MY HEALTH MY DATA

Edwin Morley-Fletcher, Lynkeus

RDA EU Data Innovation Forum, Brussels, 30 January 2018

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.
- A distributed system where:
  - Instead of “googling” for everything, we can perform the equivalent action by verifying that any digital ownership is certified by a blockchain.
  - Information access is not enough anymore. Truth access was a missing piece of the information revolution, which the blockchain fixes.
  - The old question “Is it in the database?” is being replaced by “Is it on the blockchain?”

Smart Contracts

- A blockchain can 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).
- Smart Contracts are the new form of legal contracts, which both formalizes and enforces their terms, without requiring a third-party acting as trusted authority.

A Long Historical Journey

- From having recourse to a Fair Independent Third Party (Common Law)
- To the Law Codification process (From Justinan to Napoleon, and beyond)
- To having again “the contract among the parties is law”
- In a self-enacting digital codification, which allows for the maximum personalisation

MyHealthMyData (MHMD)

- MyHealthMyData aims to guarantee **privacy** and **security** of healthcare data by:
  - introducing a distributed architecture based on **Blockchain** and **Smart Contracts**,
  - serving both clinical institutions as well as individual data subjects, who will be making use of **Personal Data Accounts**.
- MHMD develops a comprehensive methodology to guide the implementation of data and identity protection systems, specifically defining approaches and tools to classify sensitive data based on their **medical** as well as **predictive**, and potentially **economic**, value, aiming to:
  - assess the most suitable and robust de-identification and **encryption** technologies needed to secure different types of information,
  - allow **advanced analytics** applied on such data,
  - evaluate the overall reliability of a generic multi modular architecture.
- MHMD also analyses users' behavioural patterns alongside ethical and cultural orientations, to identify dynamics related to events like **WannaCry**, the coming into force of the **GDPR**, and the **interactions of hospitals and individuals** within a system like MHMD.
- MHMD will check the ability of avoiding privacy & security breaches by having recourse to:
  - active **self-hacking**,
  - public challenges of **penetration testing** and **vulnerability assessment**,
  - testing **external re-identification possibilities** on patients consenting to being used as test-basis
- MHMD ultimately aims to:
  - improve the design of data-driven biomedical platforms,
  - foster the development of an information multisided-platform, in which a growing number of clinical institutions may find secure GDPR compliant ways of sharing data and leverage their value, as well as individuals, becoming able to easily access their personal data and control what use is made of them.

MHMD Partners

- **5 SMEs:**
  Lynkeus (Italy) [Coordinator], Digi.Me (UK), HWC (UK), Gnúbila (France), SBA Research (Austria)

- **4 Clinical partners:**
  Charité Berlin (Germany), Ospedale Pediatrico Bambino Gesù (Italy), St. Bart’s-Queen Mary University London (UK), Great Ormond Street Hospital-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:**
  P&A (Italy)

- **1 Industry:**
  SIEMENS Healthcare (Germany)

- Now additionally introducing also an **Icelandic** extension, composed of both Personal Data Accounts and multimodal datasets from the National Hospital in Reykjavik

MHMD is surrounded by big expectations

Encounters and talks on MHMD

1. Health Care Data Institute – Paris, 17 November, 2016
2. BDVA, Barcelona, 1st December, 2016
3. Big Data PPP INFO DAY 2017 - Luxembourg 17-18 January 2017
4. EDBTICDT 2017 – Euro Pro Workshop – Venice – 21 March 2017
5. ITU workshop on "Security Aspects of Blockchain" - Geneva, 21 March 2017
6. BoF on Blockchain in Health within the HD-IG at RDA 9, Barcelona, 7 April, 2017
7. The Blockchain-centred approach of MyHealthMyData, eHealth Week, Malta, 11 May, 2017
8. 1st Joint EU Blockchain Conference, EU Commission - EU Parliament – Brussels, 11 May, 2017
9. RDA meets Nordic researchers - Göteborg, 14 June 2017
10. CTIE and Infrachain – Luxembourg, 16 June 2017
11. EHRA EUROPACE-CARDIOSTIM Congress - Vienna 19 June 2017
12. Meeting with F. Modafferi, Director of the Department “Public Liberty Rights and Health” within the Italian Data Protection Authority (www.gpdp.it), organised by P&A, Rome, 27 July, 2017
13. Department of Health and Dattacalabs – Reykjavik, 23 August 2017
14. MyData 2017, Tallin and Helsinky, 30-31 August, 2017
15. BoF on Blockchain in Health within the HD-IG at RDA 10, Montreal, 21 September, 2017
16. Info request on MHMD by Malte Bayer-Katzenberger, DG Connect, for speaking about our project at the Impact of Big Data Analytics on Healthcare conference, Elixir Luxembourg, 4-5 October, 2017
17. Stakeholder Workshop on GDPR Implementation and Health Data, Brussels, 23 October, 2017
18. Panel “Towards Privacy-Preserving Big Data” at the BDVA Forum, Versailles, 22 November 2017
19. In-Silico medicine in Europe, at the 12th Forum on Risk Management in Health, Florence, 29 November 2017
20. Encryption, Anonymisation, and Artificial Intelligence, at the EMA Workshop on Data Anonymisation – a Key Enabler for Clinical Data Sharing, London, 30 November-1 December 2017
21. Panel ”Short Introduction of blockchain and its possible role in IoT data trading”, at the RDA EU Data Innovation Forum, Brussels, 30 January 2018.

RDA Health Data IG: user scenarios/focus areas

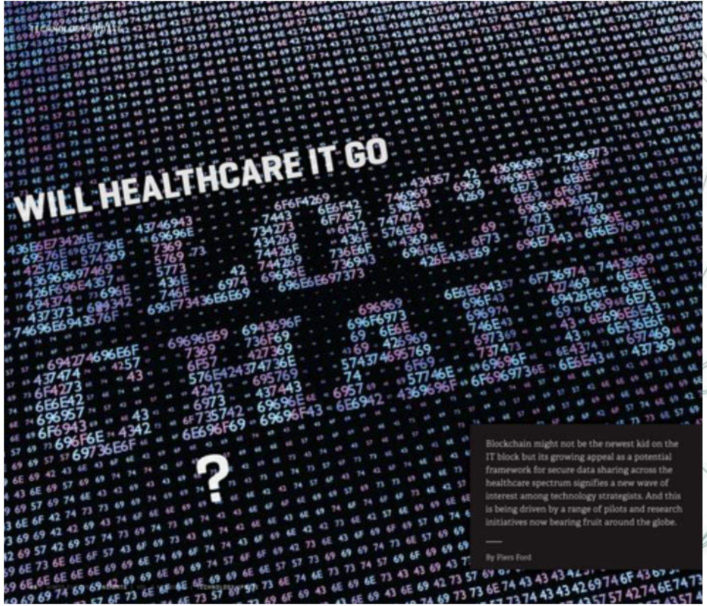
- Data access and protection
  - sharing best practice on pseudonymisation and anonymization (or “qualified anonymisation”)
  - developing models for consent that protect patients while enabling research
  - providing a forum for discussing, explaining and responding to data protection regulation
  - 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 Blockchain Applications in Health WG

- The RDA HD-IG has organised two BoFs sponsoring the idea of establishing a WG focusing on Blockchain in health data with the aims of:
  - The aim of establishing a dedicated WG is:
  - to analyse and compare usages of the blockchain in healthcare, implementations of blockchain architectures, associated legal and socio-economic impacts and perspectives
  - to assess the potential of blockchain-based self-enacting smart contracts in handling consent and data permission systems minimising transaction costs
  - to assess whether and how the blockchain can ensure compliance with advanced data protection requirements (such as those defined by the EU General Data Protection Regulation – GDPR), yet making it happen seamlessly and efficiently, at scale.
- Work Plan:
  - The final deliverable of the WG will be a set of Guidelines for establishing a scalable blockchain-based data sharing system in healthcare. These guidelines will include a state-of-the-art report and a report on regulatory and legal issues, focussing on blockchain applications in health.
  - At 6 months interval, 3 reports will be presented at each RDA Plenary WG's Session, highlighting the performed analysis and activities, following 3 steps: first, the state-of-the-art report (after 6 months) describing the current experiences in blockchain based handling of health data; second, the report on regulatory and legal issues (after 12 months); third, the comprehensive Guidelines on Blockchain applications in Health (after 18 months), inclusive also of an example of basic coding for a health-data blockchain architecture.
  - From the start of the WG, its members will be asked to join one or more of the proposed sub-groups
- Hopefully, the first meeting will be in Berlin, 21st-23rd March 2018, @ RDA 11.

Blockchain Hype ?

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



WILL HEALTHCARE IT GO

?

Blockchain might not be the newest kid on the IT block but its growing appeal as a potential framework for secure data sharing across the healthcare spectrum signifies a new wave of interest among technology strategists. And this is being driven by a range of pilots and research initiatives now bearing fruit around the globe.

By Piers Ford

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”

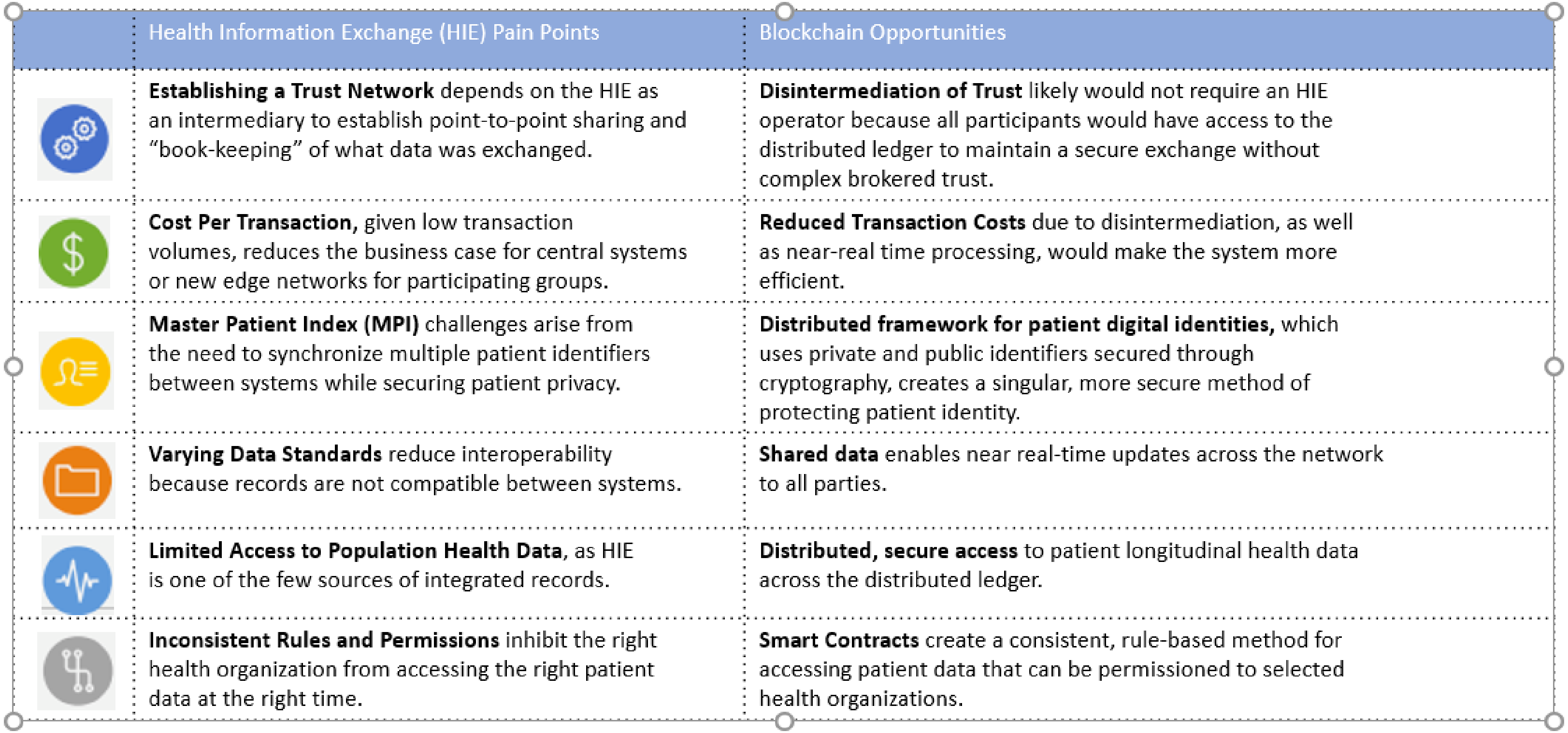
IBM Global Business Services Public Sector Team (2016), *Use of Blockchain in Health IT and Health-related Research*, proposal submitted on August 8, 2016, to the Ideation Challenge launched by the Office of the National Coordinator for Health Information Technology in the USA.

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.

RDA Discussion Paper for January 30th, 2018

Blockchains and Data

request to comment

Peter Wittenburg (Max Planck Computng and Data Facility, peter.wittenburg@mpcdf.mpg.de),
Wolfgang Kuchinke (University Hospital Düsseldorf, Wolfgang.Kuchinke@med.uni-duesseldorf.de)

- BCT is a distributed database approach where each participant maintains a replica of a shared append-only ledger of digitally signed transactions, with two different database components, one including the transaction data and/or smart contracts and another one storing the transaction sequence and pointer structures
- Allowing nodes to create indexes that can be used for searching for information in the blocks based on the metadata would create external instances about the information in the blockchain and could weaken its basic strengths of security and invariability.
- BCT is not made for big data. In most health use cases it makes sense to keep health data separate from the BC to not suffer from expensive acceptance algorithms. But keeping the "real" data outside of BCT would mean that it becomes necessary to do major actions, like data processing and analysis, outside of BCT resulting in several integration problems.
- One could even imagine to exchange the individual results by using blockchain. But it would not solve two problems:
  - High volume data (time series, images) do not fit with the BCT paradigm, i.e. separate mechanisms need to be used to exchange this kind of data.
  - At the end of a trial software will be used to run analytics on the whole data set, i.e. the data set needs to be exported and thus exists outside of BCT control.
- If there are metadata providers offering digital objects for re-use, and their portals are somehow linked so that software agents can find them and that brokers take care of the metadata to include actionable re-use conditions, with these assumptions and a certain degree of harmonisation we can speak about a global crosssector/discipline data market.
- Such a data market would create a huge stimulus for data sharing and meta-analysis of data across different research fields.

The issue of scalability

- Currently, all existing blockchains protocols have the property that every computer in the network must process every transaction
- This property provides extreme degrees of fault tolerance and security
- But at the cost of ensuring that the network’s processing power is effectively bounded by the processing power of a single node.
- New approaches move beyond this limitation, achieving the scale needed to support mainstream adoption, for example through sharding, i.e. horizontal scaling, dividing the system over multiple servers, so that while the overall speed or capacity of a single machine may not be high, each machine handles a subset of the overall workload, providing better efficiency than a single high-speed high-capacity server.
- Expanding the capacity of the deployment only requires adding additional servers as needed, which can be a lower overall cost than high-end hardware for a single machine.
- The trade off is increased complexity in infrastructure and maintenance for the deployment.

Promises and paradoxes of Algorithmic Production of Knowledge

- APK learns from previous situations to provide input and automate complex future decision processes, making it easier to arrive at concrete conclusions based on data and past experiences.
- The first phase is normally ‘unpredictable by design’: it is based on Big Data Analytics, in which large number of algorithms are tested on data in view of discovering meaningful correlations.
- Once relevant correlations are found, new algorithms based on running machine learning techniques can be applied, aiming at learning their causality status.
- Deep learning implies feeding vast quantities of data through non-linear neural networks which classify the data based on hierarchical outputs from each successive layer.
- The complexity of this self-modelling is, as yet, inherently non-self-explicative.
- This can determine a black box effect, rendering automated decision-making altogether inscrutable: no one really knows how the deep learning algorithms get to do what they do.
- In as much as this remains so, the APK is built and operates in ways which appear as incomprehensible and it seems to require paradoxically a ‘trust leap’, in order to let algorithms ultimately make decisions on your behalf.

AI as a threat to the GDPR

- Of course, AI makes it easier and easier to re-identify data subjects.
- “It may be impossible to fulfill the legal aims of the Right to Be Forgotten in AI environments”: *Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten*, Computer Law and Security Review, Elsevier, 2017.

and also as a new tool for anonymisation

- Synthetic Data Vault uses machine learning to automatically generate artificial data on which scientists can test their algorithms and models.
- The algorithm itself is a form of recursive conditional parameter aggregation of real databases, which exploits their hierarchical nature.
- “Once we model an entire database, we can sample and recreate a synthetic version of the data that very much looks like the original database, statistically speaking…If the original database has some missing values and some noise in it, we also embed that noise in the synthetic version… In a way, we are using machine learning to enable machine learning”.

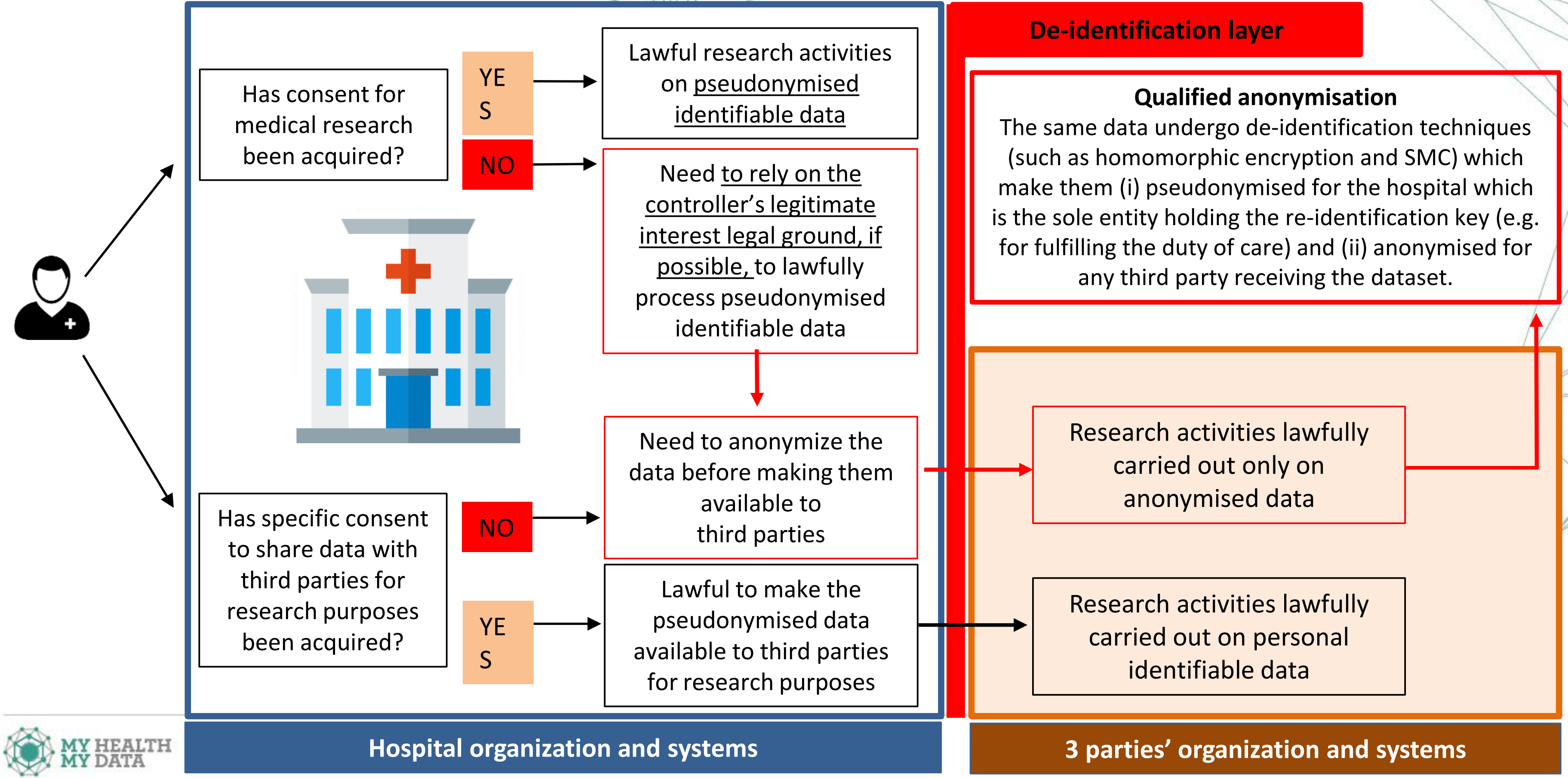
MHMD makes use of Synthetic Data

- MyHealthMyData (MHMD) initially found itself entangled within a sort of “Catch 22” condition with regard to its participating clinical institutions:
  - data could get mobilized only after the Ethics Committees would have given their green light,
  - the same Ethics Committees would not authorize the sharing of routine data until all MHMD solution details were fully clarified.
- As a a pragmatic alternative, Barts has offered to generate synthetic cardiac-oriented data sets (purporting to fictitious individuals) based on aggregate statistics of a population of 100,000 patients.
- These datasets have spurious correlations added to reflect the impact of cardiovascular risk factors on cardiovascular health.
- The datasets contain fake names, addresses, DOB, DOD, episode visits, anthropometry (e.g. weights, heights, BMI, BSA, etc.) and cardiac function parameters, etc.
- Examples of data types/sources targeted for early inclusion include Myocardial Infarction, cath lab data, demographics, CT images and text reports, MRI images and text reports, pacemaker data, echocardiography images and text reports, cardiac surgery data, data from the chest pain clinic and pathology data.
- Not only does this solution allow to get MHMD concretely unrolling, but it also makes it possible to test the major elements of MHMD development, including:
  - Evaluation of how standardized ontologies can be mapped onto such a (typical) data export format
  - Loading and processing of large datasets
  - Algorithm scaling (compute cost as a function of data size)
  - Multi-site compute (e.g. by chunking data and distributing over multiple sites, modelled for example as Virtual Machine instances)
  - Impact of pseudonymisation/obfuscation/aggregation techniques on a range of dimensional statistical measures
  - Allowing the hacking challenges and pen-tests, but, of course, for the reidentification tests, for which real data will be necessary (and are reasonably expected to be available and duly consented).

MHMD makes use of Synthetic Data

- MyHealthMyData (MHMD) initially found itself entangled within a sort of "Catch 22" condition with regard to its participating clinical institutions:
  - data could get mobilized only after the Ethics Committees would have given their green light,
  - the same Ethics Committees would not authorize the sharing of routine data until all MHMD solution details were fully clarified.
- As a a pragmatic alternative, Barts has offered to generate synthetic cardiac-oriented data sets (purporting to fictitious individuals) based on aggregate statistics of a population of 100,000 patients.
- These datasets have spurious correlations added to reflect the impact of cardiovascular risk factors on cardiovascular health.
- The datasets contain fake names, addresses, DOB, DOD, episode visits, anthropometry (e.g. weights, heights, BMI, BSA, etc.) and cardiac function parameters, etc.
- Examples of data types/sources targeted for early inclusion include Myocardial Infarction, cath lab data, demographics, CT images and text reports, MRI images and text reports, pacemaker data, echocardiography images and text reports, cardiac surgery data, data from the chest pain clinic and pathology data.
- Not only does this solution allow to get MHMD concretely unrolling, but it also makes it possible to test the major elements of MHMD development, including:
  - Evaluation of how standardized ontologies can be mapped onto such a (typical) data export format
  - Loading and processing of large datasets
  - Algorithm scaling (compute cost as a function of data size)
  - Multi-site compute (e.g. by chunking data and distributing over multiple sites, modelled for example as Virtual Machine instances)
  - Impact of pseudonymisation/obfuscation/aggregation techniques on a range of dimensional statistical measures
  - Allowing the hacking challenges and pen-tests, but, of course, for the reidentification tests, for which real data will be necessary (and are reasonably expected to be available and duly consented).

Can there be a “Qualified Anonimity” approach?



Has consent for medical research been acquired?

YES

Lawful research activities on pseudonymised identifiable data

NO

Need to rely on the controller’s legitimate interest legal ground, if possible, to lawfully process pseudonymised identifiable data

Need to anonymize the data before making them available to third parties

Has specific consent to share data with third parties for research purposes been acquired?

NO

YES

Lawful to make the pseudonymised data available to third parties for research purposes

De-identification layer

Qualified anonymisation

The same data undergo de-identification techniques (such as homomorphic encryption and SMC) which make them (i) pseudonymised for the hospital which is the sole entity holding the re-identification key (e.g. for fulfilling the duty of care) and (ii) anonymised for any third party receiving the dataset.

Research activities lawfully carried out only on anonymised data

Research activities lawfully carried out on personal identifiable data

Hospital organization and systems

3 parties’ organization and systems

MY HEALTH MY DATA

The proposed paradigm of “Qualified Anonimity”

This concept has been introduced in the EU Horizon2020 **call DS-08-2017**, with deadline for submission 24 August 2017, relating to “**Cybersecurity PPP: Privacy, Data Protection, Digital Identities**”.

There are many cases in which researchers need to keep the capacity of re-tracing and singling-out specific participants into a study in order to assess the progression of diseases and the long-term outcomes of treatments, or simply to keep them informed, also about unexpected findings or life-saving discoveries (as well as in several other situations). Applying standard anonymisation rules do not constitute a viable solution in such cases, because if truly irreversible, it would prevent anyone to re-identify the data subjects, so hindering the objectives of the research and contradicting the basic principles of medicine.

The identification of individuals is not only something that may happen, rather it is something that must happen, **under specific circumstances defining a proper “qualification” granted by the law** (e.g. judges fulfilling their official duties, researchers finding a cure which may eradicate a disease, public authorities exercising their powers, etc.).

Should the response to this need be only left to national laws defining public interest issues?

Will it be possible to navigate between Scylla and Charrybdis?

- The GDPR is not only a fundamental European regulation.
- It also establishes some key ‘civilisation principles’ in the area of data protection.
- Privacy is a common good.
- Also anonymity should be considered as a common good.
- Currently, the are some significant risks:
  1. Problem regarding the **real role remaining for anonymisation**:
     - In absolute, data are always re-identifiable.
     - Research development implies also the need of a market capable of explicating the value of data.
     - Commercial transactions on data are lawful only if they are anonymised.
  2. The ‘specific’ **consent and re-consent** requirements implied by pseudonymisation **may be unpractical** and possibly highly counterproductive.
- One solution is to **reduce the transaction cost** of any such specification.
- These are some of the **reasons why MHMD**:
  – Is **blockchain-based**
  – Transforms the consent and permission choices into friction-free and permanently modifiable self-executable **smart contracts**
  – Makes it possible for any data provider to **fully track** the usages made of their data, while remaining **encrypted**.

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?**

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

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 options
  - His/her Data Access Policy file
- **All stakeholders’ options are dealt with through Smart Contracts encoding**

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".

Personalised medicine and health insurance

- Even leaving aside the data tsunami which is due to reach us from IoT and wearables, personalised medicine will soon imply a disruptive change in the amount of basic things measured in routine medical tests.
  - These are in fact going move from 10-20 measurements, to tens of thousands, if not millions or billions of measurements, based on high-throughput omics technologies, providing the means for performing global, holistic, analyses.
- The expected vision is that of individuals assessing their health at high frequency, having literally thousands of measurements recurrently taken in the course of a year.
- Such more frequent and comprehensive tests to follow someone’s health, rather than the current practice of having individuals go to the doctor every two to three years to get a standard medical test, will drive physicians towards playing a leadership role.
- Where they will need to work with specialists who make recommendations about whether the concerned individuals should be seeing a cardiologist or a nutritionist for their metabolic conditions,
  - based on their DNA or omics profile, according to data-driven, rather than intuitive, health decisions.
- The “patient” will need to become much more involved.
- The role of the physician will increasingly focus on helping coordinate this innovation process, by:
  - making sure that patients are seeing the right people,
  - and getting the right advice,
  - in order to move as much as possible from disease treatment to preventative care.

Has the time come for health coverage plans based on data transparency and integrated care ?

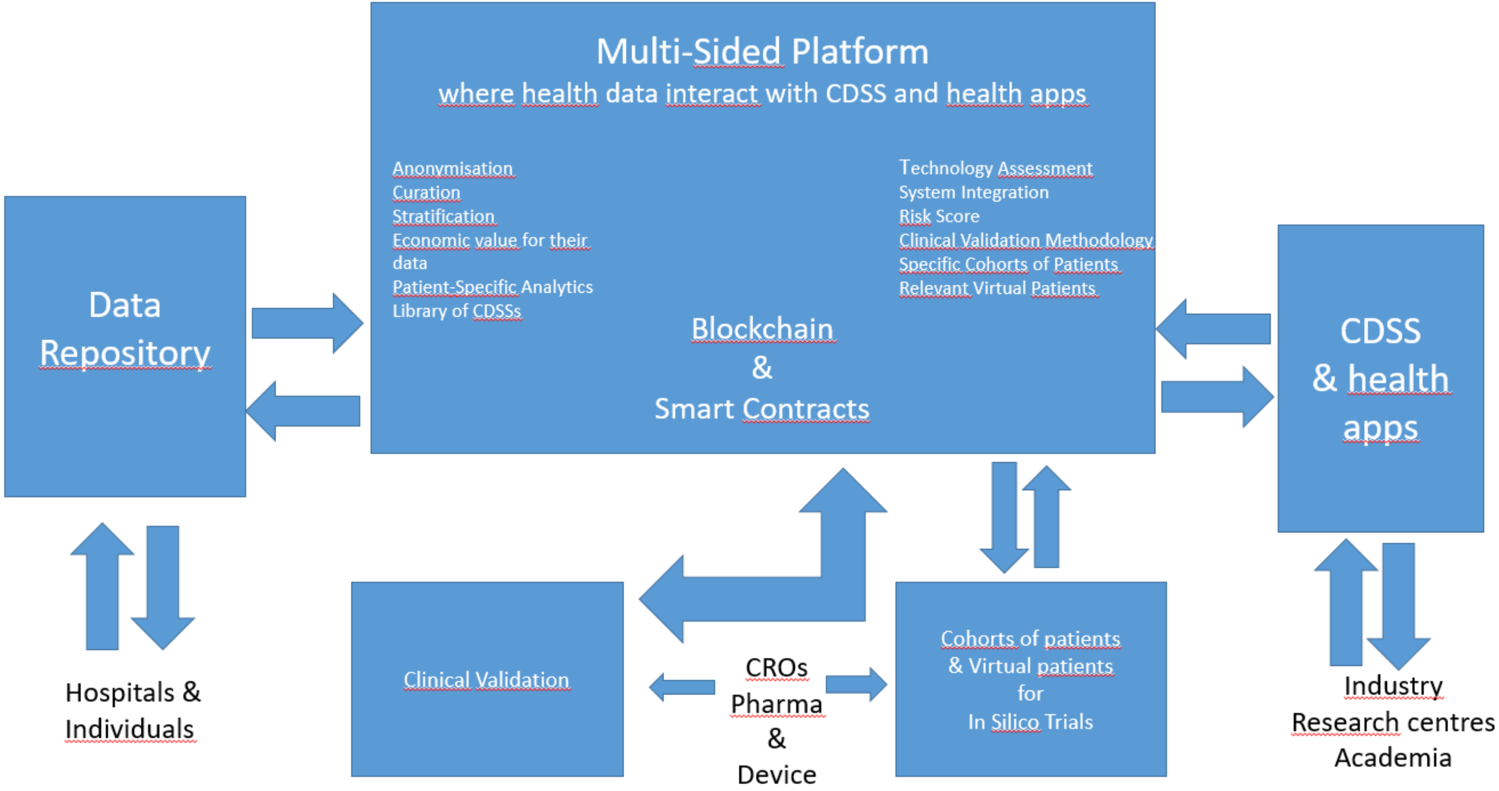
- This innovation process will also imply moving towards a different economic model:
  - in which patients are eventually reimbursed for getting their exomes and their genomes sequenced,
  - allowing to get health issues identified and diagnosed much earlier.
- All great health risks are currently covered by social insurance or national health services, and should remain so, as a distinctive feature of Europe’s social model.
- Still, it can make sense to have the drive towards preventative care being initially triggered by private actors, and especially by insurance companies
- With a substantial part of the cost being paid by the individual forerunners willing to experiment (and pay) for this new approach.
- An anticipation of such a move could be initiated by insurance companies starting to competitively offer tailored complementary health coverage plans based on data transparency and correlated integrated care agreements with their customers.
- The latter would accept to undergo recurrent health testing, making their personal health accounts or EHR available for appropriate analytics performed on them.
- The customers would this way allow the insurance companies to provide affordable preventative care reducing the cost falling on public coverage for the highly costly successive disease treatment and hospitalisation.
  - Blockchain solutions can be easily identified for incentivising customers’ behaviour collaborating with innovative health insurance companies

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 effectivenes of MSPs

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



Multi-Sided Platform

where health data interact with CDSS and health apps

Anonymisation
Curation
Stratification
Economic value for their data
Patient-Specific Analytics
Library of CDSSs

Technology Assessment
System Integration
Risk Score
Clinical Validation Methodology
Specific Cohorts of Patients
Relevant Virtual Patients

Blockchain
&
Smart Contracts

Data Repository

Hospitals & Individuals

CDSS & health apps

Industry
Research centres
Academia

Clinical Validation

CROs
Pharma
&
Device

Cohorts of patients
& Virtual patients
for
In Silico Trials