for the Next 25 Years* (Anaheim 2013) - PEDIATRIC INNOVATION LEADERSHIP FORUM (Laguna Niguel 2014; Chicago 2015)

international Society for Pediatric Innovation (iSPI)

OPBG in the Executive Committee



Health Data Interest Group (co-chaired by A. Chang, Y. Ioannidis, E. Morley-Fletcher; Meetings Paris 2015, Tokyo and Denver 2016; Barcelona 2017)

BoF on Blockchain (Barcelona 2017)



Big Data Value Public-Private Partnership (Valencia 2016)



HDI Day on Blockchain (Paris 2016)



Healthcare: New Kids on the Blockchain



Spotlight on Blockchain: a new generation of digital services
Joint Event between STOA (EP) & DG CONNECT (EC), Brussels 2017



A highly competitive context



Artificial intelligence: Can Watson save IBM? (The Financial Times, Jan. 5, 2016)

Watson Health → \$1bn spent to buy **Merge Healthcare**

Watson Imaging Clinical Review (initially aiming at patients suffering from Aortic Stenosis (AS), searching through images to reduce pattern variation, and applying cognitive text analytics)

The President of Lombardy would be willing to transfer the Region's EHRs as part of the deal for having Watson Health positioning itself within the planned **Human Technopole** to be created at Rho, in the former Milan Expo area



DeepMind Health signed in 2016 a data-sharing agreement with England NHS, allowing it to have access to “de-personalised patient data” from some hospitals in London. This is based on an “implied consent” assumption, and patients can opt out of the data-sharing system by contacting the data protection officer. In response to criticism regarding how to distinguish between uses of data for care and for research, DeepMind has now planned a digital ledger based on **blockchain** to let hospitals, the NHS, and eventually patients, track personal data. This **Verifiable Data Audit** will automatically record every interaction, making visible changes to, or access of, the patient data.

DeepMind is also experimenting a **Streams** app, making use of mobile technology to send immediate alerts to clinicians when a patient is at risk of developing acute kidney injury (AKI). “To maximise the clinical and social benefits of advanced health technology, solutions can’t be developed in labs disconnected from the hospital frontlines”.

Alphabet’s healthcare division, Verily Life Sciences, is partnering with Novartis and the European Investment Fund in Medicxi Growth 1 for cherry-picking biotech needing cash for phase III clinical trials of experimental drugs.



Microsoft Healthcare NEXt (New Experiences and Technologies), in partnership with University of Pittsburgh Medical Center, has launched an initiative to integrate robots, voice recognition, and cognitive services into new collaborative healthcare applications, with the aim of helping doctors to reduce entry tasks, triage patients more efficiently and improve outpatient care.

A critically challenged security issue



- The latest (and unprecedented in scale) ransomware cryptoworm attack started on 12 May 2017
- WannaCry targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency
- According to Europol, it has been infecting more than 200,000 computers in over 150 countries
- Parts of Britain's NHS (among which our MHMD partner St. Bart's London), Spain's Telefonica, FedEx, and Deutsche Bahn, were all hit, along with many other countries and companies worldwide
- Up to 70,000 NHS devices – including computers, MRI scanners, blood-storage refrigerators and theatre equipment – may have been affected.

A participatory environment



- One in twenty Google searches is reportedly health related
- 90% of patients search for info on line
- Only 34% of patients just trust their physician

RDA user scenarios/focus areas

- **Data access and protection**
 - sharing best practice on pseudonymisation and anonymization (or “qualified anonymisation”)
 - developing models for consent that protect patients while enabling research
 - providing a forum for discussing, explaining and responding to data protection regulation
 - secure opening up of data to facilitate research
- **Data-based healthcare for personalised medicine**
 - disease signatures identification
 - stratification of patient groups
 - patient-specific simulation and prediction
- **Data literacy in Health care**
 - providing materials for education of healthcare professionals on use and misuse of data
- **Patient data repositories/patient-centric data gathering systems**
- **In-silico drug development and clinical trials**
 - representing interests of the data-based healthcare community to policy makers
 - identifying and discussing related challenges, interdisciplinary research needs and potential roadmaps.
- **Blockchain applications to health data**

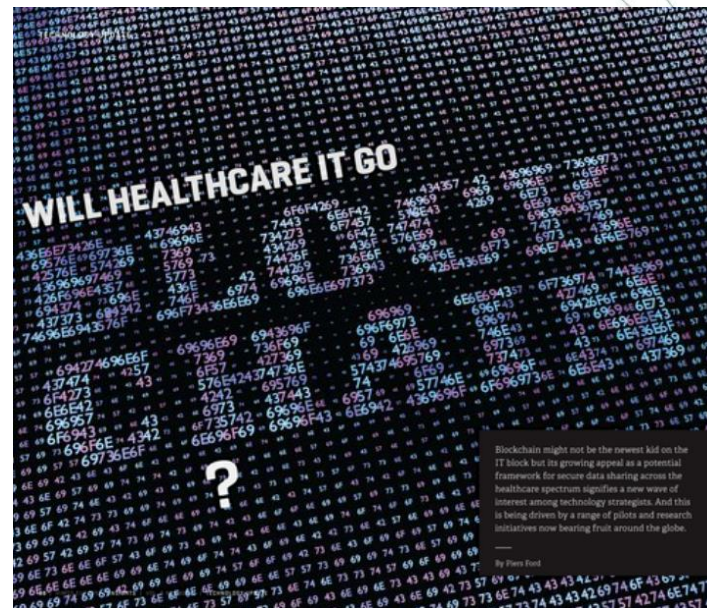
Looking forward to an RDA WG focusing on Blockchain in Health

- The RDA HD-IG is sponsoring the idea of establishing a WG focusing on Blockchain in health data with the aim of debating in depth the potential of such a system and whether the blockchain can ensure compliance with advanced data protection requirements (such as those defined by the EU GDPR), yet making it happen seamlessly and efficiently, at scale.
- Due to its scope, the next (second) preliminary BoF meeting ideally fosters relations to a number of RDA WGs and IGs that may be able to contribute with their results to, or benefit from, the proposed future WG's activities.

Blockchain Hype ?



The Economist (2015), “The promise of the blockchain: The trust machine”, October 31st



himss Europe - Health IT Central – May 15th, 2017

Blockchain Hype ? The Economist

- The Economist went so far as to state that:
 - at first sight, “the notion of shared public ledgers may not sound revolutionary or sexy. Neither did double-entry book-keeping or joint-stock companies. Yet, like them, the blockchain is an apparently mundane process that has the potential to transform how people and businesses cooperate”.
 - “A realisation that systems without centralised record-keeping can be just as trustworthy as those that have them may bring radical change. [...] A world with record-keeping mathematically immune to manipulation would have many benefits.”

Blockchain Hype ? IBM

- “Blockchain promises to put privacy and control of data back in the hands of citizens. Trust and integrity will be established without reliance on third-party intermediaries. IBM believes blockchain is an extraordinarily important phenomenon with the potential to transform industries and upend business models”.
- “In healthcare, new research is seeking to apply blockchain’s distributed ledger and decentralized database solutions to the critical issues of interoperability, security, record universality, and more. Intriguing uses in other industries are being extended to healthcare, such as extending blockchain’s smart contracts to provider network management or connecting myriad medical devices through common, blockchain-enabled systems of information relationships. While technical consensus on a distributed ledger for healthcare has yet to emerge, with debate ongoing regarding scalability, security, and regulatory compliance, blockchain technology and encryption *will* drive innovation in healthcare services and administration”







IBM Global Business Services Public Sector Team (2016), *Use of Blockchain in Health IT and Health-related Research*, proposal submitted on August 8, 2016, to the Ideation Challenge launched by the Office of the National Coordinator for Health Information Technology in the USA.

Blockchain Hype ? Deloitte

- Healthcare pain points and potential blockchain solutions were similarly indicated by IBM as well as by Deloitte, in whose White Paper, however, they appeared to be more conveniently summarised as shown in the next table, taken from:

Deloitte (2016), *Blockchain: Opportunities for Health Care*, White Paper developed in response to the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) ideation challenge on "The Use of Blockchain in Health IT and Health-Related Research".

Blockchain Value Propositions for Healthcare

	Health Information Exchange (HIE) Pain Points	Blockchain Opportunities
	Establishing a Trust Network depends on the HIE as an intermediary to establish point-to-point sharing and “book-keeping” of what data was exchanged.	Disintermediation of Trust likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.
	Cost Per Transaction , given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.	Reduced Transaction Costs due to disintermediation, as well as near-real time processing, would make the system more efficient.
	Master Patient Index (MPI) challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.	Distributed framework for patient digital identities , which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.
	Varying Data Standards reduce interoperability because records are not compatible between systems.	Shared data enables near real-time updates across the network to all parties.
	Limited Access to Population Health Data , as HIE is one of the few sources of integrated records.	Distributed, secure access to patient longitudinal health data across the distributed ledger.
	Inconsistent Rules and Permissions inhibit the right health organization from accessing the right patient data at the right time.	Smart Contracts create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.

Who is Ronald Coase ?



- Ronald Coase (1910-2013): Nobel Laureate for Economics on 1991, more than 50 years after his disruptive *The Nature of the Firm* (1937), and 30 years after *The Problem of Social Costs* (1960).
 - Why clusters of individuals operate under the direction of hierarchies and not purely under the guidance of market prices? He famously answered that using the price system is costly (in terms of "transaction costs").
 - According to the Coase Theorem, in the absence of transaction costs, the allocation of resources is independent of the distribution of property rights.
- It is now possible to reverse Ronald Coase's Transaction Costs.
- What Internet did to transaction costs regarding information, blockchain can do regarding trust.

Assumptions and Expectations

- Public and private initiatives, both in Europe and in the US, are currently addressing the potential of applying the blockchain approach to health data.
- This is related to great general expectations (“what Internet did to transaction costs regarding information, blockchain can do regarding trust”) and to the assumption that what is needed for health data is a Distributed Empowerment system, providing secure access from anywhere on any device.
- There is the need to develop new mechanisms of trust and of direct, value-based relationships between people, hospitals, research centres, and businesses, leading to an open biomedical information network centred on the connection between organisations and the individual.



Blockchain Ledger

- A Distributed Empowerment system having the Blockchain ledger as secure, non-editable record, where all transactions are confirmed by the network as entries forming blocks of transactions, and the whole network monitors the legitimacy of each transaction, guaranteeing distributed control.



Smart Contracts

- The blockchain is expected to be based on portfolios of Smart Contracts.
- Smart Contracts are the executable pieces of code, stored on the blockchain for future execution.
- These bind people and transactions to specific actions and outcomes and 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 self-enacting).

MHMD Goals

1. Be able to **Classify** sensitive data, based on their informational and economic value
2. Precisely **define the boundaries** of pseudonymised and anonymised data (including “qualified anonymisation”)
3. Assess the most suitable and robust **de-identification** and **encryption** technologies needed to secure different types of information
4. Allow having **advanced analytics** running on anonymised or pseudonymised data
5. Evaluate the overall security of MHMD multi-modular architecture by testing it through dedicated **self-hacking** simulations and **public hacking challenges**
6. Analyse **users’ behavioural patterns** alongside **ethical and cultural orientations**, to identify hidden dynamics in the interactions between humans and complex information services
7. Improve the design of **data-driven platforms**
8. 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

Further Assumptions and Question Marks

- **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 de-identified 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

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 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
- **All stakeholders' options are dealt with through Smart Contracts encoding**



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**, and possibly also testing external re-identification possibilities on patients consenting to being used as test-basis

DOI System: Handle.net

- The **Handle System** is a comprehensive system chosen **for assigning, managing, and resolving persistent identifiers for digital objects** and other resources on the Internet
- The protocols enable a distributed computer system to store identifiers of digital resources and resolve those identifiers into the information necessary to locate and access the resources
- The **handle.net 8.1 software** include :
 - a RESTful JSON-based HTTP API
 - a browser-based admin client
 - an extension framework allowing Java Servlet apps
 - authentication using handle identities without specific indexes
 - multi-primary replication
 - Security improvements

Disruptive Models of Healthcare for Europe

according to the May 2017 Friends of Europe Discussion Paper

- “If healthcare could be transformed by the kind of ‘disruptive innovation’ that has revolutionised other sectors of the economy, the potential efficiency and cost gains would be huge”.
- “Healthcare has not achieved the types of productivity increases that most other industries have experienced. In fact, healthcare ranks near the bottom in terms of productivity improvements since 1990”.
- “In healthcare we lag at least ten years behind virtually every other area in the implementation of IT solutions”.
- “Implementation is inconsistent due to the fragmented nature of the system and because of incentives that support the status quo”.
- “Transaction-based systems don’t provide citizens with an incentive to promote their own health, or medical professionals to keep patients well”.
- “The importance of building trust into the system so that people feel comfortable sharing their health data”.
- Eventually, what is needed is “a radical shift in the fundamental approach to digital health: establishing an innovation ecosystem with a central platform at its heart”.

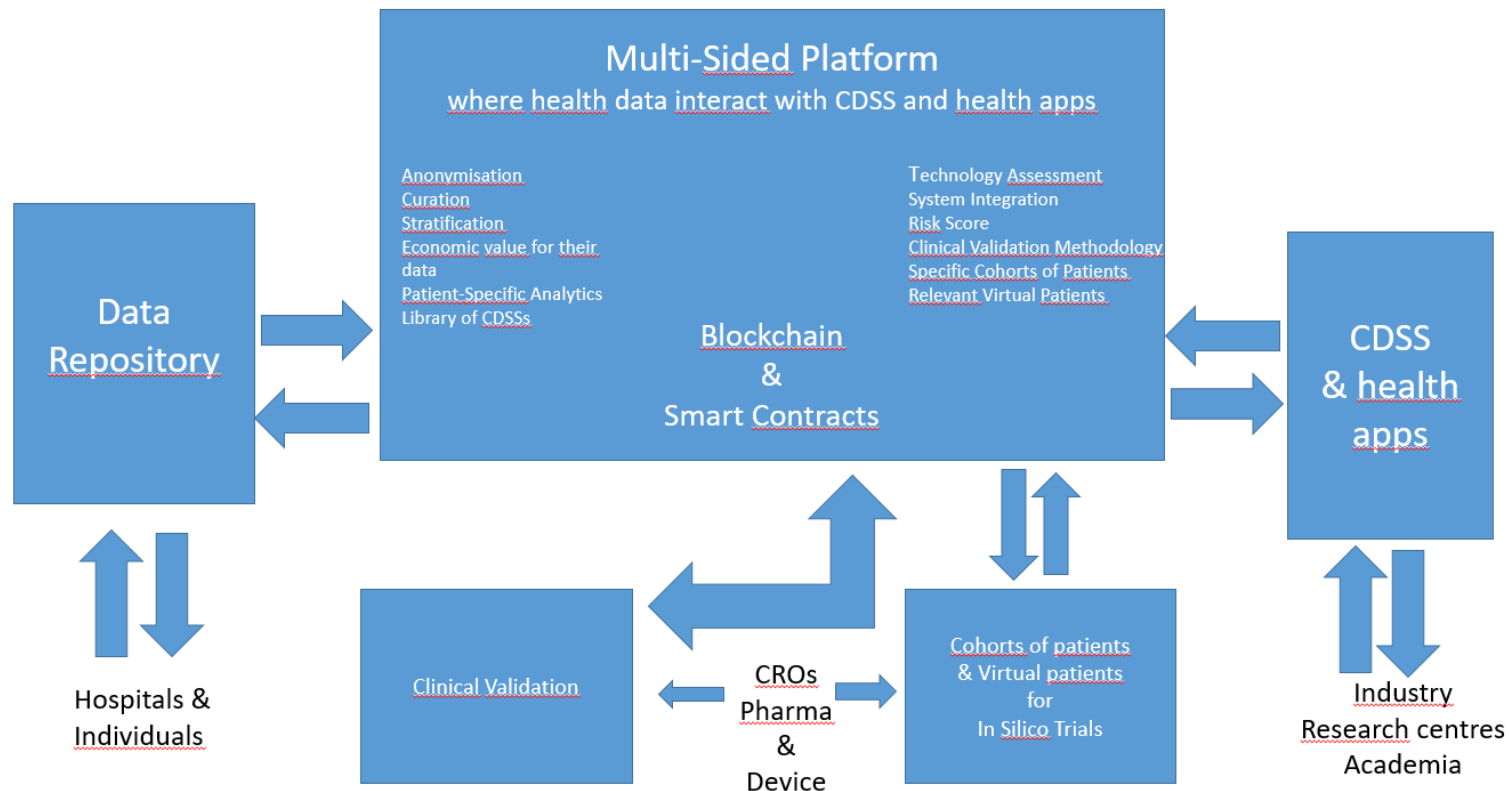
A Multi-Sided Platform for healthcare



Jean Tirole, Nobel Laureate 2014 for Economics

- Multi-sided platforms (MSPs) generating strong positive network effects appear to be the organisation model showing the **greatest capacity to scale**, based on the implicit support derived by each of the sides served by the platform.
- Professional service firms are on this basis:
 - Moving away from centralized and vertically integrated models (in which all client services are provided by their employees)
 - Moving towards the decentralized MSP model, in which they enable independent contractors to deal directly with clients, even though often maintaining a significant degree of control over the contractual terms between clients and professionals.
 - The Blockchain and its Smart Contracts complements can strongly contribute to the effectiveness of MSPs

Where health data can interact with CDSS and health Apps with Smart Contracts





Contacts:
emf@lynkeus.com

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