AMCIS 2022 Proceedings

SIG Health - Healthcare Informatics and Health Info Technology

Aug 10th, 12:00 AM

Patient Consent for Health Information Exchange: Blockchain-driven Innovation

Chad Anderson
Miami University, ander556@miamioh.edu

Arthur Carvalho
Miami University, arthur.carvalho@miamioh.edu

Jeffrey Merhout
Miami University, jmerhout@acm.org

Recommended Citation

Anderson, Chad; Carvalho, Arthur; and Merhout, Jeffrey, "Patient Consent for Health Information Exchange: Blockchain-driven Innovation" (2022). *AMCIS 2022 Proceedings*. 12.
https://aisel.aisnet.org/amcis2022/sig_health/sig_health/12

Patient Consent for Health Information Exchange: Blockchain-driven Innovation

Completed Research

Chad Anderson
Miami University
chad.anderson@miamioh.edu

Arthur Carvalho
Miami University
arthur.carvalho@miamioh.edu

Jeffrey W. Merhout
Miami University
jmerhout@miamioh.edu

Abstract

Health information exchange (HIE) is vital to improving care delivery and outcomes, and patient consent is an important component of HIE. Existing consent processes that involve completing forms at a provider, along with poor interoperability between HIEs, give patients limited control of their consent management. We developed and deployed a survey to assess how people perceive the value of HIE, the importance of controlling access to their protected health information (PHI), and how they would prefer to manage consent for the exchange of their PHI. Given the option, 70% of the participants would prefer to use a consent application (app) to manage their consent. Based on the current U.S. HIE environment, we argue that the most viable architecture for implementing an HIE consent app would be a permissioned blockchain. We describe and illustrate a consent management app prototype that is blockchain-based as an effective alternative to current HIE consent practices.

Keywords

Patient consent, health information exchange, blockchain.

Introduction

The issue of a patient's right to control who has access to their protected health information predates the widespread adoption of electronic health records (EHRs) that occurred in the 2010s as a response to the 2009 HITECH Act (Bergmann et al., 2007; Simon et al., 2009). However, the resulting digitalization of most patient records in the U.S. and the increased development of health information exchanges to enhance sharing of those digital records have made that issue more salient today (Apathy and Holmgren, 2020). Historically, sharing PHI between healthcare organizations was limited to mailing or couriering paper records, faxing documents, or sending direct electronic messages from one organization to another. What an HIE adds is both the ability to set up automated PHI sharing between EHRs (i.e., directed exchange) and for participating organizations to query the HIE for information on a patient without having to request that information from the organization(s) that created it (i.e., query-based exchange) (Esmaeilzadeh and Mirzaei, 2018). This increased access to PHI can improve care and reduce costs (Adjerid et al., 2016; Menachemi et al., 2018), but it depends, in part, on patient's consent to share their PHI, which requires both trust in sharing entities and the opportunity to make informed consent decisions (Marchesini and Pritts, 2013).

Through initiatives that included HITECH funding for each state to develop HIE (ONC, 2019), the U.S. now has a more robust HIE infrastructure with the most extensive network, the eHealth Exchange, connecting 61 regional and state HIEs and working in 75% of all U.S. hospitals (Van Dyke, 2020). However, a fully integrated national HIE network is still just a future possibility hampered by, among other things (Everson et al., 2021), the fact that HIE regulation, including patient consent, is governed primarily at the state level through various laws and policies making a nationwide HIE infrastructure more challenging to establish (Apathy and Holmgren, 2020). The basis for state-level control of consent is that the primary federal law governing PHI, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, allows, but does not require, healthcare providers to give patients a choice as to whether their health information is disclosed to others for the purposes of treatment, payment, and health care operations (Office of Civil Rights, 2002). Therefore, the states get to decide whether to offer patients a consent option regarding the sharing of their PHI.

Consent options, when made available to patients, include opt-out, opt-in, and opt-in with "break the glass" structures (Kim et al., 2015). An opt-out structure allows the exchange of PHI unless the patient has explicitly withdrawn consent, while an opt-in structure stipulates that no PHI can be exchanged until the patient has consented to that exchange. The opt-in with the "break the glass" structure allows the exchange of PHI without consent, but only in an emergency. Because sharing under both emergency and non-emergency situations is the default, an opt-out structure is the most exchange-friendly option (Downing et al., 2016). States may set specific consent rules or leave consent to be based on individual provider policies. As of 2017, eight states (e.g., California, New York) had an opt-in structure, 20 (e.g., Arizona, Ohio) had an opt-out structure, and 22 (e.g., Indiana, New Jersey) had no state-level rule, instead ceding control of consent to providers (ONC, 2017).

Whatever consent structure exists in a given locality, the current process of documenting consent for HIE is managed by providers, primarily through consent forms that patients fill out when at a provider location. Completed consent forms are retained by the provider with consent status transmitted to other participants in the HIE by either sending a scan of the consent document with the transmitted PHI, using consent metatags in the PHI, or storing the consent status in a central database (e.g., on the HIE) for providers to query (ONC, 2018). A form-based process for documenting consent adds administrative costs for providers but also imposes time and opportunity costs on patients as they must travel to a provider to change their consent status. Given the importance of patient consent in realizing the potential benefits of health information exchange, there is a need to understand how people perceive the value of HIE (Ancker et al., 2012; Esmaeilzadeh and Sambasivan, 2017) and the importance they place on controlling access to their PHI (Caine and Hanania, 2012; Kim et al., 2017). We argue that, based on the limitations of current consent management processes, there is also a need to provide patients with innovative ways to manage consent for the exchange of their PHI.

Below we discuss a survey conducted to understand how people perceive the value of HIE, the importance of controlling access to their PHI, and how they would prefer to manage consent for the exchange of their PHI using either traditional consent forms filled out at their provider or a consent app allowing them to manage their consent anywhere, anytime. We then demonstrate how a permissioned blockchain is the best choice for architecting the app to allow consent management across all HIE networks in the U.S.

Methods

We developed a 23-question survey instrument that included a video explaining the current form-based consent process and demonstrating an alternative consent management app. To assess the value of HIE for participants, we included questions about care continuity gaps using four questions from the 2016 Commonwealth Fund International Health Policy (CFIHP) Survey, a validated 11-country survey that asked participants about their experiences with the healthcare system in their country (The Commonwealth Fund, 2016). These were followed by questions about the importance of providers having access to all of the participant's PHI that included one CFIHP question. To assess the importance of controlling access to PHI, we included questions on participant perceptions of patient control of HIE, including their preferred consent structure (i.e., opt-out, opt-in, break the glass) and their experiences with consent for HIE that included one CFIHP question. To assess preferences for consent management, we presented participants with a video that first described the typical structure of completing a consent form at the provider and then demonstrated a potential consent management app in which patients could grant and revoke consent for any or all of their providers through the app anywhere, anytime. At the conclusion of the video, we asked participants whether they would prefer to fill out a form at the provider or use the app to manage their consent for HIE and to explain the reasons for their choice. Finally, we concluded the survey with a set of demographic questions. The study design along with the survey instrument and consent form were approved by the authors' university's Institutional Review Board.

Amazon Mechanical Turk (MTurk) was used to solicit survey participation. Mturk workers must be 18 or older, and based on our focus on consent in the context of the U.S. healthcare system, we limited participation to workers in the U.S. To improve the likelihood of receiving valid responses, we also limited participation to MTurk workers with a master qualification, which requires workers to achieve high-quality results for a large number of requests (Amazon, 2018). We employed validation checks in the survey to identify any use of bots and to ensure the respondent was truly paying attention to the content. Through these methods, we rejected six responses continuing data collection until we had acquired 200 responses that met our validation criteria.

Results

While MTurk workers may not have been in the role of a patient when they participated in the survey, that would not have precluded them from having valid opinions on HIE and consent rights regarding their PHI. Also, based on our question about the frequency of their visits to a healthcare provider, nearly two-thirds reported at least annual provider visits, giving most participants relatively recent experience with the healthcare system. The demographic characteristics of our participants are presented in Table 1. Our participant pool was split evenly by gender and distributed across all age categories, with the largest group in the 35-44 age range and the smallest group in the 65+ age range. All minority groups were represented. Most participants had a college degree or higher, and just over half had household incomes higher than $50,000. Additionally, 42 states were represented in the participant pool. 32% of respondents reported experiencing at least one type of care continuity gap (e.g., unavailable medical records, unnecessary testing, doctors giving conflicting information). While 55% reported that when they needed care, their healthcare providers knew important information about their medical history most of the time, only 28% reported that was always the case, indicating an awareness of information access gaps by providers for a majority of the survey participants.

			N=200 (%)
Age		Ethnicity	
18-34	41 (20.5%)	Asian or Pacific Islander	5 (2.5%)
35-44	70 (35%)	Black or African American	14 (7%)
45-54	32 (16%)	Hispanic or Latino	7 (3.5%)
55-64	44 (22%)	White or Caucasian	170 (85%)
65+	11 (5.5%)	Multiracial/Biracial/Other	4 (2%)
Gender		Household Income	
Male	99 (49.5%)	$0-$24,999	36 (18%)
Female	100 (50%)	$25,000-$49,999	61 (30.5%)
Preferred not to say	1 (.5%)	$50,000-$74,999	50 (25%)
Education		$75,000-$99,999	26 (13%)
High school or less	34 (17%)	$100,000-$149,999	19 (4.5%)
Some college	47 (23.5%)	$150,000-$199,999	5 (2.5%)
College degree or higher	119 (59.5%)	$200,000 and up	3 (1.5%)

Table 1. Participant Demographics.

When asked how important it was that their healthcare providers had access to all of their medical information to make care decisions, 82% indicated it was very or extremely important, and 86% said that when seeing a new doctor, they would want the doctor to have access to their previous medical records. Additionally, 65% also indicated that a provider's participation in an HIE that would enable access to all the participant's medical information was very or extremely important in their provider selection process. Therefore, most participants see their provider having access to their medical information as an important feature and HIE as an essential element in that access.

Almost all participants (96%) felt that patients should have full control over which healthcare providers can access their medical information, and 66% indicated they were aware of their rights to limit who could access their medical records. When asked their preference for how permission should be managed for electronically sharing their health information between providers, the opt-out option was preferred by 34% of participants, the break the glass option was preferred by 44%, and 21% preferred the opt-in option. The fact that 86% said they would want a new doctor to have access to their previous medical records, but nearly half preferred the sharing of their PHI electronically only in the case of emergency suggests many participants want the benefits of PHI sharing while retaining access control.

After showing participants our video that explained both a typical consent form filled out at the provider and an example consent management app that would allow consent to be managed anywhere, anytime, we asked the participants to indicate which option they would prefer and explain why they would choose that option. A total of 70% indicated they would choose to use the consent app. By asking our participants to explain their choice, we were also able to conduct an analysis of the reasons for those preferences by coding each comment. The most common reasons (% of comments) participants gave for wanting to use the app were ease (51%), convenience (34%), and speed (22%), while the most common reasons given for wanting to fill out a form at the provider were app/account fatigue, i.e., maintaining access credentials (33%) and security concerns (22%). We present a selection of participant comments in Table 2 to provide additional elaboration on why participants preferred either the app or form. Each cell in the table represents the full comment of one participant who chose the option indicated in the column heading.

Use the consent app (70%)	**Fill out a form at my provider's office (30%)**
It seems easier to manage and could be done ahead of time. It also would give me ongoing control to change and view who had access to my information. It would be beneficial for doctors to see this ahead of time when seeing a new doctor, rather than them being rushed to do it when you are already in office.	I wouldn't have to bother having a separate account and it would easily be done right there in the waiting room / office. I do however like the ability given with the app to go in at any point and grant / revoke access for a given provider. I'd use it in those instances, but for a doctor visit, clearing just a form.
It seems very easy to manage and it would also be nice to have a record of providers seen and to know the status at any given time. The paper consent forms that I've signed are distant memories; the app would keep things current.	It might sound weird, but such a decision seems best in-person and in an intimate setting like the provider's office. Giving consent in my home feels weird, a distance that kind of diminishes the value of such a major decision.
Because it's convenient, I'd trust that the information would actually be shared with the relevant providers/doctors/locations, I'd like medical authorities to have access to all of my information in one place in general, and that it still seems to give users control over specifics if they want.	In modern times, you are more likely to be a victim of a data breach via online, such as a system hack, as opposed to doing it the old fashion way at the doctor's office. Additionally, I personally feel a bit of extra security knowing I personally signed and handed it to the admin at the office.
I like the idea of being able to control access on the fly - instead of having to submit paperwork or something I can just open an app and click a few buttons? Sounds easier, plus it lets me reviews a list of people I've granted access to, which is helpful.	If I'm already going to be at the office receiving care I might as well fill out the form since I'll be filling out many others. I really don't want to have to download yet another app that will inevitably be used to mine data and surveil me.

Table 2. Comments on Consent Management Option Choice.

Bivariate relationships in our data were examined using the Pearson chi-square test for independence. The only demographic variable with a significant relationship to consent management preference was an aggregate of income, where participants with incomes of $75,000 and up were more likely to prefer the consent app than participants with incomes below $75,000, X^2 (1) = 5.82, p = .016. The limited connection between demographics and consent management preference indicates that other factors are more salient in guiding participants to prefer one option over the other. To that end, we found that participants who had experienced at least one type of care continuity gap were more likely to prefer the consent app X^2 (1) = 6.79, p = .009. They were also more likely to indicate that it was very or extremely important that their healthcare providers had access to all their medical information to make care decisions X^2 (1) = 5.14, p = .023. Participants who preferred the opt-out or break the glass options for permission management were also more likely to select the consent app than participants who preferred the opt-in option, X^2 (2) = 8.33, p = .015. While greater control was mentioned by 13 participants as a reason for why they preferred the consent app, the relationship between the importance of control and preference for the consent app was not significant, X^2 (1) = 1.03, p = .311. Multivariate analysis using logistic regression was also performed on the data. The results corroborated the bivariate analysis findings but did not provide evidence of additional meaningful relationships in the data. Table 3 displays the results of one logistic regression analysis.

Coefficients	**Estimate**	**Std. Error**	***z*-value**	***p*-value**
Intercept	-0.7692	0.4546	-1.692	0.0907
Access to Records by Healthcare Team	1.1148	0.4531	2.461	0.0139
Permission Management	0.7016	0.4053	1.731	0.0834
Control Importance	0.3521	0.3875	0.909	0.3636
Education	0.6333	0.4169	1.519	0.1288
Income	0.7769	0.4195	1.852	0.0640

Table 3. Results of a Logistic Regression Analysis.

The relationships we found, along with comments from participants that include examples in Table 2, suggest that many participants, especially those who had experienced a care continuity gap, saw the consent app as an effective way to confirm that providers had their permission to access all their medical information. In other words, preferring the consent app was often less about increasing control over providers' access to PHI and more about making sure providers did have access to all the participant's medical information to make informed care decisions. Consequently, the current process of filling out consent forms at a provider may be hampering efforts to increase the PHI available through HIE by making it more difficult for patients to give consent and verify that consent to access their PHI has been given.

Discussion

Given the option, 70% of the study participants would choose to use an app that would allow them to self-manage their consent for HIE rather than continue to use the current process of filling out consent forms at a provider. Based on the current U.S. HIE environment, where there are more than 100 HIEs across the country and with each state determining its own consent structure, we argue that the most viable architecture for implementing such an app that would enable consent management beyond a single HIE network would be a blockchain-based solution. Recent literature reviews have noted the potential value of blockchain in healthcare for, among other things, health information exchange (Abu-elezz et al., 2020; Hasselgren et al., 2020). Others have proposed a blockchain architecture to support health records management, including personal health records (Leeming et al., 2019). Below we describe the structure of a novel blockchain-based network for HIE consent management and explain why it is an appropriate model for managing HIE consent.

Blockchain for HIE Networks

Blockchain technology represents a distributed and decentralized append-only database. Distributed storage relates to the redundancy resulting from storing the same transactional data across many computational devices, also called *nodes*. Decentralized storage means that such computational devices may belong to different organizations. Nodes create a peer-to-peer network, henceforth called the *blockchain network*, to validate, process, and store transactions and share data. In the context of HIE networks, we envision each node in the blockchain network representing one HIE.

The system users can, under some conditions, add data to or retrieve data from the blockchain. One can add data to the blockchain through transactions. In the context of HIE networks, transactions can be, for example, a patient granting consent for sharing their PHI through a specific HIE. Similarly, the patient can subsequently revoke the previously granted consent. It is worthwhile to explain how the underlying data are stored after a transaction is created. The following steps are abstract enough to roughly describe several blockchain models. First, the user connects with one node of the blockchain network and submits the created transaction. Second, that node may broadcast the transaction to several other nodes. Third, a subset of the nodes can group transactions into blocks. This means that transactions are processed in batches rather than individually. Fourth, one node is periodically selected to propose a block to be stored locally by the other nodes. This step is fundamental in that the selected node is indirectly responsible for ensuring consensus, and, as such, the node selection scheme is traditionally called a *consensus mechanism*. Fifth, the other nodes verify the transactions in the block proposed by the previously selected node. Finally, if valid, the block is stored locally by each node and linked to the previously stored block to create a chain of blocks (i.e., a blockchain). That linking operation ensures that previously stored data are tamper-proof (i.e., any attempts to change previous transactions can be easily detected). Moreover, every transaction and block are timestamped and, consequently, blockchain technology provides an unequivocal source of truth concerning when different consent/revoke operations happen. That said, previous consent operations can be revoked by creating new transactions instead of updating previous transactions. Therefore, a history of each patient's consent decisions will be maintained on the blockchain, with the most recent decision on the chain representing the patient's current consent status.

Having data stored by nodes in the blockchain network, a user can subsequently query any node (HIE) that user has access to retrieve relevant data. For example, patients can list all the HIEs they interacted with before (i.e., they issued/revoked consent). Moreover, a healthcare provider can query a node to determine whether it needs to ask for an incoming patient's consent or not. All the interactions between users and blockchains happen through an application called a *wallet*, which works as a gateway between decentralized applications (DApps) and the blockchain. Wallets manage digital identities and all cryptographic keys, thus having no need for an application to store and manage those keys. Universal wallets (Jørgensen and Beck, 2022) have the potential to address some of the concerns raised by some of the participants in our survey. For example, Table 2 highlights a comment from one participant concerned about downloading and installing another application ("*I really don't want to have to download yet another app that will inevitably be used to mine data and surveil me*"). Universal wallets enable users to manage identifiers used by several blockchain-based applications, including a potential blockchain application for consent management, in a single place.

Naturally, healthcare-related data, including consent data, are highly private and sensitive. In particular, a user's consent status should only be available to that user, relevant healthcare providers, and the HIEs. Hence, blockchain technology must support those privacy constraints, which brings us to the concept of public and permissioned blockchains. Public blockchains are open to anyone, and no special permissions are required to join the network as a user or node. Clearly, this type of blockchain network is undesirable in our context as it implies that all consent information may be available to the public. Unlike public blockchains, permissioned blockchains focus on networks of known, vetted participants operating under a well-defined governance model. In particular, one needs to secure special permissions ex-ante to join the network as a user and/or node. In our application, one can establish a network where HIEs are the nodes, and patients can only retrieve consent data that have them as the consent issuer. In this sense, the goal of permissioned blockchains is to secure and share transaction data among a group of participants who know each other. Technically, one advantage of knowing the participants' identities is that permissioned blockchains can rely on less computationally intensive consensus mechanisms and, thus, increase the number of transactions processed by unit of time and decrease the underlying digital carbon footprint.

A Decision Model Concerning Blockchain Adoption

Figure 1 presents a model used in the work by Carvalho (2021), which we use to further motivate the application of blockchain technology in the context of an HIE network. This eight-step decision path helps determine whether and which blockchain technology should be used in a given domain.

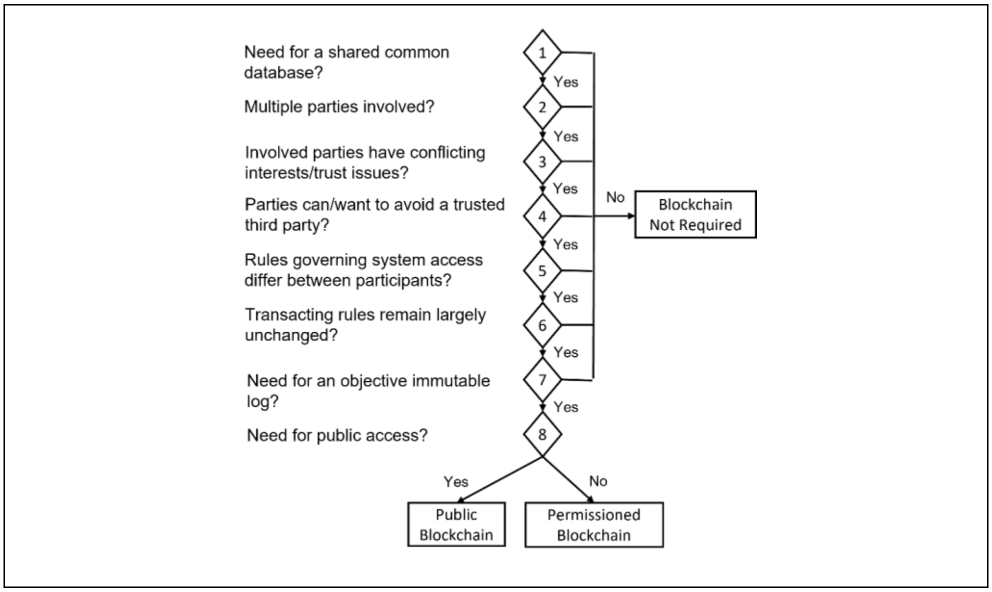


Figure 1. Blockchain Eight-Step Decision Path (Carvalho, 2021).

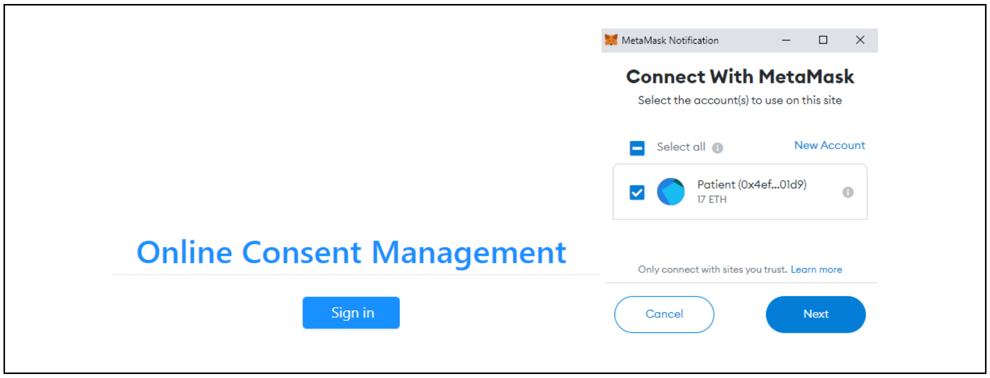
For consent management of PHI, the answers to the questions in the decision path model are as follows.

1. Yes, it is clearly desirable for every transaction involving healthcare consent to be stored in a database. We further argue that a database shared by many HIEs is crucial to increasing efficiency. For example, consider when a patient moves from one region to another served by a different HIE. In this case, after receiving the patient's consent, the new HIE can quickly verify which other HIEs have also received the patient's consent and, thus, request PHI in a timelier manner.
2. Yes, because many HIEs might need a patient's consent. Returning to the previous scenario where a patient moves to a region served by a different HIE, that patient can now potentially indirectly interact with two different HIEs from the new and previous region where the patient lived.
3. Yes, patients and HIEs might have different interests and goals concerning PHI. For example, it is convenient for the HIEs to collect as much health-related data as possible together with patients' consent to share PHI. However, this practice, in turn, creates privacy concerns for the underlying patients with regards to who has access to personal data and for how long.
4. Yes, having a third-party entity responsible for collecting and managing patients' consent and, potentially, EHRs may work for countries with universal healthcare systems, but it is unfeasible for countries where states or provinces have different regulations, such as the United States.
5. Yes, HIEs and patients have different roles. Specifically, HIEs have access to all consent data issued by patients, whereas patients can issue or revoke consent.
6. Yes, the roles of HIEs and patients remain largely unchanged over time, as do the rules governing transactions.
7. Yes, in the context of HIE networks and consent management, an immutable (and trusted) log system can unequivocally show a patient's preferences regarding whom can access and share his/her healthcare data.
8. No, permissioned blockchains require one to obtain permissions to join the network as a node or user, whereas public blockchains allow universal access. In our context, allowing for universal access and public transactions may violate privacy regulations, meaning that permissioned blockchains are more suitable than public ones.

The answers to the blockchain decision path model suggest that a permissioned blockchain can effectively form the underlying information technology infrastructure for HIEs to store, manage, and share patients' consent. A consent management app would provide the frontend interface that could leverage the permissioned blockchain to enable patients to manage their consent for HIE across all providers who participate in an HIE on the blockchain network.

Prototype Development

To instantiate our ideas, we developed a prototype running on a private instance of the Ethereum blockchain network. Specifically, we developed a web-based interface for patients to manage their consent data. A smart contract — an algorithm deployed to and executed in tandem by nodes — helps system users add data to and query the blockchain. When a user accesses the web application, s/he is asked to authenticate using a wallet (Figure 2). We use the MetaMask wallet in our prototype.



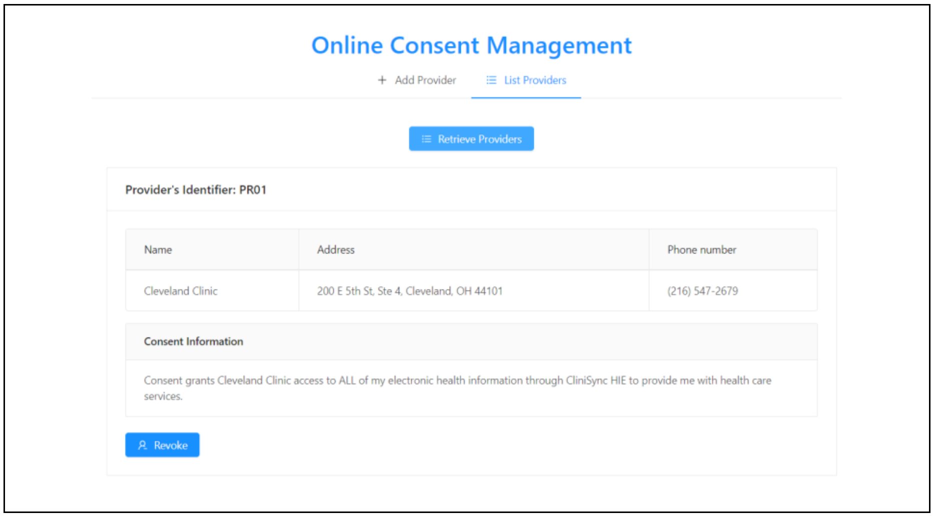
Select the account(s) to use on this site

☑ Patient (0x4ef...01d9) 17 ETH

Only connect with sites you trust. Learn more

Figure 2. User Authentication Using the MetaMask Wallet.

After authenticating, the user can view a list of all the providers to whom the user has granted consent to exchange their PHI (Figure 3). For that to happen, the web application queries the blockchain through the smart contract, which in turn uses the user's credentials provided by the wallet to retrieve the relevant data. The user can revoke consent by simply pressing a button. When that happens, a new transaction is created by the web interface and submitted to the blockchain.



Provider's Identifier: PR01

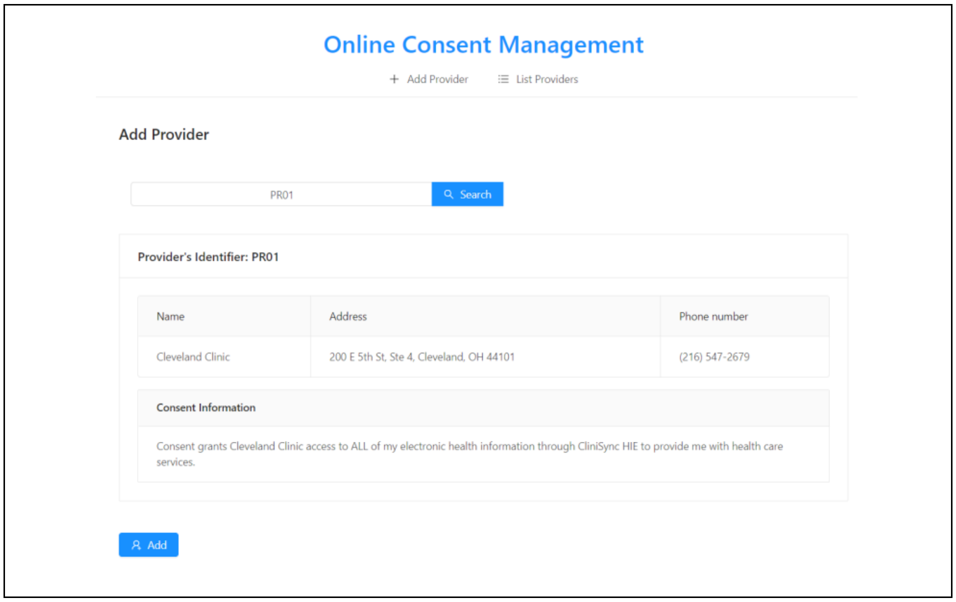
Name	Address	Phone number
Cleveland Clinic	200 E 5th St, Ste 4, Cleveland, OH 44101	(216) 547-2679

Consent Information

Consent grants Cleveland Clinic access to ALL of my electronic health information through CliniSync HIE to provide me with health care services.

Figure 3. List of Providers Who Received Consent from the User.

Finally, the user can search for a provider with the provider's identifier (Figure 4). A blockchain transaction is then created if consent is granted. Note that all blocks with transactions are shared with all blockchain network nodes (HIEs), thus granting them near-real-time access to consent information.



Add Provider

PR01

Provider's Identifier: PR01

Name	Address	Phone number
Cleveland Clinic	200 E 5th St, Ste 4, Cleveland, OH 44101	(216) 547-2679

Consent Information

Consent grants Cleveland Clinic access to ALL of my electronic health information through CliniSync HIE to provide me with health care services.

Figure 4. Searching for and Granting Consent to a Provider.

Conclusion

Our study finds that the majority of people see the value of HIE and would prefer that providers have access to all their PHI to make informed care decisions. The current practice of completing consent forms at a provider limits how patients give consent and verify that consent has been given, thus hampering efforts to increase the PHI available through HIE. Given the potential value of increased exchange of health information and the need for patient consent to achieve high levels of HIE, alternative consent methods are needed. Our study finds that if an app were available for managing consent, most people would be interested in using it. To make such an app work within the current structure of HIE in the U.S., we argue that a back-end blockchain solution would be necessary, and we have explained how that solution would need to be architected. Additionally, we have developed a prototype app demonstrating how patients and providers can interact with the blockchain-based system. In future work, we plan to develop design principles and validate them with experts. Those will be used to refine our system design and prototype. Finally, we want to generalize our work by creating a design theory that addresses distributed consent management for use in healthcare and other domains.

Acknowledgments

This work was supported by the EY Cybersecurity Initiative at Farmer School of Business, Miami University.

REFERENCES

Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., and Abd-alrazaq, A. 2020. "The Benefits and Threats of Blockchain Technology in Healthcare: A Scoping Review," *International Journal of Medical Informatics* (142), p. 104246.

Adjerid, I., Acquisti, A., Telang, R., Padman, R., and Adler-Milstein, J. 2016. "The Impact of Privacy Regulation and Technology Incentives: The Case of Health Information Exchanges," *Management Science* (62:4), pp. 1042-1063.

Amazon. 2018. "Amazon Mechanical Turk Worker FAQs." Retrieved on October 8, 2021, from https://www.mturk.com/worker/help

Ancker, J. S., Edwards, A. M., Miller, M. C., and Kaushal, R. 2012. "Consumer Perceptions of Electronic Health Information Exchange," *American Journal of Preventive Medicine* (43:1), pp. 76-80.

Apathy, N. C., and Holmgren, A. J. 2020. "Opt-in Consent Policies: Potential Barriers to Hospital Health Information Exchange," *The American Journal of Managed Care* (26:1), pp. e14-e20.

Bergmann, J., Bott, O. J., Pretschner, D. P., and Haux, R. 2007. "An E-Consent-Based Shared Ehr System Architecture for Integrated Healthcare Networks," *International Journal of Medical Informatics* (76:2), pp. 130-136.

Caine, K., and Hanania, R. 2012. "Patients Want Granular Privacy Control over Health Information in Electronic Medical Records," *Journal of the American Medical Informatics Association* (20:1), pp. 7-15.

Carvalho, A. 2021. "Bringing Transparency and Trustworthiness to Loot Boxes with Blockchain and Smart Contracts," *Decision Support Systems* (144), pp. 1-13.

Downing, N. L., Adler-Milstein, J., Palma, J. P., Lane, S., Eisenberg, M., Sharp, C., Collaborative, N. C. H., and Longhurst, C. A. 2016. "Health Information Exchange Policies of 11 Diverse Health Systems and the Associated Impact on Volume of Exchange," *Journal of the American Medical Informatics Association* (24:1), pp. 113-122.

Esmaeilzadeh, P., and Mirzaei, T. 2018. "Comparison of Consumers' Perspectives on Different Health Information Exchange (HIE) Mechanisms: An Experimental Study," *International Journal of Medical Informatics* (119), pp. 1-7.

Esmaeilzadeh, P., and Sambasivan, M. 2017. "Patients' Support for Health Information Exchange: A Literature Review and Classification of Key Factors," *BMC Medical Informatics and Decision Making* (17:1), p. 1-21.

Everson, J., Patel, V., and Adler-Milstein, J. 2021. "Information Blocking Remains Prevalent at the Start of 21st Century Cures Act: Results from a Survey of Health Information Exchange Organizations," *Journal of the American Medical Informatics Association* (28:4), pp. 727-732.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., and Faxvaag, A. 2020. "Blockchain in Healthcare and Health Sciences—a Scoping Review," *International Journal of Medical Informatics* (134), p. 104040.

Kim, K. K., Joseph, J. G., and Ohno-Machado, L. 2015. "Comparison of Consumers' Views on Electronic Data Sharing for Healthcare and Research," *Journal of the American Medical Informatics Association* (22:4), pp. 821-830.

Kim, K. K., Sankar, P., Wilson, M. D., and Haynes, S. C. 2017. "Factors Affecting Willingness to Share Electronic Health Data among California Consumers," *BMC Medical Ethics* (18:1), pp. 1-10.

Jørgensen, K. P., and Beck, R. 2022. "Universal Wallets," *Business and Information Systems Engineering* (64:1), pp. 115–125.

Leeming, G., Cunningham, J., and Ainsworth, J. 2019. "A Ledger of Me: Personalizing Healthcare Using Blockchain Technology," *Frontiers in Medicine* (6:171).

Marchesini, K., and Pritts, J. 2013. "Meaningful Consent in Electronic Health Information Exchange: A Technology-Centric Approach," in: *Health Affairs Blog*. Retrieved on April 22, 2022, from https://www.healthaffairs.org/do/10.1377/forefront.20130917.034263/

Menachemi, N., Rahurkar, S., Harle, C. A., and Vest, J. R. 2018. "The Benefits of Health Information Exchange: An Updated Systematic Review," *Journal of the American Medical Informatics Association* (25:9), pp. 1259-1265.

Office of Civil Rights. 2002. "Standards for Privacy of Individually Identifiable Health Information; Final Rule," D.o.H.a.H. Services (ed.).

ONC. 2017. "State Health It Privacy and Consent Laws and Policies." Office of the National Coordinator for Health Information Technology (ONC).

ONC. 2018. "Health Information Technology." Retrieved on April 4, 2022 from https://www.healthit.gov/topic/health-information-technology

ONC. 2019. "State Health Information Exchange." Retrieved on October 10, 2021, from https://www.healthit.gov/topic/onc-hitech-programs/state-health-information-exchange

Simon, S. R., Evans, J. S., Benjamin, A., Delano, D., and Bates, D. W. 2009. "Patients' Attitudes toward Electronic Health Information Exchange: Qualitative Study," *Journal of Medical Internet Research* (11:3), pp. 1-8.

The Commonwealth Fund. 2016. "2016 Commonwealth Fund International Health Policy Survey of Adults." Retrieved on October 10, 2021, from https://www.commonwealthfund.org/publications/surveys/2016/nov/2016-commonwealth-fund-international-health-policy-survey-adults

Van Dyke, D. 2020. "Ehealth Exchange Health Information Network Welcomes Hie Networks, First Vendor Participant." *eHealth Exchange*. Retrieved on April 22, 2022 from https://ehealthexchange.org/ehealth-exchange-health-information-network-welcomes-hie-networks-first-vendor-participant/

Vogels, E. A. 2021. "Digital Divide Persists Even as Americans with Lower Incomes Make Gains in Tech Adoption." Pew Research Center.