Enhancing the Trust in e-Health by Secure and Privacy-Preserving Identity Management

Bian Yang, Dr., Assoc. Prof.,
Center for Cyber & Information Security
Department of Information Security and Communication Technology
Norwegian University of Science & Technology (NTNU)
bian.yang@ntnu.no

digital enlightenment forum

About NTNU IIK and CCIS

NTNU

Kunnskap for en bedre verden

- Norges teknisk-naturvitenskapelige universitet – NTNU Largest Science and Technology University in Norway
- One of the “Nordic Five Tech”
- Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK)

Center for Cyber and Information Security

- Based on IIK and collaborated with external partners

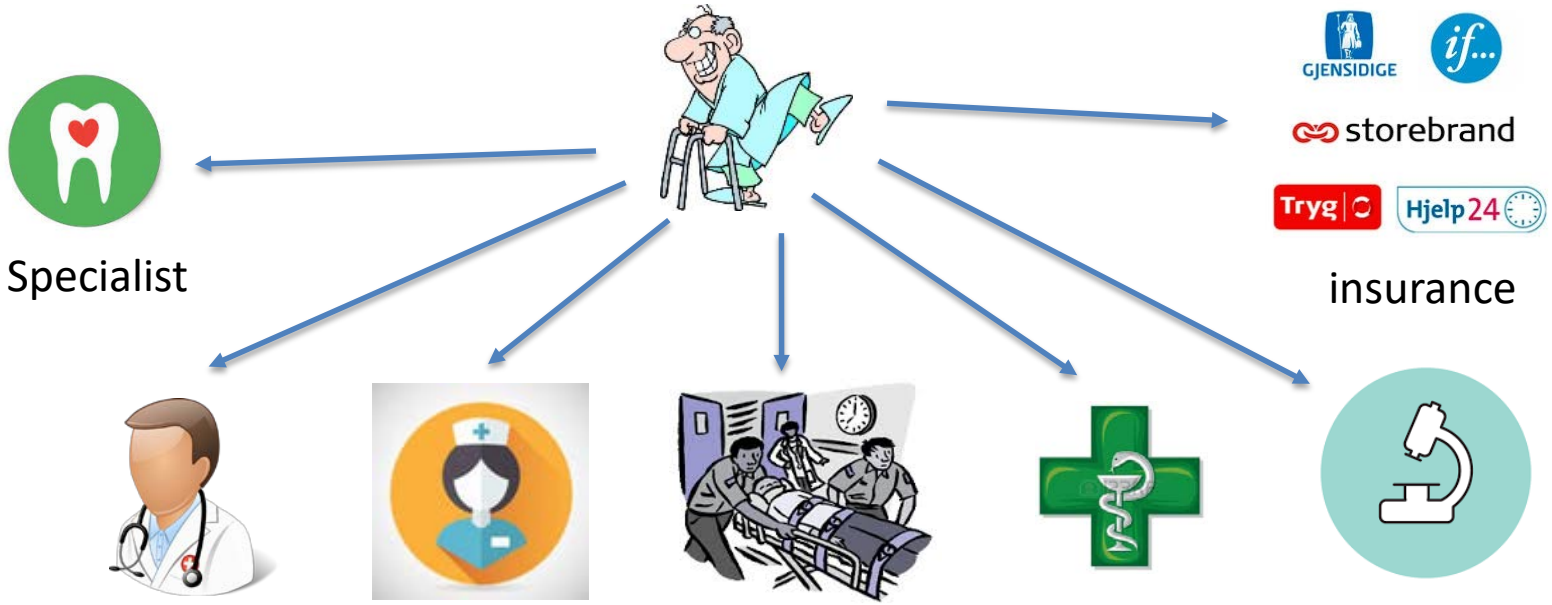
Data is the key to all

Data are generated from everywhere in e-health, for instance, but not limited to

- Paper-based medical records
- EMR
- EHR
- Patient-Generated Health Data (PGHD)
- PHR
- Health databases for scientific research
- Agreements (contract, consents, etc.)
- Operational data
  - Identities (patient, staff, technician, device, equipment, syste, etc.)
  - Transaction records (data sharing, payment, manual, etc.)
  - Logistic and work process logs and performance (equipment, staff, system, etc.)

Data is the key to all

Players in the health data eco-system

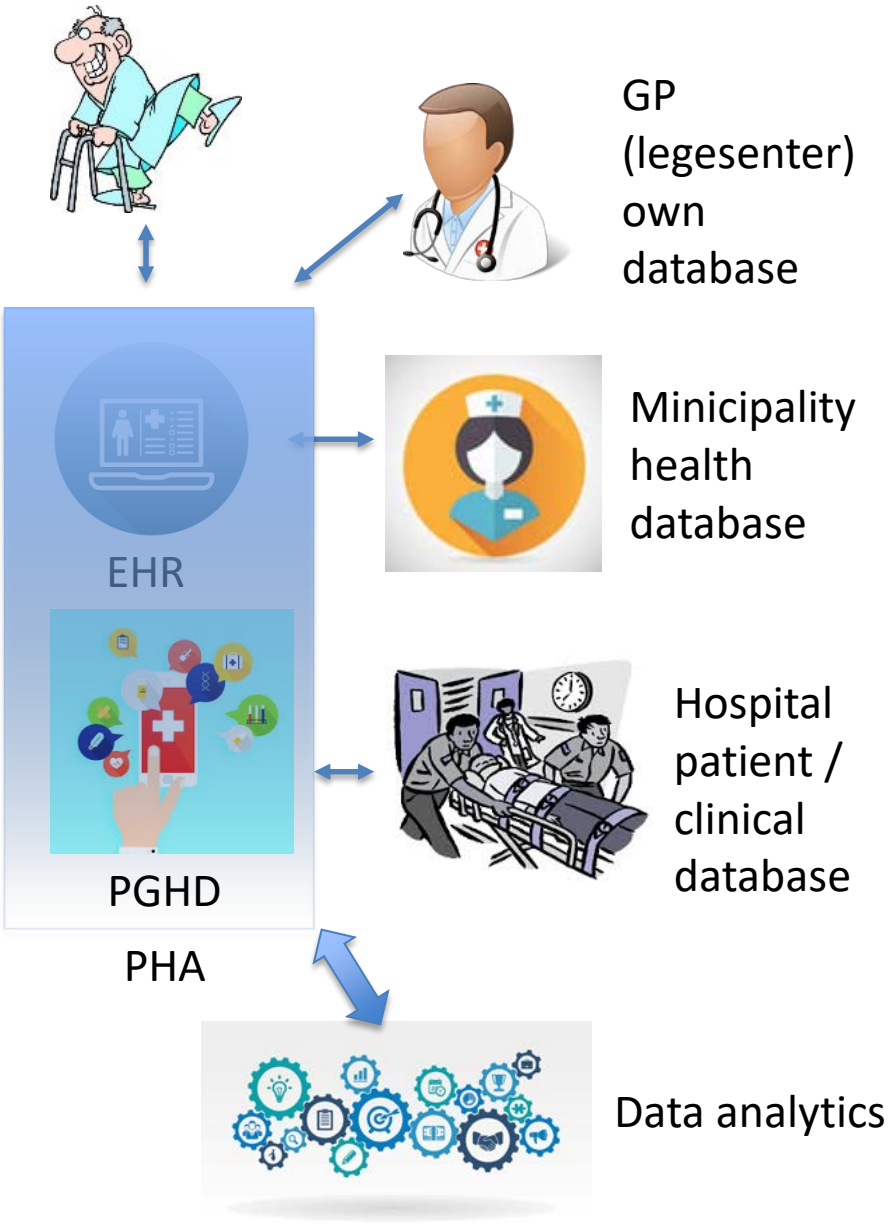


Data is the key to all

Challenges

- (Health 1.0) Electronic Medical Records (EMR) -> data silos
- (Health 2.0) Electronic Health Records (EHR) -> interoperability, consent and privacy management
- (Health 3.0) Personal Health Records / Accounts (PHR/PHA)

  -> patient-centred data management



Data is the key to all

Health 3.0 essentials

- Patient's full health data profile accessible
- Patient-centred data management, patient decides the data to be shared with
  - Whom
  - For what purpose(s)
  - At what time
  - For how long
  - Via which channel(s)
- Patient-centred privacy configuration
  - To which degree personal information can be shared (privacy impact assessment and best practice)
  - At which conditions the privacy configuration is to be changed

Relevance to Identity

- **Identity** (ISO 24760-1: 2011)

set of **attributes** related to an entity

- **Attribute** (ISO 24760-1: 2011)

characteristic or property of an **entity** that can be used to describe its state, appearance, or other aspects

- **Identifier** (ISO 24760-1: 2011)

unique identity

Relevance to Identity

Identity Management screnarios in healthcare

- Identity Proofing (ISO 29003)
  - establishing a new identity outside the trust domain (e.g., another hospital, regional health authority, member state, etc.)
  - Health notary (certification of medical / health records / transactions)
  - Professional medical certificates
- Patient identification (particularly those unconscious, elderly, and challenged)
  - Token based
  - Biometrics
- Person / device identity authentication (e.g., password, card, biometrics)

Relevance to Identity

Identity Management screnarios in healthcare

Privacy-Preserving Identity Management

Identity Proofing

- Selective disclosure and certification of identity attributes
- Anonymous attribute proofing / ownership verification

Related methods: Open Identity Exchange, zero-knowledge proof, homomorphic encryption, secure multi-party computation, etc.

Relevance to Identity

Identity Management screnarios in healthcare

Privacy-Preserving Identity Management

Identity Authentication

- Federated identities and Single-Sign-On (SSO)
- User-centric (e.g., OpenID, FIDO, GOV.UK Verify, etc.)
- Self-sovereignty identities (full under the control of the identity principals, able to create new identities by assembling certified attributes, etc.)

Related methods: biometric template protection, biometric-secret binding schemes, zero-knowledge proof, homomorphic encryption, secure multi-party computation, oblivious transfer, distributed ledger technologies e.g. blockchain, etc.

Relevance to Identity

Identity Management screnarios in healthcare

Privacy-Preserving Identity Management

Data Outsourcing for Analysis

- De-identification for data analytics
- Re-identification (GDPR's right to access, portability, and be forgotten)

Related methods: anonymisation, pseudonymisation, differential privacy methods, zero-knowledge proof, commitment schemes, etc.

Research efforts needed in …

- Privacy-preserving biometrics (ISO 24745)
  - Renewability
  - Irreversibility
  - Unlinkability
- Privacy-preserving attributes proofing
  - Selective disclosure
  - Selective property/value proofing
  - Anonymous ownership verification
- Distributed ledger technology
  - Flat structure to facilitate attribute certification
  - Trusted platform for creating self-sovereignty identities
  - Potential platform for data subjects to trade their data for profit

NTNU IIK involved in EU projects

Related to privacy-preserving identity management

- TURBINE (2008-2011): revocable biometrics
- FIDELITY (2012-2016): privacy-preserving passport life cycle
- PIDaaS (2014-2016): private identities as a service
- ORIGINS (2014-2017): breeder document security and identity proofing
- SMILE (2017-2020): privacy-enhancing land border control

Contact

Bian Yang, Dr.

Associate Professor,

eHealth and Welfare Security group at Center for Cyber and Information Security (CCIS) at

Institutt for informasjonssikkerhet og kommunikasjonsteknologi, NTNU Gjøvik.

bian.yang@ntnu.no

Tel. +47 611 35 486