Call identifier: H2020-ICT-2016 - **Grant agreement no**: 732907
Topic: ICT-18-2016 - Big data PPP: privacy-preserving big data technologies

Deliverable 11.2
Project Presentation

Due date of delivery: January 31st, 2017
Actual submission date: February 6th, 2017

Start of the project: 1st November 2016
Ending Date: 31st October 2019

Partner responsible for this deliverable: LYNKEUS
Version: 2.0

Dissemination Level: Public Document Classification

Title	Project Presentation
Deliverable	D11.2
Reporting Period	
Authors	Anna Rizzo
Work Package	WP11
Security	
Nature	
Keyword(s)	

Document History

Name	Remark	Version	Date
Anna Rizzo	First Draft	1.0	January 27th

List of Contributors

Name	Affiliation
Anna Rizzo	LYNKEUS

List of reviewers

Name	Affiliation
Mirko De Maldè	LYNKEUS
Edwin Morley-Fletcher	LYNKEUS

Index

Introduction ... 4
Project Objectives ... 5
Project Timeline ... 6
Project Structure ... 7
Presentation Materials ... 10
  Presentations ... 10
  Press release ... 11
  Flyer ... 12
  Project website ... 14

Introduction

This document contains the presentation of the project, as well as the presentation materials, and aims at introducing MyHealthMyData (MHMD) scopes and peculiar features.

MHMD is intended to address the topical issues underlying the sharing, management and protection of personal health data in the EU context. Its goal is to develop the first open biomedical information network centred on the connection between organisations and the individual, aiming at encouraging hospitals to start making anonymised data available for open research through MHMD secure federated Infostructure, while prompting citizens to become the ultimate owners and controllers of their health data.
MHMD profiles and classifies sensitive data based on their informational and economic value, and assesses the most suitable and robust de-identification and encryption technologies needed to secure different types of information, while still allowing advanced knowledge discovery through analytics and deep learning applications running on a growing amount of anonymised or pseudonymised data.

The system will rely on the introduction of some key innovations, including:

- **Blockchain:** a digital ledger where information relating to the distributed storage of the health data is trimmed in hash-based language code, making it possible both to assign to each dataset a unique, fully traceable, digital Persistent Identifier (PID), and to associate it with metadata describing exactly what type of data are available, and referring to what cohorts of patients, while data transactions are continuously validated to the entire network of stakeholders, avoiding any possibility of fraudulent usage;
- **dynamic consent:** the possibility for individuals to provide different types of consent according to distinct potential data uses, taking control over who will access his/her data and for what purpose;
- **personal data accounts:** personal data storage clouds enabling individual access from any personal device through the blockchain in a probative, secure, open and decentralized manner;
- **smart contracts:** self-executing contractual states, based on the formalisation of contractual relations in digital form, which are stored on the blockchain and automate the execution of peer-to-peer transactions under user-defined conditions;
- **multilevel de-identification and encryption technologies:** advanced techniques for encoding and de-associating sensible data from the owners' identity (*i.e.* multi-party secure computation, homomorphic encryptions), while allowing analytics applications to leverage the information.

Project Objectives

1. **CITIZENS' EMPOWERMENT, by**
   - Development of the **dynamic consent** interface, aimed at enabling data subjects to allow, refuse and withdraw access to their data according to different types of potential usage.
   - Build-up of a **blockchain-based software infrastructure** in which institutional and individual data exchanges are governed by peer-to-peer relationships between all the stakeholders.
   - Implementation of the **personal data account**, a personal cloud allowing data subjects for direct access to their whole clinical data from any personal device through the blockchain.
   - Use of **smart contracts** to define permissions to access the data and assist data subjects in their right to access, erase, modify delete or even "be forgotten".
   - Analysis of the **regulatory framework**, and particularly of the EU **General Data Protection Regulation** entering in force in 2018, with regard not only to the current rules for processing health data and other personal information, but also with the aim of checking how the whole of MHMD Infostructure, ad in particular its blockchain and smart contracts systems, will be operationally applicable, representing an innovative challenge for the detection of **new rules and best practices** for uncovered processes, solutions and methodologies.
   - Analysis of **users' behavioural patterns** alongside **ethical and cultural orientations**, to identify hidden dynamics in the interactions between humans and complex information services.

2. **DATA PROTECTION, by**
   - Application of the **blockchain** model, a resilient and decentralised secure control system to monitor and assess the legitimacy of data transactions and detect fraudulent activities in real time.
   - Identification and system implementation of the most suitable and robust **de-identification and encryption technologies** needed to secure different types of information.
   - Evaluation of the overall security of the system architecture by testing it through dedicated re-identification and penetration **self-hacking simulations and public hacking challenges, performed on synthetic data sets.**

3. **DATA VALUE ENHANCEMENT, by**
   - Profiling and classification of sensitive data based on their **informational, scientific and economic value**.
   - Implementation of **normalisation services** able to process, harmonize and semantically consolidate all authorized data allowing rapid merging of heterogeneous sources.
   - Creation of a unique application programming interface (API) to facilitate **lawful data access to all registered stakeholders with a user-friendly registration process**, supporting development of a proper **Big Data analytical framework**.
   - Exploring potential ways to make use of **anonymised or pseudonymised data** with **advanced data analytics and patient-specific model-based prediction applications**, accelerating discoveries, fostering technological innovation and improving clinical care.

Project Timeline

Phase 1 (running from month M1 to M12) – Project Set-up and Requirements Analysis

The first phase, running from M1 to M12 of the project, will deal with the definition and acquisition of the user requirements and technical requirements, with the support of the end-users and of all the technical partners that will be implementing the security solutions and the data exchange platform. In this phase, the key methodologies will be formalised, which will inform the core implementation phase of the project. Furthermore, during this phase a dedicated analysis of EU and national relevant regulation will be started, with the evaluation of the state-of-the-art regulatory framework, and the analysis of the compliance of the project approach with the regulatory constraints. The legal evaluation of the dynamic consent approach will be also started. An ethics review of the dynamic consent will be also performed, together with the design of the user interface. Also, the construction of the data catalogue will be completed, while the definition of the data dictionary will be started. Finally, blockchain and smart contracts definition will be completed. At the end of this phase, the first Milestone will be reached (Milestone 1 – user and technical requirement- compliance assessment- dynamic consent design- data catalogue – blockchain and smart contract definition).

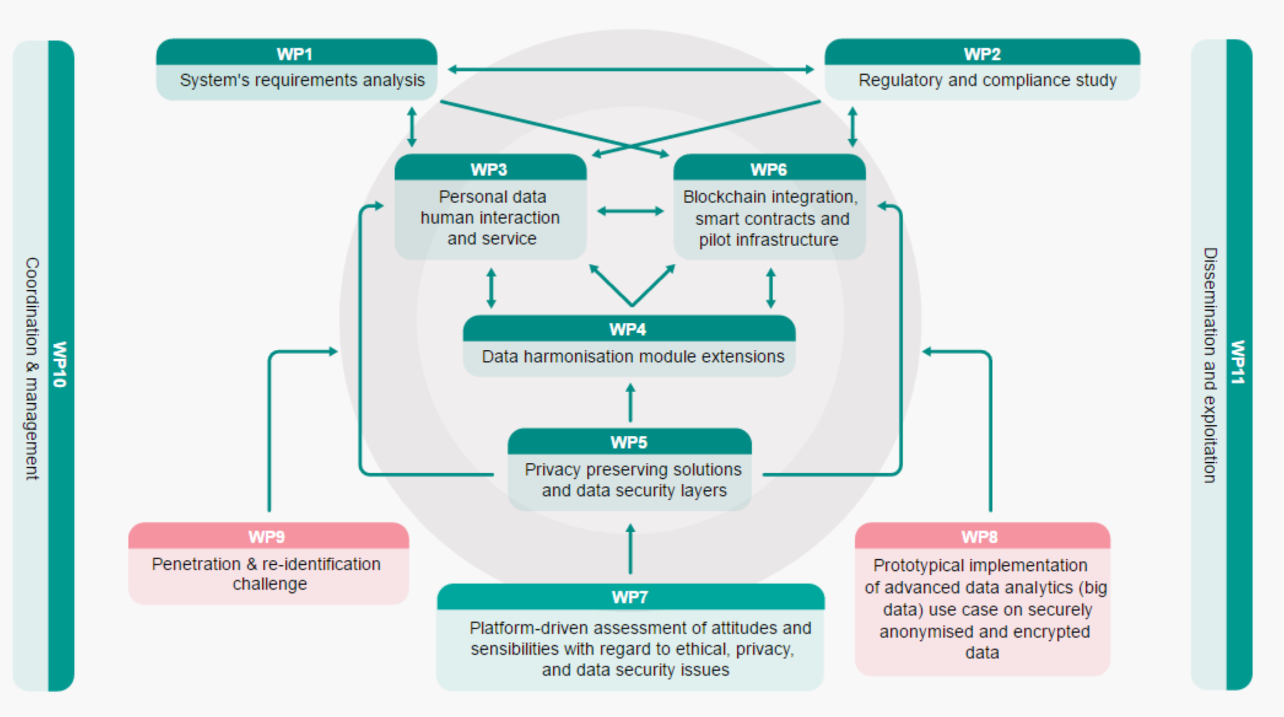
Phase 2 (running from month M12 to M18) – Securitization of the Prototypical Platform

Based on the established requirements and regulatory analysis, the core implementation phase will start, with the deployment of the technical methods and tools for the data anonymization and encryption. This phase will also be the core developmental phase for the blockchain and associated smart contracts, together with the interaction with the data platform. During this phase, the data analytics tools will be adapted to deal with encrypted and anonymised data. Furthermore, the questionnaire for the ethical ad societal analysis will be deployed and integrated in the user interface. Finally, the penetration testing preparation will star. Additionally, during this phase, the Strategic Exploitation Seminar will be held and the 1st Exploitation Plan will be drafted. At the end of this phase, the Second Milestone will be reached (Milestone 2- anonymization and encryption compliance- ethics, security and privacy- prototype in its alpha version).

Phase 3 (running from month M18 to M30) – Implementation of platform

During this phase, the blockchain application will be fully deployed, while the evaluation of the different anonymization and encryption techniques developed will start. The exploration of applicability of data analytics tools to secured data will continue and the results will be reported. In this phase the penetration challenge will also be publicly administered. The ethical and societal analysis will be completed. Finally, the Personal Data Platform will be fully integrated with blockchain and security solutions. The final exploitation plan will be issued. At the end of this phase, the Third Milestone will be reached (Milestone 3 – tools and platform’s components deployed- prototypical platform in final version).

Project Structure


WP1
System's requirements analysis
WP2
Regulatory and compliance study
WP3
Personal data human interaction and service
WP6
Blockchain integration, smart contracts and pilot infrastructure
WP4
Data harmonisation module extensions
WP5
Privacy preserving solutions and data security layers
WP9
Penetration & re-identification challenge
WP7
Platform-driven assessment of attitudes and sensibilities with regard to ethical, privacy, and data security issues
WP8
Prototypical implementation of advanced data analytics (big data) use case on securely anonymised and encrypted data
WP10
Coordination & management
WP11
Dissemination and exploitation

WP1 - Leader: HES-SO

This work package will take care of the gathering and iterative update of **system requirements** during the project lifetime, particularly **user requirements, architecture design requirements, application programming interface (API) specifications, performance requirements and existing security and privacy solutions.** These are going to be defined in collaboration with users' representatives of the involved stakeholder groups, namely **individual data subjects, hospitals, research centers and businesses**, through questionnaires, interviews and focus groups.

WP2 - Leader: Nctm

This work package will deal with the **evaluation of project developments to ensure compliance with the current privacy and data protection applicable legislation** at EU, national and international level, with particular attention to the novel framework laid down by the **General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).**

WP3 - Leader: HWC

This work package will **assure the willingness of patients as data subjects to donate their information**, and to allow them to be used within their control through the **Dynamic Consent model**.

The user interface will be implemented to empower data subjects with the **ability to allow or revoke data access** for specific purposes with the use of **Smart Contracts**, and **to be notified** about the use of their information, by whom and for what purpose.

WP4 - Leader: HES-SO

The work package will take care of the **development of normalisation services designed to process,**

harmonize and integrate the highly heterogeneous data coming from the different data sources.

WP5 - Leader: Athena

This work package will be devoted to the development of **solutions for data protection and privacy preservation,** including data publication and flow execution engines incorporating **anonymisation and encryption** techniques, implementation of methods for **data profiling, application of watermarks and fingerprints** to datasets, and **privacy-by-design analytics**.

WP6 - Leader: Gnùbila

The goal of this work package is to **design, implement and deploy the blockchain technology** as the transparent and distributed **data transaction ledger**. The infrastructure will comprise an **identity provider, a blockchain ledger, an application programming interface (API)**, second level anonymisation and data replication services. The platform will be delivered, documented and thoroughly tested, and made available for penetration challenges and the execution of re-identification threat scenarios.

WP7 - Leader: Lynkeus

The goal of this work package is to **assess the public perceptions and attitudes towards privacy and data security**, which will be employed to drive the design of MHMD platform, Personal Data Accounts, Dynamic Consent Module and Smart Contracts. The study will utilize two complementary information gathering approaches: the former investigating **users' actual behaviors** through the use of **data mining techniques** applied to data transactions and user profiles, to study what type of data users tend to give or deny permission access to, under what circumstances, and for what reasons; the latter measuring their **stated values and preferences**, by electronic questionnaires which will capture user values and preferences under different scenarios.

WP8 - Leader: Siemens Healthcare GmbH

The main objective of this work package is to **demonstrate the feasibility of clinical applications using the MHMD infrastructure** and to explore potential ways to exploit the value of large medical and non-medical datasets. In particular, the possibility of making use of **securely anonymised or encrypted data for advanced data analytics and patient-specific model-based prediction applications**, such as personalized physiological modeling for clinical risk estimation, or retrieval of medical annotations relative to a clinical case as well as identification of similar cases from the database.

WP9 - Leader: CNR

This work package deals with **penetration challenge activities**, or else the simulation of attacks to synthetic data sets with virtual subjects' information, to validate the overall system security against re-identification and privacy violation attacks, together with a risk-based cost/benefit analysis of privacy schemes. Ù

WP10 - Leader: Lynkeus

This work package will be dedicated to **disseminate project contents and outcomes** to the public, fostering the creation of a community dedicated to the themes of **data privacy and security in the e-health sector**, by dissemination materials, website and social media accounts, attendance to relevant conferences and public events, collaborations and cross-fertilization with other EU projects, and organisation of dissemination events. In parallel, this will take care of optimal **commercial exploitation of the project technological and scientific outcomes** through development of an appropriate strategy plan.

WP11 - Leader: Lynkeus

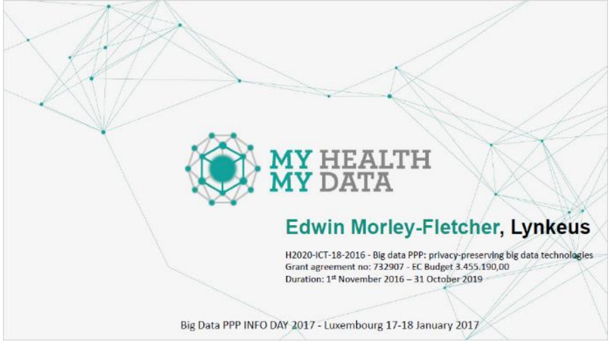
This work package is meant to **monitor and ensure the compliance of partners with their obligations under the grant agreement** by assessing the efforts performed, the accomplishment of tasks and the achievement of milestones, as well as **risk identification, assessment and mitigation**. Besides, the Coordinator will **interface on behalf of the consortium with the European Commission**, being responsible for managing financial contribution, and interface with general external requests for information.

Presentation Materials

Presentations

The project has already been presented to some dedicated events and workshops, including

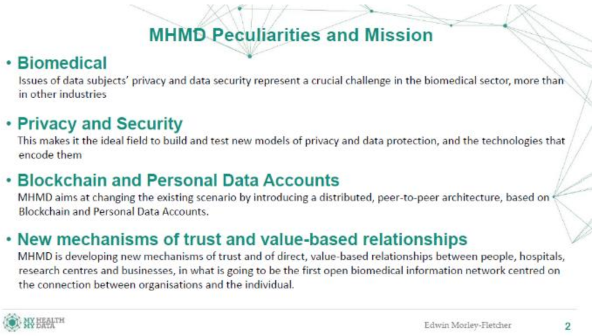
- **the Big Data Value Association Summit** held in Valencia on November 30-December 2, 2016; the meeting convened more than 350 experts from Industry, Academia, Public Administration, data owners and users from all Europe, offering a perfect opportunity to present the project to this huge network;
- **the Information and Networking Days on Horizon 2020 Big Data Public-Private Partnership topics 2017**, taking place in Luxembourg on January 17–18, 2017, where MHMD was presented with a specific effort to start networking activities with the Coordination and Support Action of the Big Data PPP call ICT-18 (Privacy-preserving big data technologies), which has the mandate to explore the societal and ethical implications and provide a broad basis and wider context to validate privacy-preserving technologies.


MY HEALTH MY DATA

Edwin Morley-Fletcher, Lynkeus

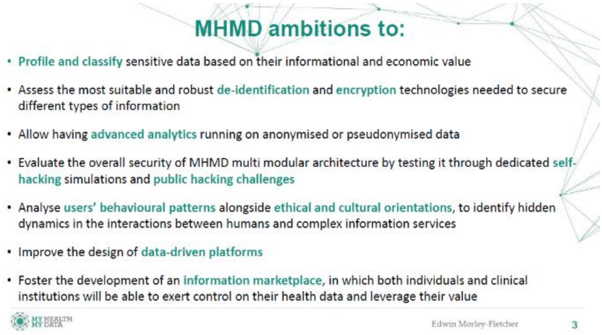
H2020-ICT-18-2016 - Big data PPP: privacy-preserving big data technologies
Grant agreement no: 732907 - EC Budget 3.455.190,00
Duration: 1st November 2016 – 31 October 2019

Big Data PPP INFO DAY 2017 - Luxembourg 17-18 January 2017


MHMD Peculiarities and Mission

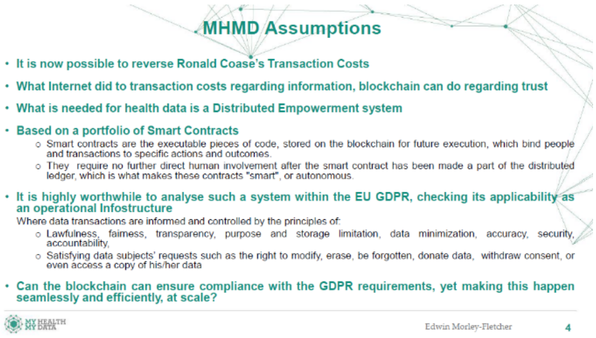
- Biomedical
  Issues of data subjects' privacy and data security represent a crucial challenge in the biomedical sector, more than in other industries
- Privacy and Security
  This makes it the ideal field to build and test new models of privacy and data protection, and the technologies that encode 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.

MY HEALTH MY DATA Edwin Morley-Fletcher 2


MHMD ambitions to:

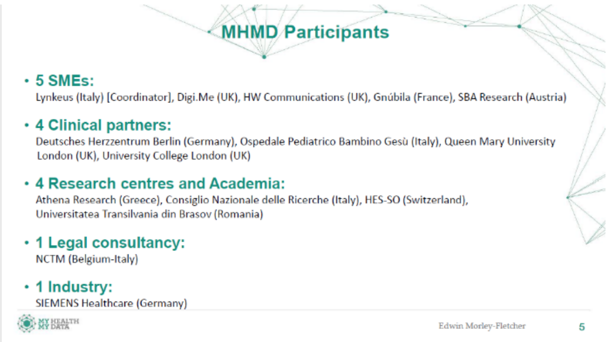
- Profile and classify sensitive data based on their informational and economic value
- Assess the most suitable and robust de-identification and encryption technologies needed to secure different types of information
- Allow having advanced analytics running on anonymised or pseudonymised data
- Evaluate 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

MY HEALTH MY DATA Edwin Morley-Fletcher 3


MHMD Assumptions

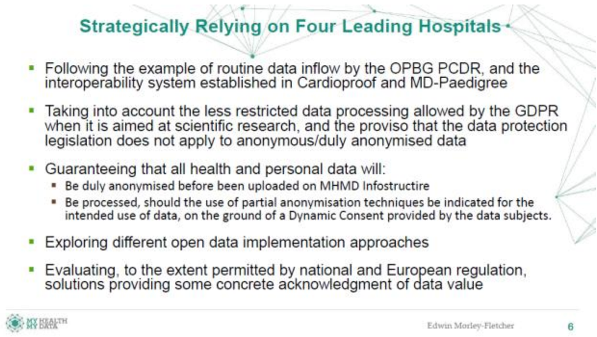
- It is now possible to reverse Ronald Coase's Transaction Costs
- What Internet did to transaction costs regarding information, blockchain can do regarding trust
- What is needed for health data is a Distributed Empowerment system
- Based on a portfolio of Smart Contracts
  - Smart contracts are the 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 can ensure compliance with the GDPR requirements, yet making this happen seamlessly and efficiently, at scale?

MY HEALTH MY DATA Edwin Morley-Fletcher 4


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)

MY HEALTH MY DATA Edwin Morley-Fletcher 5


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 Infostructire
  - 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

MY HEALTH MY DATA Edwin Morley-Fletcher 6

Press release

MyHealthMyData: Blockchain and Smart Contracts enhance utmost privacy and security in healthcare
An EU project to empower citizens with regard to the usage of their own health data

MyHealthMyData (MHMD), a H2020 EU-funded research and innovation project, is poised to be the first open **biomedical information network** centred on the **connection between organisations and the individual**, aiming at **encouraging hospitals** to start making anonymised data available for open research, while **prompting citizens** to become the ultimate owners and controllers of their health data.

MHMD profiles and classifies sensitive data based on their **informational and economic value**, and assesses the most suitable and robust **de-identification and encryption technologies** needed to secure different types of information, while still allowing **advanced knowledge discovery** through **analytics and deep learning** applications running on a growing amount of anonymised or pseudonymised data.

MHMD develops **new mechanisms of trust** and of direct, value-based relationships between people, hospitals, research centres, and businesses, by making use, for the very first time in healthcare, of a **blockchain system**, i.e. a digital ledger where information relating to the distributed storage of the health data is trimmed in hash-based language code, making it possible to describe exactly **what type of data are available**, referring to **what cohorts of patients**, and **data transactions are continuously validated to the entire network** of stakeholders, avoiding any possibility of fraudulent usage.

A **dynamic consent** interface will allow users to grant, deny and revoke data access for different uses according to their preferences through **personal data accounts**, storage clouds enabling individual access from any personal device. In this way, patients will be able to fully leverage the value of their clinical information, turning to different healthcare professionals for second opinion, or searching for profiles of similar patients and contact them upon their permission. Physicians, in turn, will have the possibility to retrieve medical annotations or execute queries to identify patients with analogous features to find cues about a specific clinical case.

Smart contracts, self-executing contractual states in digital form, will regulate data transactions between users, allowing the **permission to access**, and stakeholders, who will be enabled to make direct requests and offer **incentives** in exchange of access rights. This system will be checking its applicability as an operational Infostructure, and will represent an innovative challenge within the EU **General Data Protection Regulation** entering in force in 2018. On this basis, MHMD has the ambition to foster the development of a **true information marketplace** for healthcare.

MHMD will also analyse **users' behavioural patterns** alongside **ethical and cultural orientations**, to identify hidden dynamics in the interactions between humans and complex information services, and will assess the overall security of its multi-modular architecture by testing it through **dedicated self-hacking simulations** and **public hacking challenges**, performed on synthetic data sets.

“MyHealthMyData is an exciting project which aims at fundamentally changing the propensity to share sensitive data between clinical institutions while facilitating the transition towards a patient-centric approach based on the direct engagement of citizens” declared Edwin Morley-Fletcher, the Project Coordinator. “Blockchain and Smart Contracts will play a key role in providing the maximum degree of privacy protection and security by making trust digitally self-enacted when accessing health data”.

MHMD officially started on 1st November 2016, and is now online at www.myhealthmydata.eu. The project, is coordinated by Lynkeus (an Italian SME, based in Rome), and involves 4 other SMEs (from Austria, France, and the UK), 4 research centres and academia (Greece, Italy, Romania, Switzerland), 4 clinical centres (Germany, Italy, UK), a legal firm (Belgium/Italy), and 1 industry (Siemens).

Flyer

MY HEALTH MY DATA

A NEW PARADIGM IN HEALTHCARE DATA PRIVACY AND SECURITY

Shortage of biomedical data is rapidly becoming a thing of the past as wearable devices, integrated hospital IT systems and full scale genome sequencing become the norm in medical and wellbeing care, all this leading to an expected 40 exabytes of data produced every year in 10-year time. The challenge is now **storing and securing patients data**, in an industry were *data breaches and identity thefts are rampant, but in which, at the same time, availability of extensive, multidimensional data sets is crucial to foster innovation and improving clinical outcomes.* Reducing costs and liabilities, by **reducing 'by design' the risk of identity theft and privacy breaches, while accelerating discoveries and technological innovation**, is the fundamental goal of MyHealth-MyData.

5.6 BILLION DOLLARS/YEAR SPENT IN THE US TO PROTECT HEALTHCARE DATA

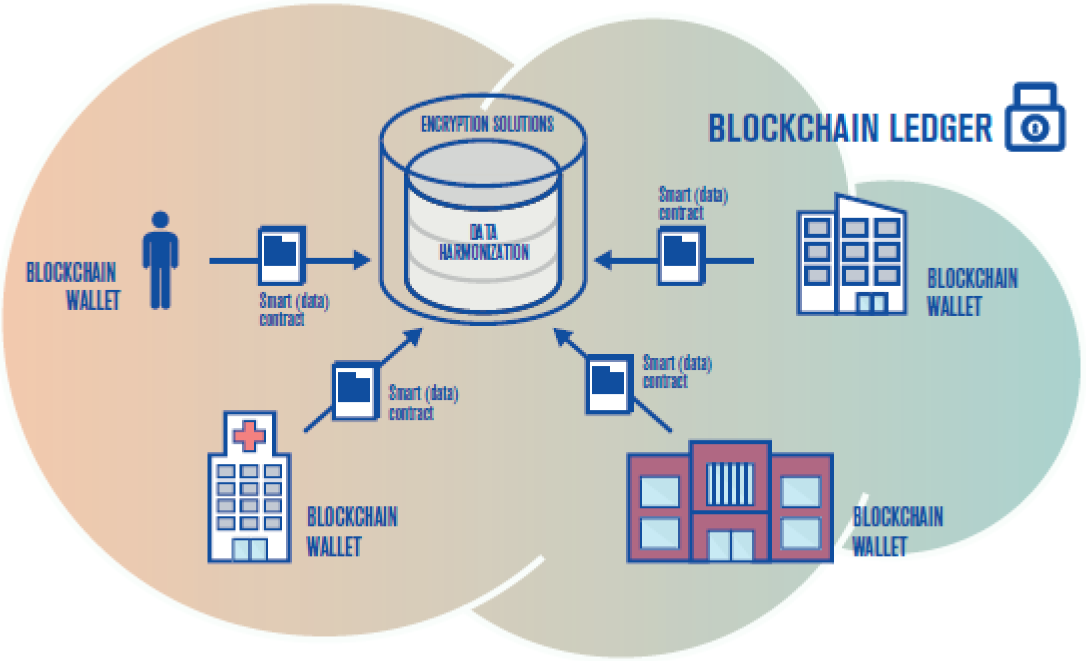
27.8/67.7 MILLIONS OF MEDICAL RECORDS BREACHED SINCE 2009

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

Today's health IT landscape is a constellation of isolated, locally hosted data repositories, managed by diverse 'data owners', which take on the cost and the risks of this still ill-defined prerogative. Punitive but unclear regulations make for high regulatory risks, while *patients remain disenfranchised, without an actual understanding of or control over who uses their personal information and for what purposes.* MyHealth-MyData (MHMD) aims at fundamentally changing these assumptions by introducing **a new way to share private information and to empower their primary owners, the patients**. This new model implements **Dynamic Consent** to drive data exchanges in a probative, secure, open and decentralized manner. **Personal Data Accounts** empower the individual over who access his/her data and for what purpose, while **Smart Contracts** automate the execution of legitimate data transactions under constantly evolving conditions. In the MHMD architecture, a **Blockchain** system is used to distribute control and detection of fraudulent activities to the entire network of stakeholders, from patients to businesses and institutions. Peer-to-peer data transactions are allowed based on explicit access rights set by individuals (not by policies that are seldom understood or properly implemented) and monitored by the entire community. The project also wants to develop a new methodology to design and apply identity protection provisions, to select, for instance, **Multilevel De-identification and Encryption technologies** based on data value and intended use, while allowing analytics applications to leverage the information. In this way, MHMD will foster the development of **true information marketplaces**, in which individuals can exercise full control on their personal data and leverage their value, implementing new mechanisms of trust and direct, value-based relationships between people, hospitals, research centres and businesses.



PARTNERS:

LYNKEUS

ATHENA Research & Innovation Information Technologies

National Research Council of Italy IEIIT Institute of Electronics, Computer and Telecommunication Engineering

digi.me it's your life

gnúbila

Hes·so Haute Ecole Spécialisée de Suisse occidentale

HWC

Nctm

SBA Research

SIEMENS Healthineers

Universitatea TRANSILVANIA din Brașov

Deutsches Herzzentrum Berlin

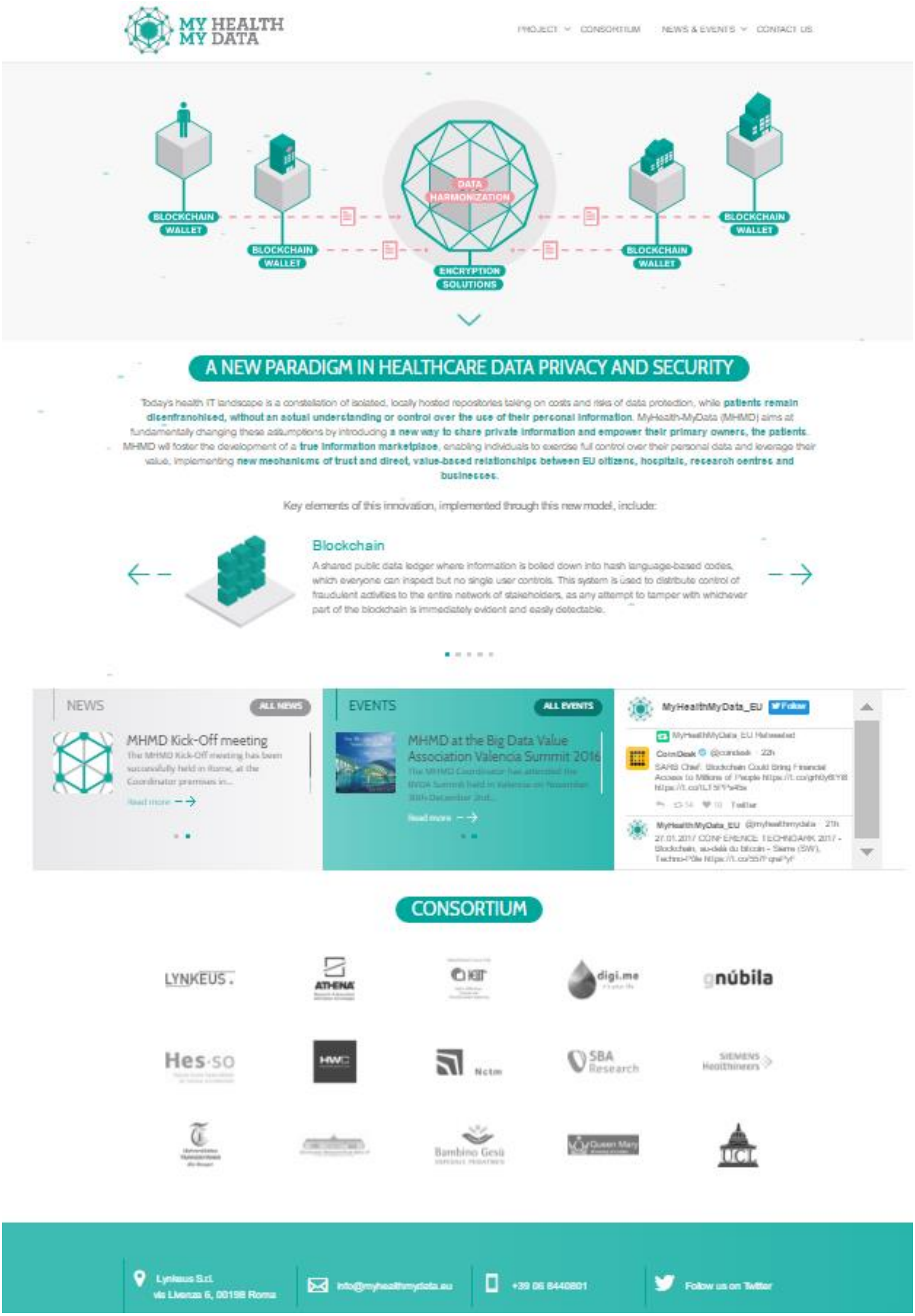
Bambino Gesù OSPEDALE PEDIATRICO

Queen Mary University of London

UCL

MyHealth-MyData (MH-MD) is a project partially funded by the EU, under Horizon2020 ICT WOrkProgramme. EU Funding: 3,456,190.00 | Start date: 1st November 2016 | End date 30th October 2019

Project website



A NEW PARADIGM IN HEALTHCARE DATA PRIVACY AND SECURITY

Today's health IT landscape is a constellation of isolated, locally hosted repositories taking on costs and risks of data protection, while **patients remain disenfranchised, without an actual understanding or control over the use of their personal information**. MyHealth-MyData (MHMD) aims at fundamentally changing these assumptions by introducing **a new way to share private information and empower their primary owners, the patients**. MHMD will foster the development of a **true information marketplace**, enabling individuals to exercise full control over their personal data and leverage their value, implementing **new mechanisms of trust and direct, value-based relationships between EU citizens, hospitals, research centres and businesses**.

Key elements of this innovation, implemented through this new model, include:

Blockchain

A shared public data ledger where information is boiled down into hash language-based codes, which everyone can inspect but no single user controls. This system is used to distribute control of fraudulent activities to the entire network of stakeholders, as any attempt to tamper with whichever part of the blockchain is immediately evident and easily detectable.

NEWS ALL NEWS

MHMD Kick-Off meeting

The MHMD Kick-Off meeting has been successfully held in Rome, at the Coordinator premises in...

Read more →

EVENTS ALL EVENTS

MHMD at the Big Data Value Association Valencia Summit 2016

The MHMD Coordinator has attended the BDVA Summit held in Valencia on November 30th-December 2nd...

Read more →

MyHealthMyData_EU Follow

MyHealthMyData_EU Retweeted

CoinDesk @coindesk · 22h

SARB Chief: Blockchain Could Bring Financial Access to Millions of People https://t.co/ghfdy8YI8 https://t.co/LT5FPs4tx

Twitter

MyHealthMyData_EU @myhealthmydata · 21h

27.01.2017 CONFERENCE TECHNOARK 2017 - Blockchain, au-delà du bitcoin - Sierre (SW), Techno-Pôle https://t.co/55P qnPyF

CONSORTIUM

Lynkeus S.r.l.
via Livenza 6, 00198 Roma

info@myhealthmydata.eu

+39 06 8440801

Follow us on Twitter