SHARING MEDICAL DATA

- Primary care
- Medical research
- Connected health
ELECTRONIC MEDICAL RECORDS (EMR)

• HITECH Act (US, 2009) provided a series of incentives to encourage widespread EHR adoption
  – As of 2015, nearly 9 in 10 (87%) of office-based physicians

• Countries of the European Region: According to WHO 59% have a national electronic health record system; 69% of those have legislation governing its use
MANAGEMENT OF PROTECTED HEALTH INFORMATION (PHI)

• **HIPAA** (Health Insurance Portability & Accountability Act of 1996)


• Health information exchange (**HIE**) is a sharing infrastructure for electronic healthcare information across organizations within a region, community or hospital system
EMR DATA SHARING BETWEEN PROVIDERS: CURRENT STATUS

• Patient (or legal representative) signs a disclosure form
  – Patient contact
  – Visit dates
  – Types of records
  – Who will receive it

• Printed records sent by fax or mail (CDs for images), or carried by patients: taking days
PROBLEMS

• Complicated processes on consent management
  – Patient transfer between hospitals may not be predicted
  – Time consuming and delay treatment
  – Wasted resources and increased costs

• Hard copied data difficult to manage
• Control over the data is lost once records shared
PROBLEMS

• Complicated processes on consent management
  – Patient transfer between hospitals may not be predicted
  – Time consuming and delay treatment
  – Wasted resources and increased costs
• Hard copied data difficult to manage
• Control over the data is lost once records shared

How to **speed-up & facilitate** medical data sharing while ensuring **privacy, security and auditability**?
BLOCKCHAIN FOR EHEALTH:
FROM PERSPECTIVES TO AN APPLICATION FOR RADIATION ONCOLOGY

- Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Ignaz Schumacher and Fusheng Wang
BLOCKCHAIN

- Ledger
- Distributed (non-centralised)
- Secured (using crypto)
- Immutable
BLOCKCHAIN

Block 38
- 45da07438...
- Transaction56
- Transaction57
- 09/06/17 11.03am
- 038314966...

Block 39
- 038314966...
- Transaction58
- Transaction59
- Transaction60
- 09/06/17 11.12am
- cdd31151f...

Block 40
- cdd31151f...
- Transaction61
- Transaction62
- Transaction63
- 09/06/17 11.21am
- 5635f923bd...

Id of the previous block
Transactions
Timestamp
Id of the block
DIFFERENT TYPES OF BLOCKCHAIN

- **Permissionless (public) blockchain**
  anyone in the world can read, send transactions to and expect to see them included if they are valid, can participate in the consensus process

  - Bitcoin
  - Ethereum

  - Consensus: Proof of Work* (PoW) (PoStake, PoBurn)
  - Crypto-currency
  - Anonymous nodes
  - «Smart contracts» (Solidity)
DIFFERENT TYPES OF BLOCKCHAIN

• **Permissionless (public) blockchain**
  anyone in the world can read, send transactions to and expect to see them included if they are valid, can participate in the consensus process

• **Permissioned (consortium / fully private ) blockchain**
  consensus process is controlled by a pre-selected set of nodes /one organization
  • Hyperledger
    • No crypto-currency
    • Registered nodes
    • «Chaincode» (GO, java)
DIFFERENT TYPES OF BLOCKCHAIN

- **Permissionless (public) blockchain**
  anyone in the world can read, send transactions to and expect to see them included if they are valid, can participate in the consensus process
  - Bitcoin
  - Ethereum

- **Permissioned (consortium / fully private ) blockchain**
  consensus process is controlled by a pre-selected set of nodes /one organization
  - Hyperledger

  Trade-off: the ability to create trust and the ability to scale
## BLOCKCHAIN FOR EMR

<table>
<thead>
<tr>
<th>EMR</th>
<th>Blockchain (permissioned)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private and sensitive</td>
<td>Secure and trusted</td>
</tr>
<tr>
<td>Can not be altered</td>
<td>Immutable</td>
</tr>
<tr>
<td>Audit trails needed: who accessed and reviewed</td>
<td>History kept on blockchain</td>
</tr>
<tr>
<td>Sharing needed among multiple actors</td>
<td>Distributed data sharing architecture</td>
</tr>
<tr>
<td>Fast turnaround for sharing</td>
<td>Quick (second to minute)</td>
</tr>
</tbody>
</table>
MANAGING ONCOLOGY DATA USING BLOCKCHAIN

• Oncology patients may require long term treatment and life-long monitoring.

• Diagnosis and treatment at multiple hospitals are common.

• Legislation requires signed patient consents for sharing data. Consent management may become complicated.
CHOICE OF TECHNOLOGY

• Permissionless (public) blockchain
  – Unnecessary expense of computer power
  – Transaction fee is a major hurdle for patients
  – Anonymity of nodes

• Permissioned (consortium) blockchain
  – Consensus process is controlled by a pre-selected set of nodes
  – Efficient
  – No transaction fee
EMR BLOCKCHAIN ARCHITECTURE
STRUCTURE OF THE DATA STORED IN THE CLOUD:

- **Cloud Server**
  - **Validating Node**: A, B, C, D, E
  - **Solution Users**: patients/doctors
  - **Solution Providers**: mobile/web app
  - **Auditors**: interrogate audit trails

**EMR Blockchain Network**
- Shared ledger
- Consensus

**HIPAA Compliant Cloud Storage**

**Data Categories**
- Clinical Data
- Doctor Id
- Data File

**Solution Users**
- patients/doctors
- record admin

**Solution Providers**
- mobile/web app
- Non-Validating Node

**Auditors**
- interrogate audit trails

**Membership Service**
- Reg. A
- ECA
- TCA
- TLS/CA

**The National Practitioner Data Bank**

**Validity of Data**

**Solution Users**
- patients/doctors

**Solution Providers**
- mobile/web app

**Auditors**
- interrogate audit trails

**Membership Service**
- Reg. A
- ECA
- TCA
- TLS/CA

**HIPAA Compliant Cloud Storage**

**Data File**
- Patient Private Data

**STRUCTURE OF THE DATA STORED IN THE CLOUD:**
EMR BLOCKCHAIN ARCHITECTURE

Solution Users
patients/doctors
(record admin)

Solution Provider
mobile/web app
Non-Validating Node

Auditors
interrogate
audit trails

EMR Blockchain Network
- Shared ledger
- Consensus

Validating Node D

Chaincode (smart contract): data sharing logic (key management, data operation, access control)

Validating Node E

Membership Service
- Reg. A
- ECA
- TCA
- TLS-CA

Registration authority: assign registration username/passwd pairs to participants
Enrollment CA: issue enrollment certificates to participants already registered
Transaction CA: issue transaction certificates to Ecert owners
TLS CA: issue certificates to systems that transmit message in a chain network

HIPAA Compliant
Cloud Storage

© HIMSS Europe GmbH
21.-22. September 2017
@eHealthSummit
STRUCTURE OF THE DATA STORED ON THE CHAINCODE:

- **State**
  - **Permission**
    - **Data Category**
    - Right (read/write/share)
    - From: To:
    - Timestamp
    - Study Id
    - Anonymity (y/n)
  - **Doctor Id**
  - **Clinical Metadata**
    - **Data Category**
  - **Metadata Item**
    - **Doctor Id**
    - Path To File
    - Hash(File)
    - Timestamp

- **Patient Id**
- **Permissions**
- **Doctor Id**

- **Patient Private Data (CC)**

**Chaincode**
- **Logic State**
- **Solution Users**
  - patients/doctors
  - Record admin
- **Solution Provider**
  - mobile/web app
  - Non-Validating Node
- **Auditors**
  -Interrogate audit trails

**EMR Blockchain Network**
- **Shared ledger**
- **Consensus**

**Membership Service**
- Reg. A
- ECA
- TCA
- TLS-CA

**HIPAA Compliant**
- Cloud Storage
- **The National Practitioner Data Bank**

© HIMSS Europe GmbH

21.-22. September 2017
@eHealthSummit
ADVANTAGES

• No single point of failure
  – Distributed and replicated
• No need to trust the network nodes
  – Only registered hospitals will participate
• Transparence and immutability
  – All transaction history preserved, forming audit trails
• Security and privacy
  – Enrollment, encryption, access control
WORKFLOW: SETUP

• Multiple hospitals setup an agreement to use the system and install the software

• A Web app is available for users

• Each hospital will have an admin role (virtual or real user) for retrieving EMR records

• Doctors in the hospital are registered through member service
  – A service based on the National Practitioner Bank to verify the identity
ROLES IN A TRANSACTION
 STATE OF THE ART

• **GemOS**: generic platform to create applications based on blockchain

• **Guardtime**: technology based on *KSI (Keyless signature infrastructure)*

• **MedREC**: *decentralized* system based on *public blockchain*
OPEN QUESTIONS

• No legal base
• Verification of the chaincode?
• Risks of the new technology (adoption?)
• Who controls Membership service?
• Key management
CONCLUSIONS AND FUTURE WORK

- Lack of secure and trustable sharing architecture harms the quality of patient care and increases cost
- Our solution using permissioned blockchain is the first work in this field
- Prototype ensures privacy, security, availability, and fine-grained access control over patients' data
- HyperLedger Fabric continues improving and we will improve the system based on latest release
- Next step will be testing across multiple hospitals with patients' data