Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Blockchain for mHealth consent exchange

Emmanuel Benoist and Jan Sliwa, RISIS

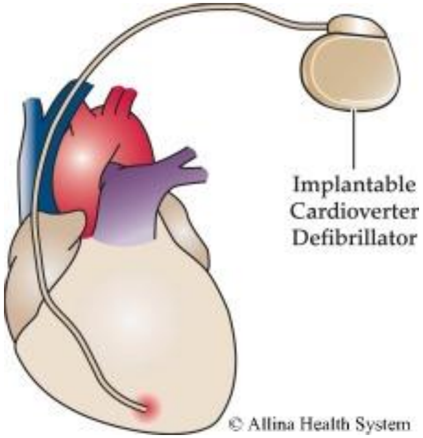
IoT Week, Geneva, June 6-9, 2017

Introduction / Motivation

IoT in mHealth - products

- **Passive**
  - Scales
  - Movement sensors
  - Clinical thermometers
  - Heart monitors (ECG)
  - Glucose meters

- **Active**
  - Implantable defibrillators
  - Insulin pumps



© Allina Health System

IoT in mHealth - usages

- **Patients follow their health / behavior**
  - Periodic / continuous measurements
  - Visualization, analysis, recommendations
  - Direct action on body – safety proven and monitored
- **Physicians receive more data**
  - Defined data flow
  - Semantic interoperability
- **Researchers may analyze results**
  - Anonymization / privacy protection
  - Consent necessary
  - Data valuable if not biased

IoT in the future of eHealth

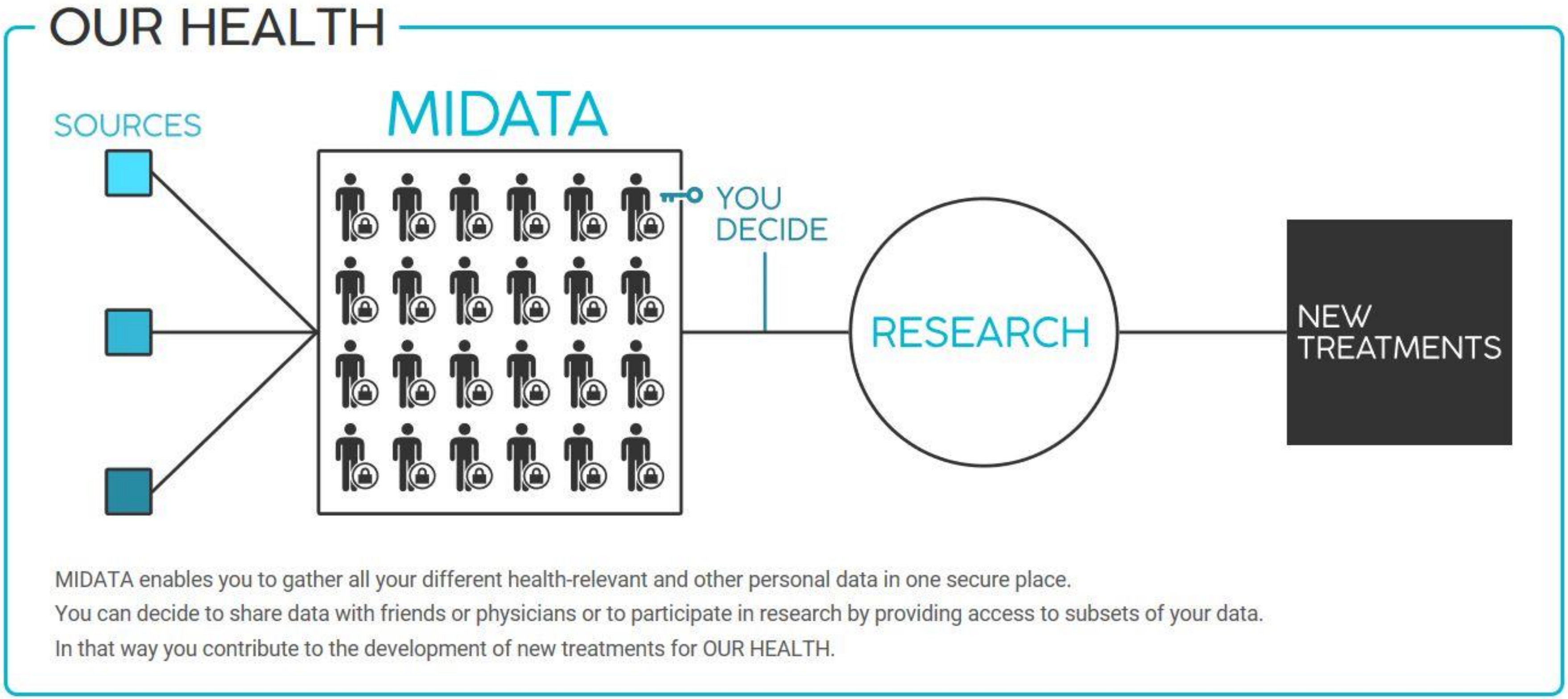
- **Mobile health**
  - Continuous health monitoring, independent of doctor visits
- **Evidence Based Medicine**
  - Efficacy of treatment based on data
- **Big Data, machine learning**
  - Processing and analyzing data streams
  - Extracting knowledge from data
- **Personalized Medicine**
  - Treatment adapted to the patient / patient group

Project partners

MiData

MIDATA.coop
MY DATA - OUR HEALTH

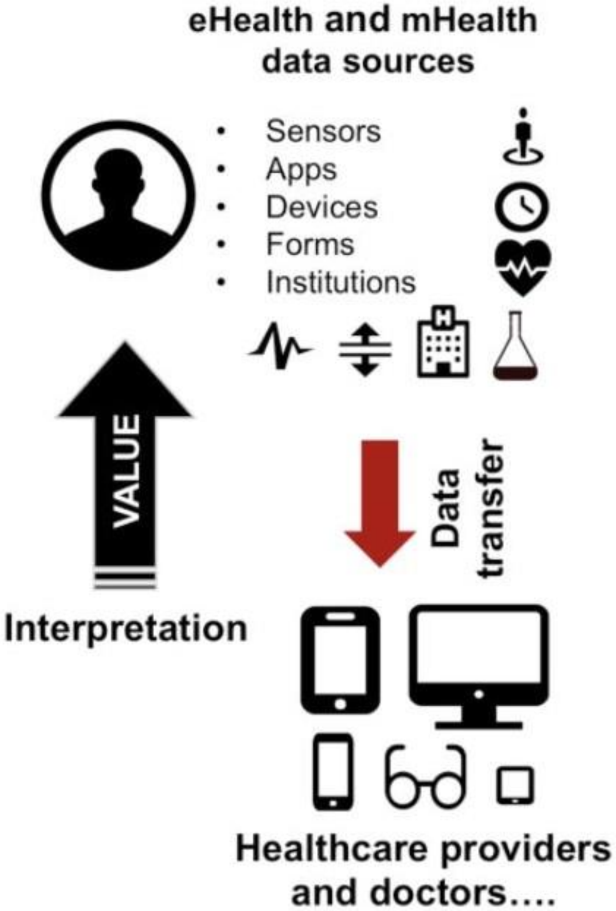
https://midata.coop/



MIDATA enables you to gather all your different health-relevant and other personal data in one secure place.
You can decide to share data with friends or physicians or to participate in research by providing access to subsets of your data.
In that way you contribute to the development of new treatments for OUR HEALTH.

Pryv

http://pryv.com/



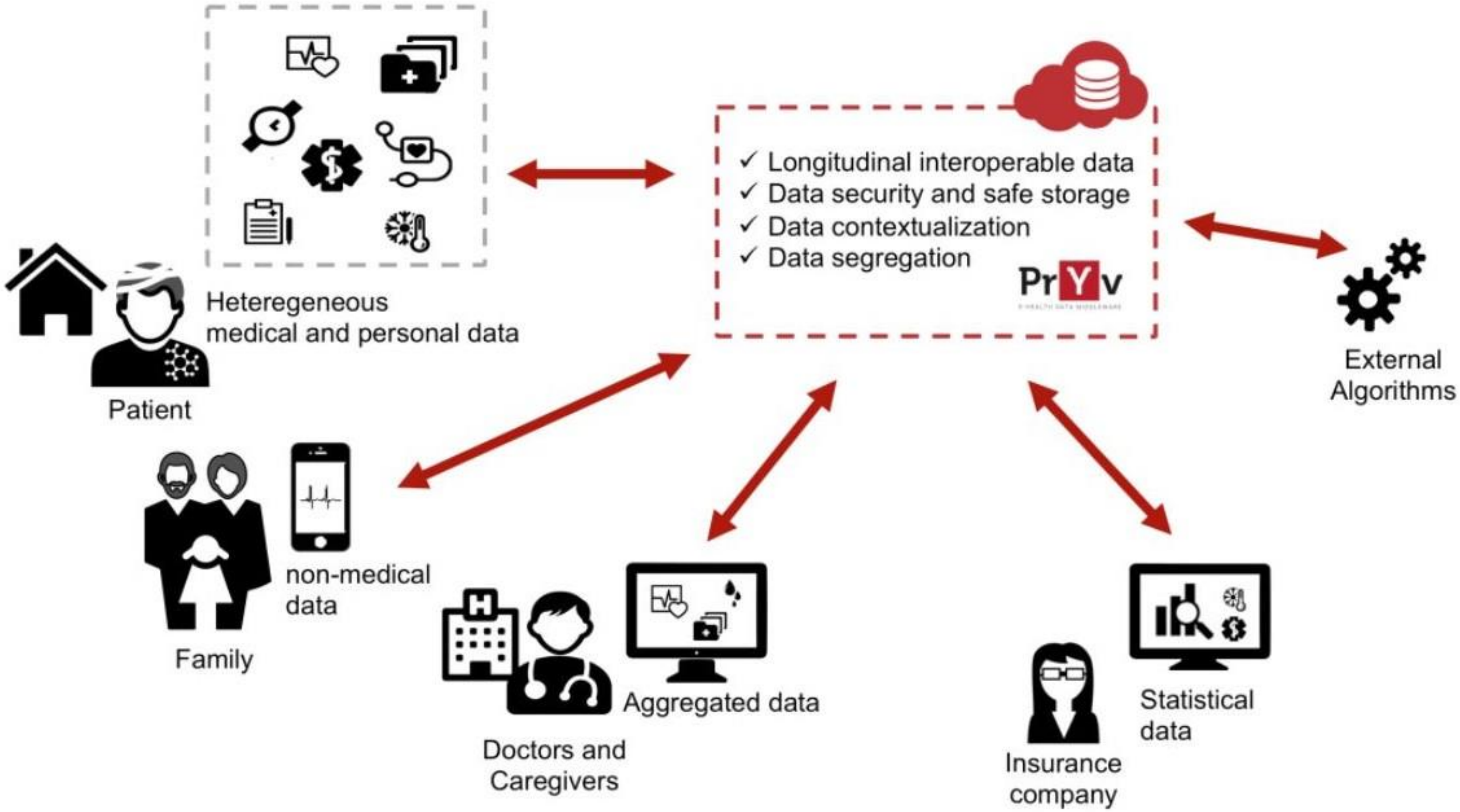
Data continuity and technical interoperability

Data security:
Encrypted transmission and safe storage

Data segregation:
access rights and ownership

Pryv

http://pryv.com/



Sharing of data

- **Research could profit from data sharing**
  - Data do not need to be sent twice
  - Reuse of data is central in medicine research
- **Requirements**
  - Patients / users are owners of their data
  - They can control the use and share of data
  - Nobody can share data from users without their consent
  - Should work even if the firms are competitors
- **Give consent**
  - Framework
  - Expendable to different actors
  - Should not require "trust" in other actors

Goals and risks

Goals

- **Give consent to share data**
  - Transfer Data - stream from Partner1 to Partner2
  - Give the Scope (which dataset)
  - Give a time frame (data already acquired and/or new data to be acquired)

- **A user can revoke the consent**
  - User do not want to share data anymore

- **User do not need to share a common identity**
  - Identity may be different on different sites

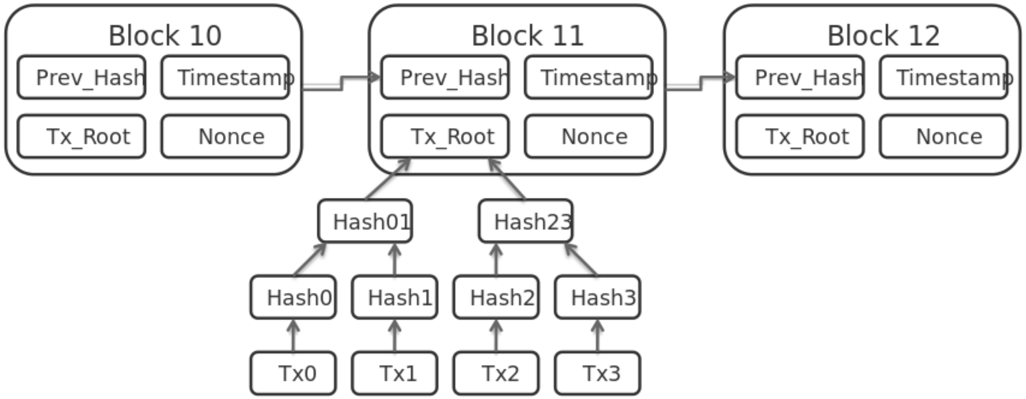
Risks

- **User cannot repudiate a given consent**
  - Repudiation not possible: "UserA gave Partner1 the order to share this dataset with Partner2"
  - Revocation is possible at any time

- **Partners can not pretend not having the consent to share**
  - The consent is written
  - Every partner can see the list

Technical solution: Blockchain

Blockchain



- **Definition**
  - One set of information
  - Shared among all actors
  - Non mutable list

- **Properties**
  - One cannot remove anything from a blockchain
  - Any actor may verify at any time what is in the blockchain

Store information inside the Blockchain

- **Consents are written in the Blockchain**
  - Together with revocations of contents

- **Consent** =

```
(Partner1, Partner2,
Identity of User on Partner1,
Identity of User on Partner2,
Scope of data sharing,
Time frame)
```

Cryptography

- **Use of Private / Public key cryptography**
  - Each of the Partners has a key pair (public/private)
  - Users do not have keys (would require a PKI infrastructure)

- **Public key is known by everybody**
  - Is transferred securely to all Partners
  - Is used to crypt messages targeted at a given Partner
  - Is used to verify the signature of a Partner

- **Private key is kept secret**
  - Is used by a Partner to read encrypted messages
  - Is used by the Partner to sign messages

Security and privacy

Security

- **Notations:**
  - Identity on Partner1 = `Id1`
  - Identity on Partner2 = `Id2`
  - Public Key of PartnerX = `PubX`
  - Private Key of PartnerY = `PrivY`
  - `nonce`s are generated by the user

- **Information stored inside the Blockchain**

```
     (Partner1, Partner2,
     Id1 + nonce1 encrypted with Pub1,
     Id2 + nonce2 encrypted with Pub2,
     Key to access information on Partner1 encrypted with
Pub2,
     Key to access information on Partner2 encrypted with
Pub1,
     Scope of data sharing,
     Time frame) Signed with Priv1, and Priv2
```

Validation

- **Impossible for one single actor to insert anything**
  - Need to be validated by the two partners

- **Impossible for anybody to repudiate an action**
  - Blockchain is immutable : Wrote once, stays forever
  - Possibility to revoke at any time

- **Actors can not pretend the consent does not exist**

- **Actors do not need to trust each other**

Why Blockchain in IoT?

Why blockchain in IoT?

- **Lot of different actors**
  - Builders of different IoT devices
  - Aggregators of data
  - Researchers
  - Physicians
  - But Number 1 = Users / Patients / Persons

- **Lack of trust**
  - No one wants to give the control to a central entity
  - Everyone can access to the entire information
  - Everyone can verify at any moment

Advantages of the Blockchain

- **The information is shared**
  - No one controls the information
  - No one can manipulate the information (add or remove elements)

- **No Need for Trust**
  - Blockchain is accessible by every actors

- **Scalability**
  - Works with 2 partners or with 26

Problems with blockchain

- **Privacy concerns**
  - Medical data are "sensitive data" (legally defined in CH)
  - Consent is already sensitive (one could see a specific illness)
- **Why not encrypt with patient Private key:**
  - Better solutions are possible using a PKI for Users/Patients, but it is not available in Switzerland.
- **Solutions**
  - The blockchain is only available for Actors of the network
  - Identifiers of persons are always cyphered
  - Dictionary attack is only possible if the nonces are known

Conclusion

Conclusion

- **Blockchain for IoT**
  - Trust in the technology more than competitors
  - Not interesting for sharing information (data to large)

- **Consent for mHealth**
  - Very important
  - Very sensitive

Thank you for your attention !

emmanuel.benoist@bfh.ch
jan.sliwa@bfh.ch