Centralised versus Decentralised Management of Patients’ Medical Records

Catherine QUANTIN¹, Gouenou COATRIEUX, Maniane FASSA, Vincent BRETON, David-Olivier JAQUET-CHIFFELLE, Paul de VLIEGER, Norbert LYPSZYC, Jean-Yves BOIRE, Christian ROUX, François-André ALLAERT

¹-Department of Biostatistics and Medical Informatics, CHU Dijon, France
Introduction

- For more than 20 years, many research projects have been conducted to create a standardised, centralised, secure and reliable Medical Record (MR) system, but with little success.
Planned standardised MR system: the reasons for the failure

- Insufficient human and financial resources
- Lack of or failure to properly deploy a Unique Patient Identifier (UPI)
- Lack of standardisation or structuration of the MRs: The only domain where real harmonisation has been obtained is with international classification of diseases – like the ICD - and treatments – like the ICOD. However, though such classifications are now included within MRs to record the activities of health structures, they are not being used for the daily management of patients in all European countries
The dangers of centralisation

- Risk of losing all data if the centralised organisation is destroyed: this weakness of a centralised system, is the main reason for the creation of the INTERNET, a network that would continue to function in the event of a catastrophe.

- Hackers or terrorists may see a centralised system as a challenge to divulge or modify patients’ medical information

- Secure management of access is difficult to achieve
A new strategy

- It is time to develop a new strategy based on a non-centralised, unstructured MR system that could really bring benefits to patients and doctors.
- The main goal of this presentation is to promote this non-centralised MR system that uses non-standardised documents and is able to search for and gain access to distributed medical data.
Decentralised management of MRs

- In industrialised countries, each health-care structure has an information system.

- Information contained in the daily routine MR is sufficient for patient care: we believe that a decentralized MR system could make available to the MP the needed information to reconstitute a patient’s medical history.

- We would thus be able to set up a system that allows each doctor, with the authorisation of the patient, to collect, synthesise, and regularly update information from the different health structures.
Basic principles

- All MRs are managed in their unmodified form in health structures with the usual identifiers (first and last names and date of birth).
- When the patient and Medical Practitioner (MP) want to gain access, they have to be connected to an electronic server to identify themselves.
- Medical Record Search Engines (MRSE) will securely gather medical information and transfer it to the MP.
- Patient’s privacy is protected (pseudonymous code derived from the patient’s identity). All communications are encrypted (asymmetric algorithm).
Step 1: Pseudonymisation of patient’s identity

- During a consultation, the patient’s identity will be anonymised, using a cryptographic hash function to provide a hashed patient identity (pseudonymous code) : H(PI)
Patient’s Identity : (PI)
Hashed patient identity : H(PI)

MP
  ej : MP’s public key
  IdMP : MP’s identity
Step 2: Sending the request to the two MRSEs

- The MP sends a request “x” to the Medical Record Search Engines and authenticates himself and the patient. To guarantee the confidentiality of the request during transmission, the information is split between the two MRSEs.

- MRSE1 receives:
  a) x, the number of the request,
  b) K, a session key,
  c) ej, the MP public key.

- MRSE2 receives:
  a) x, the number of the request,
  b) EK(H(PI)), the hashed patient identity H(PI), previously symmetrically encrypted by the MP with the session key K.
$E(x, K, e_j)_{p_{MRSE1}}$

$E(x, E_K(H(PI)))_{p_{MRSE2}}$

MP
- $e_j$: MP's public key
- IdMP: MP's identity

Patient's Identity: (PI)

Hashed patient identity: $H(PI)$

MRSE1

MRSE2
Step 3: Request transmission to all health structures

1- MRSEs decrypt the messages sent by the MP, using their own private keys
2- MRSEs consult a health structure directory
3- MRSEs sign their respective part and forward the request to all health structures
MP

e_j : MP’s public key

IdMP : MP’s identity

Patient’s Identity : (PI)

Hashed patient identity : H(PI)

E(x, K, e_j)_P_{MRSE1}

MRSE1

(x, K, e_j)

(x, K, e_j)_h_i

E(x, K, e_j)_P_{phi_i}

(x, K, e_j)_h_i

Hospital PKI directory

E(x, E_K(H(PI)))_P_{MRSE2}

MRSE2

x, E_K(H(PI))

(x, E_K(H(PI)))_h_i

E(x, E_K(H(PI)))_P_{phi_i}
Step 4: Search for the patient's MR at the health structure level

- The patient identifier (H(PI)) is decrypted with the session key K.
- Each health structure searches for medical records corresponding to H (PI)
- These corresponding MRs are sent to the aggregator.
Patient’s Identity : (PI)

Hashed patient identity : H(PI)

E(x, K, e_j)_{P_{MRSE1}}

E(x, E_k(H(PI)))_{P_{MRSE2}}

(x, K, e_j)_{P_{MRSE1}}

(x, K, e_j)_{P_{MRSE2}}

Hospital PKI directory

(x, E_k(H(PI)))_{P_{MRSE2}}

(x, K, e_j)_{P_{MRSE1}}

(x, E_k(H(PI)))_{P_{MRSE2}}

x, E_k(H(PI))

x, K, e_j

x, H(PI), e_j

x, MR, H(PI), e_j

Hospital

Identity : (PI)

Hashed patient identity : H(PI)

E(x, K, e_j)

E(x, E_k(H(PI)))

x, H(PI), e_j

x, MR, H(PI), e_j
Step 5: Results transfer to the aggregator

- Elements sent to the aggregator:
  - number of the request, x
  - hashed patient identity, H(PI)
  - patient’s MR, digitally signed by the health structure to allow non repudiation and verification of the integrity of the message.

- To ensure transmission security, confidential medical information is asymmetrically encrypted with the MP public key e_j.
E(x, K, e_j)_{P_{MRSE1}}

(x, K, e_j)_{h_i}

E(x, K, e_j)_{P_{MRSE2}}

x, E_K(H(PI))_{P_{MRSE2}}

(x, K, e_j)

Hospital PKI directory

(x, E_K(H(PI)))_{P_{MRSE2}}

x, E_K(H(PI))_{h_i}

E(x, E_K(H(PI)))_{P_{MRSE2}}

E(x, E_K(H(PI)))_{P_{MRSE2}}

E[x, E_{MR, H(PI)}e_j]_{P_A}

x, MR, H(PI), e_j

x, H(PI), e_j

(x, K, e_j)_{h_i}

Hospital {h_i}
Step 6: Gathering all patient information at the aggregator level

- The aggregator collects and gathers together all the information received from all health structures.
- These results are sent to the MP after a challenge-response authentication procedure.
- The MP will then be able to decrypt these results with his own private key.
MRSE1

\[ E(x, K, e^j)_{P_{MRSE1}} \]

MRSE2

\[ E(x, E_K(H(PI)))_{P_{MRSE2}} \]

Hospital PKI directory

\[ (x, K, e^j) \]

\[ (x, K, e^j)_{h_i} \]

\[ E(x, K, e^j)_{P_{hi}} \]

\[ E(x, E_K(H(PI)))_{P_{hi}} \]

Patient's Identity : (PI)

Hashed patient identity : H(PI)

\[ X, IdMP \]

Aggregator

\[ x, \{E(MR, H(PI))e^j\}_{e^j} \]

\[ x, \{E(MR, H(PI))\}_{e^j} \]

\[ E[x, E(MR, H(PI))e^j]_{PA} \]

Hospital \[ h_i \]

\[ x, MR, H(PI), e^j \]
Discussion : MRSEs’s attributes

- MRSEs never have access to the local HS databases
- MRSEs do not store any MRs: MRSE1 does not manage patient data, and MRSE2 only manages pseudoanonymously encrypted data
- MRSE1 and MRSE2 are not allowed to communicate.
- MRSEs and aggregators could be set up at the regional, national and European level.
Workload is not as heavy MP may think

- Some MP may complain about increased workload, but
- The contents of their local records are often sufficient to treat the patient.
- Few patient are hospitalised in many hospitals; MPs will only have to summarise one or two MRs.
- This synthesis could be done with the patient’s help.
- This effort will be reduced because one MP can pass on information about his moving patients to other MPs.
Thanks for your attention

For any detail or precision please, contact cahterine.quantin@chu-dijon.fr
No need for a UPI but DOUBLOONS AND COLLISION RISKS

- It is possible to reduce such errors by using phonetic algorithms.
- MP can send a list of pseudonymous partial identifiers for each patient.
- The MP will check information with the help of the patient.
- It is possible to give to each record a linkage probability level (high, medium or low), obtained from probabilistic modelling, so as to help the MP in the validation process.
- Whatever the amount of lost or false information, the situation (from the professionals' and patients’ point of view) will be better than the great lack of information we have now.