Original Article

Healthc Inform Res. 2020 October;26(4):265-273.
https://doi.org/10.4258/hir.2020.26.4.265
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

Patient Consent Management by a Purpose-Based Consent Model for Electronic Health Record Based on Blockchain Technology

Dara Tith, Joong-Sun Lee, Hiroyuki Suzuki, W. M. A. B. Wijesundara, Naoko Taira, Takashi Obi, Nagaaki Ohyama

Institute of Innovative Research, Tokyo Institute of Technology, Yokohama, Japan

Objectives: Currently, patients' consent is essential to use their medical records for various purposes; however, most people give their consent using paper forms and have no control over it. Healthcare organizations also have difficulties in dealing with patient consent. The objective of this research is to develop a system for patients to manage their consent flexibly and for healthcare organizations to obtain patient consent efficiently for a variety of purposes. **Methods:** We introduce a new e-consent model, which uses a purpose-based access control scheme; it is implemented by a blockchain system using Hyperledger Fabric. All metadata of patient records, consents, and data access are written immutably on the blockchain and shared among participant organizations. We also created a blockchain chaincode that performs business logic managing patient consent. **Results:** We developed a prototype and checked business logics with the chaincode by validating doctors' data access with purpose-based consent of patients stored in the blockchain. The results demonstrate that our system provides a fine-grained way of handling medical staff's access requests with diverse intended purposes for accessing data. In addition, patients can create, update, and withdraw their consents in the blockchain. **Conclusions:** Our consent model is a solution for consent management both for patients and healthcare organizations. Our system, as a blockchain-based solution that provides high reliability and availability with transparency and traceability, is expected to be used not only for patient data sharing in hospitals, but also for data donation for biobank research purposes.

Keywords: Health Information Exchange, Electronic Health Records, Blockchain, Consent Forms, Access to Information

Submitted: June 14, 2020
Revised: August 9, 2020
Accepted: August 21, 2020

Corresponding Author
Joong-Sun Lee
Institute of Innovative Research, Tokyo Institute of Technology, 4259 Nagatsuta, Midori-ku, Yokohama, Kanagawa 226-8503, Japan. Tel: +81-0459245482, E-mail: j-lee@isl.titech.ac.jp (https://orcid.org/0000-0002-6976-6472)

I. Introduction

For the last decade, digital transformation has been an important development in all industries, and it is also happening rapidly in the healthcare field, bringing positive changes. Patient records are now more efficiently stored and transmitted. They can be effectively shared among hospitals where patient visits are logged through Electronic Health Record (EHR) systems, thus reducing the inconvenience and burden for patients. Stored patient data may be collected with the patient's permission to make a big data, which enables healthcare providers to analyze it and to offer personalized services. It is also expected to contribute to medical and

pharmaceutical research. However, before the sharing and use of patient data, it is mandatory to obtain patient consent.

In the context of healthcare information, consent [1] refers to patients' granting requestors access to their records stored in the health record system. Furthermore, in the context of healthcare professional and patient interaction, informed consent [2] refers to the voluntary agreement given by the patient before having a medical treatment. In any case, a patient's consent is essential, and traditionally, it has been given using paper-based [3-5] forms with the patient signature at the end. Once submitted, it is difficult for patients to change their decisions, which makes them cautious in signing papers, and they tend to be reluctant to share their data with others.

To address the above problem, various types of e-consent [6,7] have been introduced that allow patients to give consent electronically with their digital signatures and to withdraw it later if necessary. So far, most e-consent models are based on a centralized architecture, and some are built with trusted third-party delegation to evaluate patient consent and guarantee it [8]. There are also decentralized models that employ blockchain technology [9,10]. Among them, the Dwarna project [11] provides a well-designed web portal for dynamic consent that harnesses the blockchain ledger, which acts as a hub connecting participants in the biobank project.

Meanwhile, we introduce an important aspect of a data access control model, so-called purpose-based access control, which confines the usage of a patient's data to the prior intended purpose designated by the patient. Byun and his colleagues [12,13] proposed a model for relational databases, in which purpose information associated with the given data specifies the intended use of the data. Their proposed solution relies on the well-known role-based access-control (RBAC) model, in which data access permissions are assigned to functional roles within an organization that has a role hierarchy. Later, Kabir et al. [14] improved the model by suggesting conditional purpose-based access control for dynamic roles.

In this paper, we propose an e-consent system that has a fully decentralized architecture based on the blockchain. We adopt a purpose-based access control scheme adapted from RBAC model. The system enables patients to give their consent flexibly. In this work, there are two main contributions for the management of patient consent across different organizations: (1) allowing patients to manage their consent specifically by assigning their intended purpose of the use to each piece of data and (2) allowing healthcare organizations and research institutions to obtain patient records for future needs based on patients' consents.

We use a consortium blockchain platform, Hyperledger Fabric (HLF) [15,16], to build a secure channel in a network among participant healthcare organizations. Patient consent is written on the ledger of the blockchain along with the address of the patient's record, its metadata, as well as hash values of all the data, whereas patient records are stored off-chain in the relevant EHRs. However, the patient consent also can be stored off-chain along with the patient records. Malicious modification of the data on the blockchain is practically impossible, and the data integrity is preserved by comparing the hash value on the blockchain with that of the received one.

II. Methods

In this section, we explain the purpose-based access control scheme and how it is adapted for our patient consent model, including the way a data request is made in the model. Then, we briefly present blockchain and HLF, followed by our system concept and how it works.

1. Definition of Purpose

A purpose is defined as the reason for data collection and use [12]. It is the main keyword of a patient's consent, because the patient decides to confine the collection and use of their data within a certain range of a specified purpose. In that respect, purpose has its scope of coverage, narrow and wide, and it can be organized in a hierarchical tree structure, a so-called purpose-tree, as shown in Figure 1. The top node of the tree is the general purpose, which has the widest scope containing its descendant purpose nodes. Each connection line from one node to another represents their relationship in the purpose-tree. The purpose-tree represents the common goal of the organizations for exchanging data with each other. The purpose-tree is so closely related with the privacy policy that member organizations need to agree on its structure and attributes.

The purpose associated with data, regulating access to the data, is referred to as the "intended purpose", and the purpose for accessing data is referred to as the "access purpose" [12,13]. Usually, intended purpose is described in a patient consent in advance; it states the purpose for which the data can be accessed. Thus, when a requestor asks for access to data, they should clarify the access purpose, which is checked against the intended purpose of the data written in the patient consent. If the two purposes match, the system allows the requestor to access the data. The match-

 https://doi.org/10.4258/hir.2020.26.4.265

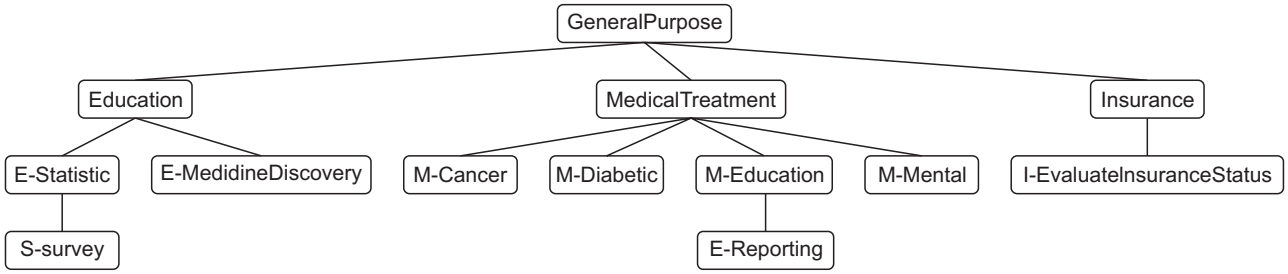

Figure 1. Example purpose-tree.

```
"GeneralPurpose": {
    "Education": {
        "E-Statistic": {
              "S-Survey":{}
        },
        "E-MedicineDiscovery":{}
      },
    "MedicalTreatment": {
        "M-Cancer":{},
        "M-Diabetic":{},
        "M-Education": {
              "E-Reporting":{}
        },
         "M-Mental":{}
      },
    "Insurance": {
        "I-EvaluateInsuranceStatus":{}
      }
  }
```

Figure 2. JSON array-type of the purpose-tree of Figure 1.

ing rule is provided by the consent model, which stipulates how the patient consent describes the intended-purpose and how a requestor prescribes an access request with the access purpose. In a general consent model, for instance, when a patient chose "MedicalTreatment" as the intended purpose for a data access, the system only allows requestors to access the data when their access-purpose matches with the intended-purpose, "MedicalTreatment" or its descendants in the purpose-tree. Figure 2 shows the purpose-tree of Figure 1 converted to a JSON array type stored in the blockchain.

2. Consent Model and Consent List

As previously mentioned, when a patient gives consent to usage of his or her data, it is confined within the specified intended purpose. In addition, patients usually give healthcare professionals different levels of permission according to their roles. In the RBAC model [14,17], the role represents the job function or job title in the organization, and it is defined in the role hierarchy. Access privilege is given based on the job title. It eases data owners to allow requestors data access based on the requestor's role rather than pointing to the user in the organization.

In our consent model, we adapt the purpose-based access control scheme and RBAC's concept. The patient consent in our model contains the intended-purpose of data access and the specific user's role. However, we do not use role hierarchy; rather, we make our model as simple and clear as possible with a generally acceptable structure. We modified the intended-purpose-based model of Byun and his colleagues [12,13].

The data access control in our consent model adopts basically whitelisting with an exception that the patient can make some designated blacklists within a whitelist. The consent model and rules are presented in Table 1.

To respond to various demands for data access from diverse requestors, a patient can make a list of consents for the data. The patient consent list is made by binding together multiple consents in combination with a variety of roles and intended purposes. If an access request matches one of the consents in the list, the data access is allowed. Figure 3 shows a simple example. In our system, a consent is stored in a blockchain with its hash value and the metadata of the relevant patient records. However, it also can be stored off-chain along with the patient records.

3. Access Request

When a requestor asks for data access, he or she must possess proper qualification and must state an appropriate purpose for the access. After the requestor's role and the access purpose are validated successfully, the system allows the access within the designated activity on the data.

Actually, when a requestor tries to obtain some patient data for any purpose, he or she sends the system a query having data attributes for a data search together with the access request and additional helpful keywords. The data attributes and the keywords include patient-related information, hospital, department, doctor, disease, time and date, demography, and so forth. After obtaining the target list, the system starts to validate the access request with the patient consent

Table 1. Consent model and its rules

Consent model	Rules
Each consent consists of four main tuples expressed as follows: **<Role; AdmitteeIds; Action; Intended-Purpose>** - **Role:** Job title or job function of requestor who has their specific eID (it is id of Enrolment certificate and explained in section 5). Examples are Cardiologist, Physician, etc. - **DoctorID:** Patient can add some designated doctors or healthcare professionals such as family doctor or medical specialist etc., who are allowed to access to the patient data. Their eIDs are listed here, or this element may remain blank. - **Action:** The activity on the data. Examples are Copy, Read, etc. Actions can have access privilege levels, so that the privilege of Copy includes that of Read, and the opposite is not allowed, i.e., $Copy \supset Read$. - **Intended-Purpose:** This element consists of two tuples as follows: **<AIP; PDP>** where AIP is Allowed Intended Purpose and PDP is Prohibited Descendant Purpose. AIP contains PDP, as the former is the ancestor of the latter.	Role and DoctorID are basic qualifiers necessary to specify requestor's legitimacy. One of these two and the other two tuples should be simultaneously complied by the requestor, i.e., $(Role \vee DoctorID) \wedge Action \wedge IntendedPurpose$ A data access is allowed only for the AIP that are explicitly written in a patient consent for the data, making all the other purposes implicitly prohibited one. Multiple AIPs constitutes a whitelist, for which data access is allowed. If an AIP has descendant purposes in the purpose-tree, then all of the descendants are also allowed purposes, belonging to the whitelist except some specific ones. Some of descendants of an AIP can be as PDP, for which data access is not allowed, such that, $\exists\ PDP \in AIP$. Multiple PDPs under an AIP constitutes a blacklist (BlackList), consisting of a subset of the ancestor AIP, such that, $\forall\ PDP \in BlackList \subset AIP$. If a PDP has descendant purposes, then all of the descendants are also prohibited purposes without any exception, belonging to the BlackList, equally saying that there is no AIP that is a descendant of PDP, such that, $\forall\ AIP \notin PDP \subset AIP$. This rule brings about simplicity in our model.

```
"Consent": [
"consentId" : "#123",
  {
      "role": "nurse, physician",
      "action": "read",
      "intendedPurpose": "generalPurpose; M-Education, M-Mental"
  },
  {
      "role": "cardiologist, pharmacist",
      "action": "copy",
      "intendedPurpose": "generalPurpose; Education"
  },
  {
      "role": "health insurance staff",
      "admitteeIds": "#2",
      "action": "read",
      "intendedPurpose": "I-EvaluateInsuranceStatus; null"
  }
]
```

Figure 3. Simple example of a patient's consent for a specific data in the state database.

pertaining to each of the candidates. Table 2 shows the access request and validation rules.

Among the four main tuples in patient consent of our model, the requestor's role and eID are usually invariable, and they are registered in the system or the organization to which they belong. Thus, the access request contains only variable elements, access purpose and action. The requestor is authenticated by the system using the eID, and the re-

 https://doi.org/10.4258/hir.2020.26.4.265

Table 2. Access request model and validation rules

Access request model	Validation rules
In our system, the access request has simply two tuples **<Access-Purpose; Action>** - **Access-Purpose:** The data requestor's purpose of using the data - **Action:** The activity on the data. Examples are Copy, Read, etc., having access privilege levels the same as in the patient consent.	Whether a data access is allowed or not depends on the relationship between requestor's Access Purpose (AP) and Intended-Purpose in the patient consent. The following is basic compliance rule to which access request is subject. - If AP is included in Prohibited Descendant Purposes (PDP), the access request is rejected at all, i.e., $AP \notin PDP$ - Any of consent, which has Allowed Intended-Purposes (AIP) that is ancestor of AP, allows the access requests excluding PDP in the AIP, i.e. $AP \in AIP$ and $AP \notin PDP \subset AIP$

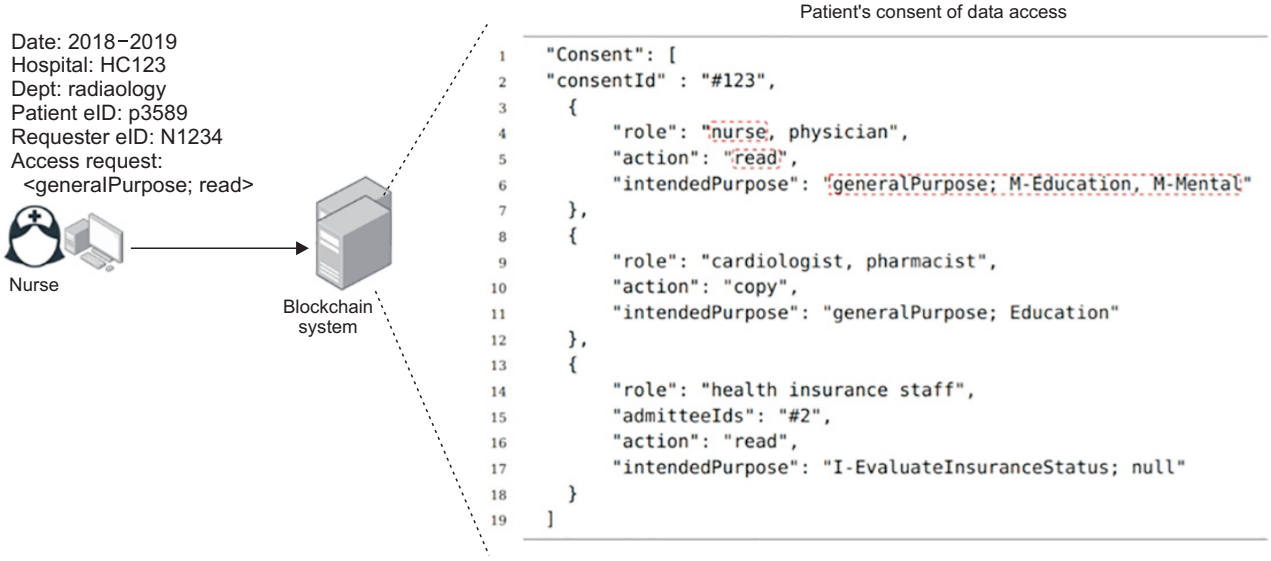

Figure 4. Validation of requestor's access request with patient's consent list.

questor's role is also identified by the system, which can consult participant organizations if necessary.

Figure 4 shows a case in which a nurse wants to read a patient's data, and submits an access request with data attributes and keywords for the query. The system produces a resultant list of data and then checks the patient consent pertaining to each piece of data in the list. If the access request matches with the patient consent, then the requestor can have access to the data and take action on the data. In this case, she can read data for general purposes, except education and mental illness-related purposes.

4. Blockchain Platform and System Conceptual Design

A blockchain is a group of blocks containing all the transactions in a designated network and shared among participants of the network. Each block is linked [18,19] to the next by its hash value stored in the next block as shown in Figure 5. This structure makes the blockchain immutable; if someone tries to alter certain data in a block, they must recalculate hash of the block with the forged data, continuing to the last block, and replace the blockchains of all other nodes with the forged one.

Blockchains are widely categorized into two types, public and private, the latter usually subdivided into consortium and private according to the purpose of use and features of members of the systems [20].

As the blockchain platform, we use HLF [16], which is a consortium blockchain in that all the participants are identified in the network of a consortium. The ledger of HLF consists of a world state database and a blockchain. The former contains the final state of variables of the program, so-called chaincodes, while the latter consists of all transactions that cannot be altered once written. HLF provides a membership service provider (MSP), which offers membership opera-

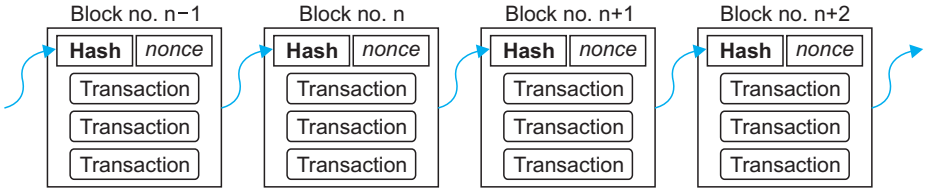

Figure 5. Typical structure of a blockchain.

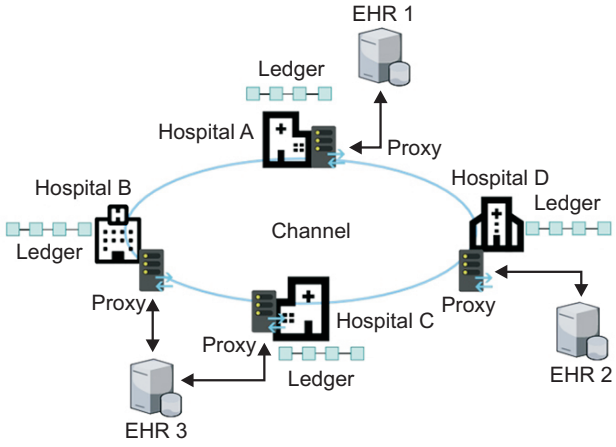

Figure 6. Channel of hospitals for exchanging patient records in an Electronic Health Record (EHR) system.

tions providing all cryptographic mechanisms and protocols behind issuing and validating enrolment certificates (ECerts and its ID called eID) of users and user authentication with the local certificate authority (CA). HLF also provides three main user roles, client, endorser, and orderer. Each endorser invokes the chaincode to endorse a tentative transaction, a so-called proposal, after validating it. An orderer wraps endorsed proposals into a block and distributes it among peers to append in the blockchain [16].

We adapt the same system design to our previous research [21] as shown in Figure 6. It has a channel that is built for exchanging patient records among participant hospitals, which are connected to independent EHR systems. Each member must have an ECert issued by the membership service provider, and its ID is used as the member's ID in the system, which stores the user's role. If not, it can consult the participant hospitals. Each proxy of a hospital communicates with other hospitals and is involved in proxy re-encryption to protect patient data.

5. Procedure of Chaincode

A chaincode is a program that performs business logic agreed by members of the network; it works in the same way as a smart contract in Ethereum. It is run by endorsers to access a blockchain through transactions [16]. We created a chaincode to handle patient consent. The following describes the chaincode's operations.

1) Consent management

This function manages patient consent, allowing a patient to make a query for past records, review the consent and update it in a blockchain as shown in Figure 7. First, it checks the validity of the proposal's format and intended purpose with the purpose-tree. Then, it queries for the consent policies and medical record transactions in the blockchain based on the patient's eID. The patient can update his or her consents by appending new ones to the relevant medical record transactions.

2) Consent check

This function checks a requestor's access request with the patient's consent stored in the blockchain as shown in Figure 8. After extracting the proposal, it checks the validity of the proposal's format and the requestor's role in the organization. Then, it queries for transactions in the blockchain based on searching keywords in the proposal. After querying successfully, the chaincode compares entities of access request in the proposal with attributes of the patient's consent in the transactions. Finally, the chaincode only sends transactions for which the patient's consents match the access request. As previously mentioned, transactions in a blockchain contain records' URLs in EHR systems, which are used to identify the location of patient medical data.

III. Results

1. Prototype System

We built a prototype system in a local network with four Linux PCs to provide a user interface to patients and doctors who made and sent requests to the blockchain system. Four endorser peers were made in the PCs, which invoked chaincodes in the Docker (https://www.docker.com/), where the HLF platform was installed. In addition, MSPs of HLF were installed in two of the PCs separately.

https://doi.org/10.4258/hir.2020.26.4.265

```
Input: PatientProposal /* It has "eID" of patient and the "NewConsent"                    */
Output: Message /* of successful or unsuccessful of creating or updating the "Newconsent" */
1  Function ConsentActivities(PatientProposal):
2      if PatientProposal format is correct then
3          Query in the blockchain for patient's record transactions based on eID, then store
           these query results to the array of RecordTransaction
4          if Patient selects a transaction from the array of RecordTransaction then
5              if Patient wants to upload a Newconsent of the selected transaction then
6                  Append the Newconsent to the selected transaction
7                  Return Message
8              else if Patient wants to update a consent in the selected transaction then
9                  Deactivate the old consent
10                 Append the Newconsent to the selected transaction
11                 Return Message
```

Figure 7. Pseudocode of a part of a chaincode for patient consent management.

```
Input: PatientRecordTx, AccessRequest
/* PatientRecordTx is the transaction of patient's records, which the doctor received after he
   queries in blockchain using keywords                                                    */
/* AccessRequest is a request of the doctor, which contains "Action" and "AccessPurpose"   */
Output: RecordURL, RecordMetaData
1  Function ConsentChecked(PatientRecordTx, AccessRequest):
2      Query in the blockchain for doctor's role
3      Compare attributes of patient's consent of each PatientRecordTx with the doctor's role
       and the AccessRequest; if a consent of PatientRecordTx is matched with AccessRequest
       and the doctor's role then
4          Return the RecordURL and RecordMetaData of that PatientRecordTx
```

Figure 8. Pseudocode of a part of a chaincode for patient consent check.

2. Prototype Analysis

We evaluated the prototype system with the following targets: (1) to check the integrity of data of history, which included creating, withdrawing, and updating patient consent; (2) to check the chaincode's function of validation of the provided intended purpose and access-purpose with the purpose-tree; and (3) to investigate whether the chaincode worked correctly in validating the access request of a doctor with the patient's consent for data access.

We could identify a peer that had a wrong blockchain because it was intentionally provided with wrong query results. During the process of building a block, the consensus protocol of HLF can check it by comparing results from all endorser peers. The processing time required to validate an access request depended on the complexity and length of the purpose-tree and the consent list in the individual transaction. Simultaneously, the speed of validating the proposal is based on the privacy policies and the legal requirements set by the consortium.

IV. Discussion

The patient's consent plays a crucial role in preserving the patient's privacy in healthcare data sharing. If restrictively given, it would cause inconvenience in dealing with the data, while indulgently given, patients would be exposed to the risk of privacy disclosure. Accordingly, patients want to monitor how their data is used based on their consent. Without appropriate measures, they tend to be inactive in data sharing and even reluctant to provide data for research purposes.

In this paper, we proposed a new type of e-consent system

for patients to manage consent elaborately in dealing with their data. We adopted the purpose-based access control scheme from the RBAC model of a relational database [12-14]. Our system also has a hierarchical structure of the user's intended purposes, but it does not have a hierarchical structure for user roles; combining both hierarchical structures makes consent too complicated for patient to understand when they apply it to their data. RBAC, from its name, is role-based and hospital-centric, whereas our concept is patient-centric.

Our system is different from most purpose-based centralized systems, in that ours is a fully decentralized blockchain approach. The Dwarna project [11] also provides a blockchain solution for dynamic consent in biobanking; however, they use boolean-based consent to allow requestors to access data because the purpose is very simple in their research.

To share data among multiple organizations, participants must reach an agreement with a common privacy policy that might compromise each member's unique feature in their own policy. It may be desirable for the purpose-tree to cover all participants' usable purposes with plenty of branches in each node; however, it leads to complexity and reduction of data usability. To address these discrepancies, we tried to make the rules of our model simple and generally acceptable.

In reality, the purpose-tree could be updated by the agreement of participant organizations for some reason, such as when their privacy policy is updated or a new member organization is added. In such a case, it would be difficult to interpret patient's consent based on the new purpose-tree, so all the organizations would need to get new patient consents again. However, the contract with a patient can prepare in advance a description of how to deal with this kind of situation.

The European General Data Protection Regulation (GDPR) [22,23] states that data subjects, i.e., patients, have the right to request the erasure of personal data related to them, the so-called right of erasure. Apparently, this is considered incompatible with the blockchain's immutability, so it is a big challenge for all blockchain-based systems to comply with this type of request. To address this difficult problem, our system stores patient records off-chain in EHRs. In addition, it makes each transaction on-chain have a unique hash number of the patient's eID with a random number, a so-called salt [21,24], to thoroughly pseudonymize the data owner, even though this sacrifices data searching performance. The link that connects the randomized patient eID to off-chain records resides in the off-chain database [11], and in case a patient asks for his or her data to be erased, the system removes the link and off-chain record. The URL written in the transaction, which is the address of the data site in the EHR, might be a clue to specify the patient; however, it is very difficult to do that because the URL is shared with many other patients. The patient consent may be stored off-chain along with the patient record, and the hash remains on-chain to maintain the integrity.

Our system has high reliability and availability as well as transparency and traceability, which are common prominent features of the blockchain system. Transparency and traceability are considered especially important in dealing with patient consent to ensure that patient data is shared properly. We expect that our system can be used as a solution not only in patient data sharing between hospitals, but also in data donation for research purposes in biobanking.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

ORCID

Dara Tith (http://orcid.org/0000-0003-4372-7640)
Joong-Sun Lee (http://orcid.org/0000-0002-6976-6472)
Hiroyuki Suzuki (http://orcid.org/0000-0002-5028-5388)
W. M. A. B. Wijesundara (http://orcid.org/0000-0002-7228-524X)
Naoko Taira (http://orcid.org/0000-0001-6169-8957)
Takashi Obi (http://orcid.org/0000-0001-9430-2728)
Nagaaki Ohyama (http://orcid.org/0000-0002-4297-2575)

References

1. World Health Organization, Council for International Organizations of Medical Sciences. International ethical guidelines for health-related research involving humans. Geneva, Switzerland: Council for International Organizations of Medical Sciences; 2017.
2. World Medical Association. World Medical Association Declaration of Helsinki: ethical principles for medical research involving human subjects. JAMA 2013;310(20):2191-4.
3. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic Consent: a patient interface for twenty-first century research networks. Eur J Hum Genet 2015;23(2):141-6.
4. Budin-Ljosne I, Teare HJ, Kaye J, Beck S, Bentzen HB, Caenazzo L, et al. Dynamic Consent: a potential solu-

 https://doi.org/10.4258/hir.2020.26.4.265

tion to some of the challenges of modern biomedical research. BMC Med Ethics 2017;18(1):4.
5. Albanese G, Calbimonte JP, Schumacher M, Calvaresi D. Dynamic consent management for clinical trials via private blockchain technology. J Ambient Intell Humaniz Comput 2020 Feb 14 [Epub]. https://doi.org/10.1007/s12652-020-01761-1.
6. Coiera E, Clarke R. e-Consent: the design and implementation of consumer consent mechanisms in an electronic environment. J Am Med Inform Assoc 2004;11(2):129-40.
7. Wuyts K, Scandariato R, Verhenneman G, Joosen W. Integrating patient consent in e-health access control. Int J Secur Softw Eng 2011;2(2):1-24.
8. Asghar MR, Russello G. Flexible and dynamic consent-capturing. In: Camenisch J, Kesdogan D, editors. Open problems in network security. Heidelberg, Germany: Springer: 2011. p. 119-31.
9. Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality. Trials 2017;18(1):335.
10. Rantos K, Drosatos G, Kritsas A, Ilioudis C, Papanikolaou A, Filippidis AP. A blockchain-based platform for consent management of personal data processing in the IoT ecosystem. Secur Commun Netw 2019;2019:1431578.
11. Mamo N, Martin GM, Desira M, Ellul B, Ebejer JP. Dwarna: a blockchain solution for dynamic consent in biobanking. Eur J Hum Genet 2020;28(5):609-26.
12. Byun JW, Li N. Purpose based access control for privacy protection in relational database systems. VLDB J 2008;17(4):603-19.
13. Byun JW, Bertino E, Li N. Purpose based access control of complex data for privacy protection. Proceedings of the 10th ACM Symposium on Access Control Models and Technologies; 2005 Jun 1-3; Stockholm, Sweden. p. 102-10.
14. Kabir ME, Wang H, Bertino E. A conditional purpose-based access control model with dynamic roles. Expert Syst Appl 2011;38(3):1482-9.
15. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al. Hyperledger Fabric: a distributed operating system for permissioned blockchains. Proceedings of the 13th EuroSys Conference; 2018 Apr 23-26; Porto, Portugal. p. 1-15.
16. Hyperledger. What is Hyperledger Fabric [Internet]. Dublin, Ireland: Hyperledge; c2020 [cited at 2020 Sep 15]. Available from: https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html.
17. Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. Computer 1996;29(2):38-47.
18. Zhang R, George A, Kim J, Johnson V, Ramesh B. Benefits of blockchain initiatives for value-based care: proposed framework. J Med Internet Res 2019;21(9):e13595.
19. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Bitcoin.org; 2008 [cited at 2020 Sep 15]. Available from: https://bitcoin.org/en/bitcoin-paper.
20. Viriyasitavat W, Hoonsopon D. Blockchain characteristics and consensus in modern business processes. J Ind Inf Integr 2019;13:32-9.
21. Tith D, Lee JS, Suzuki H, Wijesundara WM, Taira N, Obi T, et al. Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthc Inform Res 2020;26(1):3-12.
22. Truong NB, Sun K, Lee GM, Guo Y. GDPR-compliant personal data management: a blockchain-based solution. IEEE Trans Inf Forensic Secur 2019;15:1746-61.
23. General Data Protection Regulation. Art. 17 GDPR: Right to erasure ('right to be forgotten') [Internet]. Brussel, Belgium: European Union; c2020 [cited at 2020 Sep 15]. Available from: https://gdpr.eu/article-17-right-to-be-forgotten/.
24. Gauravaram P. Security analysis of salt||password hashes. Proceedings of 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT); 2012 Nov 26-28; Kuala Lumpur, Malaysia. p. 25-30.