Coded Dynamic Consent framework using blockchain for healthcare information exchange

1st Ah Ra Lee
School of Computer Science&Engineering
College of IT Engineering
Kyungpook National University
Daegu, Republic of Korea
eara0367@gmail.com

2nd Min Gyu Kim
Qucell Networks Co., Ltd.
Seoul, Republic of Korea
mingyu3317@gmail.com

3rd Kyung Jae Won
School of Computer Science&Engineering
College of IT Engineering
Kyungpook National University
Daegu, Republic of Korea
yui06031@gmail.com

4th Il Kon Kim
School of Computer Science&Engineering
College of IT Engineering
Kyungpook National University
Daegu, Republic of Korea
ikkim@knu.ac.kr

5th Eunjoo Lee
College of Nursing
Kyungpook National University
Daegu, Republic of Korea
jewelee@knu.ac.kr

2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM) 978-1-7281-6215-7/20/$31.00 ©2020 IEEE DOI: 10.1109/BIBM49941.2020.9313330

***Abstract*—As personalized digital healthcare is attracting attention, recognition of data sovereignty has been essential in healthcare data exchange. Dynamic consent is a new approach that patients enable to tailor and manage their consent. It expands patients' autonomy by giving the right to intervene in the healthcare data exchange process. This study proposes a Coded Dynamic Consent framework based on blockchain. We developed five design criteria to support dynamic consent and represent consent preferences as a coded format. The framework ensures data sovereignty and autonomy of a data provider so that patient-centered healthcare data exchange environment could be achieved.**

***Index Terms*—dynamic consent, data sovereignty, blockchain, patient-centered healthcare, healthcare information exchange**

I. Introduction

With the advent of digital healthcare, there has been growing interest in the use of personal health records [1-4]. To efficiently and effectively use big healthcare data scattered in multiple places, a patient-centered data exchange environment with a consent system that guarantees data sovereignty is essential. Several studies on the consent system define various consent types, including future consent, broad consent, and informed consent [5-7]. However, there is no way to guarantee data sovereignty with these consent types. The patient cannot remember all the history of where and what data they provided, so it is challenging to request a change or withdraw the contract.

This research was supported by a grant of the Korea Health Technology R&D Project through the Korea Health Industry Development Institute(KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea(HI19C0808).

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2019R1I1A3A01058112) & (NRF-2019R1l1A3A01060579) & (NRF-2018R1A6A1A03025109)

For this reason, the need for dynamic consent has been drawing more attention as a possible solution to the problem [8]. The dynamic consent provides data providers with a choice to actively intervene in the healthcare data exchange process. Patients could be not only data providers but also health service customers. It supports various consent types, interactions within data providers and consumers, and data use history management. Data providers can freely request at any time a change in their contract according to their preference. Moreover, they can set whether to allow data consumers for secondary use, whether to receive the new information derived from provided data and how to receive it. The dynamic consent gives more controlling power to data providers over their data usage. While giving choices has the advantage of ensuring autonomy, it is considered difficult or cumbersome. Some people prefer broad consent that gives only rough information about their data usage [9].

In this study, we propose a Coded Dynamic Consent (CDC) Framework. We aim to establish a patient-centered healthcare data exchange environment. The CDC framework adopts dynamic consent to guarantee data sovereignty, and it supports a tailored consent system that reflects preferences and health literacy of data providers. The CDC framework ensures autonomy of data providers. Of course, it also provides the possibility to take advantage of the broad consent system for those who feel inconvenient to making many choices. We use blockchain and smart contract to implement the CDC framework. The data providers and institutions participate in the blockchain network and sign a contract related to data use. The result of the contract is coded in a standardized format and stored in the blockchain. The integrity and transparency of consent history can be ensured by storing the consent code in the blockchain network.

II. Related Work

Most previous studies focused on the organization-centered way. As a result, patients do not have complete control over their data. The previous consent system was static, and it is nothing but to get one ultimate consent from data providers so that the system does not have to ask for another. Also, it lacks comprehensive management for data use history, making it difficult for data providers to change or withdraw the contract after the initial consent. A few studies have implemented blockchain-based dynamic consent system to encourage patients' participation in the healthcare data exchange process [10-12]. Unlike the previous studies, we designed a code for dynamic consent with data sovereignty. To the best of our knowledge, previous blockchain-based consent systems do not use the coded format. Using code has advantages in standardizing contract contents, facilitating identification and managing data use history. In addition, previous studies only supported a part of dynamic consent, such as withdrawal of consent. In contrast, to fully establish dynamic consent, the CDC framework includes additional dynamic factors such as delegation of authority and providing derived information.

III. Method

The Coded Dynamic Consent (CDC) framework adopts a dynamic consent system. Previous studies on dynamic consent have limitations since they partially include dynamic factors. Five design goals are selected to support fully dynamic consent. The key idea of this study is a code that makes a contract into a standardized and machine-readable format. We developed a dynamic consent code so that data providers could deliver their detailed consent preference, in terms of data provision, to data consumers. The code is transparently stored as an attribute of digital assets in the blockchain network.

A. Design goals for dynamic consent

The CDC framework aims to have a fully dynamic consent feature. Five design goals are selected which define a fully dynamic consent model [13].

- **DG1. (Different consent type)** Does it support various consent types, including broad consent from traditional consent systems and specific consent?
- **DG2. (Change consent preference)** Can a data provider change the settings for consent in real-time according to changing circumstances and preferences?
- **DG3. (Transparent history management)** Can a person's consent history related to consent, such as details of data provision and changes in consent setting, be managed comprehensively and transparently?
- **DG4. (Same data reuse)** Does it provide consent methods which allows data consumers to reuse the same data, such as automatic consent for further use in similar studies?
- **DG5. (Providing information)** Does it deliver new information which derived from one's data provision to the data provider? Is it possible for the subject to set how to receive such information?

In a dynamic consent system, data providers and data consumers interact based on digital interfaces. In traditional paper-based consent, a data consumer must have met a data provider face-to-face to get consent. Also, the system's ability to manage data use history was not so effective. The digital interface has the advantage of being easier to manage and eliminating unnecessary obstacle in the consent process. However, it may be difficult for generations unfamiliar with digital devices to use the system. The CDC framework provides delegation of authority feature so that even people who are not accustomed to digital services can use the dynamic consent system. Through the feature, they can express their consent with help from others, such as family or caregivers.

B. Dynamic Consent Code System

The key idea of our CDC framework is the dynamic consent code. Data provision contract is performed electronically via two-way communication based on digital interfaces. The dynamic consent code can show the contract process in the machine-readable format, and its purpose is to present consent preferences or contract process in a standardized format. The code can arrange, identify, and classify a variety of consent types. The contract between a data provider and a data consumer is performed using smart contracts. The dynamic consent code can be used to show the contract related to data provision. The code satisfies dynamic factors, including the five design goals above. Ultimately, eight characteristics represent the dynamic consent code: Consent, Extension, Authority, Withdrawal, Modify, Reuse, Information, and Notification. The code consists of a mnemonic alphabet and two digits sequence code. The mnemonic field is from the first alphabets of eight characteristics. And the two digits field represents possible options for each characteristic.

- **C (Consent).** It represents what type of consent to be used. There are various consent types, and appropriate types are needed according to the preferences of data providers and consumers.
- **E (Extension).** It indicates whether the contract can be extended. In some cases, a data provider could receive a re-approval request to extend contract expiration date. The CDC framework provides automatically extend options of re-approval. It would be convenient for people who are willing to provide their data until an unspecified period and feel annoyed to give consent repeatedly.
- **A (Authority).** It is related to the authority delegation regarding data consent. If a data provider is unable to agree, the right to consent can be delegated to a family, caregivers, or institutions. It can be used for those who are unfamiliar with digital interfaces.
- **W (Withdrawal).** It represents whether the withdrawal request can be made. There could be a situation which is impossible for a data provider to withdrawal. For instance, if a research institution has already utilized provided data, the withdrawal cannot have an impact. To inform the risk of unable to withdrawal, the CDC supports the withdrawal option before providing data.

- **M (Modify).** It shows whether the modification request of consent terms can be made.
- **R (Reuse).** Reuse field is related to the secondary use of provided data. Suppose another data consumer wants to reuse already provided data within the scope that the data provider agreed before, such as the similar purpose of use. In that case, the data request can be automatically accepted without waiting for consent from the provider.
- **I (Information).** Data providers can choose whether to receive new information derived from the provided data. The provider also could choose the channel to receive such information, for example e-mail or text message.
- **N (Notification).** The field contains information related to the notification of data use. A data provider can also set the frequency to receive notifications.

C. Data Model

The CDC framework has two digital assets, profile and consent block. The CDC framework manages consent using codes which show consent preference and contract process. The profile block is created at user's first time using the framework and stores basic settings. The dynamic consent code is generated based on the answers from the data provider. The consent process can be made whenever a data consumer requests for some data or automatically with specified scope in the profile block for those who are annoyed to consent each time of data provision. The dynamic consent code can be updated according to one's preference and health literacy.

The consent block consists of contract information as shown in Table. I. It also represents a contract process between data providers and consumers. Fig. 1 shows the state transition diagram of the consent block. When a data consumer requests data, a new consent block is created. It can be updated by the interaction between data providers and consumers. All transactions on the blockchain network are recorded transparently, thus supporting reliable management of consent history. Healthcare data includes sensitive personal information. To address privacy concerns, the consent block contains no critical information about the data and stores only the identifier of the metadata. Therefore, it is impossible to know what kind of data is provided by checking the consent block alone.

TABLE I
CONSENT BLOCK ATTRIBUTES

Name	Description
consentId	Consent block identifier
patientId	Patient identifier
institution	Data consumer identifier
metadataId	Metadata identifier
creationTime	The time of consent block created
consentCode	The value of dynamic consent code
status	The status of consent process
expiredDate	(optional) The maturity of data use
uri	(optional) Reference address to contract documents
token	(optional) Access token to data storage
updateTime	(optional) The time of consent block updated

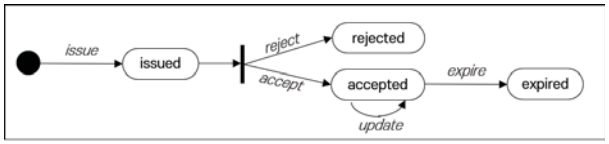

Fig. 1. consent

The CDC framework supports access control based on consent. It issues a token after acquiring a data provider's consent and stores the token in the consent block. The data consumer should access the data with this token. When the data consumer requests data, token validation could be requested to the CDC framework. As the token is stored in the consent block, the integrity of the token is ensured.

IV. RESULT

We applied our CDC framework to the healthcare data-sharing platform, SHAREChain [14]. In SHAREChain, the original data is stored in a repository, and Blockchain-registry stores the metadata of original data. Suppose a patient who has been living in an elderly care facility is hospitalized. The hospital needs different types of data to treat the patient. Therefore, the hospital would likely request patient records from the facility to check the patient's medical history. When the hospital requests data, a consent block is created. The patient and the hospital electronically sign a contract allowing the hospital to use the patient's data. As the data provision process progresses, the fields of the consent block are updated, and the related transactions are transparently recorded in the blockchain network. If the patient agrees to that request, an access token is issued. It is passed to the consumer and stored in the consent block. The integrity of the access token is ensured by storing it in the blockchain. Those who have a valid token can access to the data. After validating the token, the data can be shared with the hospital. Fig. 2 shows the process of requesting data and receiving the token.

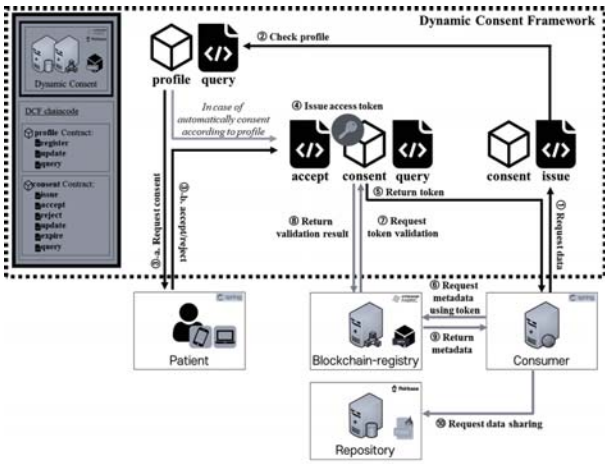

Fig. 2. Consent process using CDC framework in SHAREChain

V. Discussion

For a patient-centered healthcare data exchange environment, data sovereignty is essential. Traditional consent systems have raised diverse issues. As a remedy to the problem, dynamic consent has been discussed to enhance patients' autonomy in managing their own data. However, as more options are available, people with low health literacy may feel overwhelmed by too many consent options. The CDC framework ensures data sovereignty by providing autonomy via various consent types, including traditional consent methods. In addition, breaking away from hierarchical medical requests between large medical institutions and general hospitals, all the institutions form a mesh with a horizontal blockchain network. The data exchange takes place under the control of a patient, not an organization-centered way. The contract is conducted electronically, and the result is coded and stored in the blockchain. The blockchain-based dynamic consent system ensures the integrity of the contract contents and the transparency of the consent history.

To evaluate our CDC framework, we compared with the previous studies. Table. II shows the comparison results based on the dynamic consent system design goals defined above. There are three points in which the CDC framework is distinguished from others. The first is the code. In the CDC framework, contract contents are presented as codes and stored in the blockchain. The code facilitates management and identification of consent. Moreover, the code is possible to detect its own errors, such as finding missing values before data is stored. The second point is the delegation of authority. The dynamic consent system enables two-way communication between data providers and consumers based on digital interfaces rather than face-to-face. In this case, people who are unfamiliar with digital services may have difficulty in using the dynamic consent system. The CDC framework provides a function to delegate consent authority. By delegating consent authority to family members, guardians, or nursing homes, it can be used by people who are not accustomed to digital interfaces. Finally, it offers options for receiving new information derived from previously provided data. To effectively utilize big healthcare data, a patient-centered healthcare information exchange environment should be established. For this, the participation of data providers is essential. It needs to benefit data providers for increasing engagement. The CDC framework supports options utilizing derived information that can be used for personal healthcare management.

TABLE II
Qualitative evaluation with dynamic consent design goals

Criteria	**[10]**	**[11]**	**[12]**	CDC
C1. Different consent type	N	N	N	Y
C2. Change consent preference	Y	Y	Y	Y
C3. Transparent history management	Y	Y	Y	Y
C4. Same data reuse	N	N	N	Y
C5. Providing information	N	N	N	Y

As future works, we plan to apply our CDC framework to an actual environment and to check its practicality. As the outlook for personalized digital healthcare is bright, we believe much progress will be done in data sovereignty and dynamic consent system.

VI. Conclusion

This study proposed a Coded Dynamic Consent(CDC) framework which guarantees data sovereignty in healthcare data exchange. Five design goals are selected to support fully dynamic consent, and qualitative evaluation is conducted according to the criteria. The key point of the CDC framework is a dynamic consent code. It is developed to integrate dynamic factors, including five design goals. Dynamic consent is based on digital interfaces. Therefore, representing consent preferences and contract processes to machine-readable code is an effective way to manage consent information. The CDC framework proposed in this study can be used with healthcare information exchange systems that need to ensure data sovereignty.

References

[1] W. Duan et al., "How great is the medical burden of disease on the aged? Research based on "System of Health Account 2011"", Health and Quality of Life Outcomes, vol. 15, no. 1, 2017.

[2] S. Wang, M. Petzold, J. Cao, Y. Zhang and W. Wang, "Direct Medical Costs of Hospitalizations for Cardiovascular Diseases in Shanghai, China", Medicine, vol. 94, no. 20, p. e837, 2015.

[3] K. Abouelmehdi, A. Beni-Hessane and H. Khaloufi, "Big healthcare data: preserving security and privacy", Journal of Big Data, vol. 5, no. 1, 2018.

[4] V. Palanisamy and R. Thirunavukarasu, "Implications of big data analytics in developing healthcare frameworks – A review", Journal of King Saud University - Computer and Information Sciences, vol. 31, no. 4, pp. 415-425, 2019.

[5] C. McGowan, C. Houlihan, P. Kingori and J. Glynn, "The Acceptability of Online Consent in a Self-Test Serosurvey of Responders to the 2014–2016 West African Ebola Outbreak", Public Health Ethics, vol. 11, no. 2, pp. 201-212, 2017.

[6] B. Hofmann, "Broadening consent–and diluting ethics?", Journal of Medical Ethics, vol. 35, no. 2, pp. 125-129, 2009.

[7] P. Singleton and M. Wadsworth, "Consent for the use of personal medical data in research", BMJ, vol. 333, no. 7561, pp. 255-258, 2006.

[8] I. Budin-Ljøsne et al., "Dynamic Consent: a potential solution to some of the challenges of modern biomedical research", BMC Medical Ethics, vol. 18, no. 1, 2017. A

[9] C. Grady et al., "Broad Consent for Research With Biological Samples: Workshop Conclusions", The American Journal of Bioethics, vol. 15, no. 9, pp. 34-42, 2015.

[10] G. Albanese, J. Calbimonte, M. Schumacher and D. Calvaresi, "Dynamic consent management for clinical trials via private blockchain technology", Journal of Ambient Intelligence and Humanized Computing, 2020.

[11] G. Despotou, J. Evans, W. Nash, A. Eavis, T. Robbins and T. Arvanitis, "Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the Dovetail digital consent application: A cross sectional exploratory study", DIGITAL HEALTH, vol. 6, p. 205520762092494, 2020.

[12] Tharuka Rupasinghe, Frada Burstein, Carsten Rudolph, "Blockchain based Dynamic Patient Consent: A Privacy-Preserving Data Acquisition Architecture for Clinical Data Analytics", ICIS 2019 Proceedings, 2019.

[13] J. Kaye, E. Whitley, D. Lund, M. Morrison, H. Teare and K. Melham, "Dynamic consent: a patient interface for twenty-first century research networks", European Journal of Human Genetics, vol. 23, no. 2, pp. 141-146, 2014.

[14] A. Lee, M. Kim and I. Kim, "SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR", 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2019.