A Novel Blockchain based Platform to Support Chronic Care Model Information Management

Luigi Lella and Sergio Piersantelli
Azienda Sanitaria Unica Regionale delle Marche, via Oberdan n.2, 60122 Ancona, Italy

Keywords: eHealth, eHealth Applications, Design and Development of Methodologies for Healthcare IT.

Abstract: Blockchain technology has been successfully used in many healthcare contexts, guaranteeing not only high security and privacy levels in clinical data management, but also the continuous updating of patient clinical pictures, to ensure the continuity of care and the reliability of data sources in statistical processing. These results are related to the peculiar features of this technology such as the distributed ledger, the chaincode, the encryption algorithms used to cypher information, the technological solutions used for block validation and the use of smart contracts. This article aims to present a possible solution based on blockchain technology to the problem of information management in the Chronic Care Model. The use of the blockchain makes it possible to create a patient-centred system that not only allows patients, or authorized people, to exercise a constant control over their health data, but it is also able to "contractualize" the agreements made in this regard together with the collection of consent for the processing of health data. The blockchain also allows the preparation of validated data sources for the subsequent statistical processing to update process and outcome indicators and the risk prospects related to the care pathways activated for patients suffering from chronic pathologies.

1 INTRODUCTION

Patients involvement within the health information system can lead to a marked improvement in individual and social health outcomes (Kushniruk and Nøhr, 2016). These results are even more evident when strategies are adopted to address the education of patients in order to create a sort of partnership with health professionals and other caregivers (Batalden et al., 2016; Bodenheimer et al. 2002).

Designing an information system to support healthcare activities can however be an extremely complex activity, especially in the case of the treatment of patients suffering from chronic pathologies that require long and prolonged interactions with various actors of the information system. These actors can be not only professionals and caregivers, but also IoMT devices that must constantly monitor vital parameters.

This is the case of the Chronic Care Model (CCM), a model of health care for chronically ill patients developed by Professor Wagner and his colleagues at the McColl Institute for Healthcare Innovation, in California (Wagner et al., 2001; Wagner et al., 1999). The model proposes a series of changes at the level of health systems useful in favouring the improvement of the condition of chronic patients and suggests a "proactive" approach between health personnel and the patients themselves, with the latter becoming an integral part of the care process (Coleman et al., 2009).

The CCM model is characterized by six fundamental characteristics (Wagner et al.,1996).

Delivery System Design: the care activity is provided with a clear subdivision of the tasks and responsibilities between the various caregivers and health professionals that take care of the patient, making a clear distinction between planned assistance (e.g.: follow up) and assistance in the acute phase (acute care);

Self-management Support: that consists in assisting in a collaborative way the patients and their families in the acquisition of the necessary skills for the treated disorders and diseases. The information system intervenes in this phase by making available self-care tools, references to community resources and tools for assessing therapeutic compliance;

Decision Support: the presence of evidence based decision support tools that can also be used by patients to agree with their GPs the therapeutic or pharmacological pathway to follow;

Clinical Information System: the information system must mainly provide tools to support therapeutic compliance, a system of indicators for the assessment

Lella, L. and Piersantelli, S.
A Novel Blockchain based Platform to Support Chronic Care Model Information Management.
DOI: 10.5220/0008869003030309
In *Proceedings of the 13th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2020) - Volume 5: HEALTHINF*, pages 303-309
ISBN: 978-989-758-398-8; ISSN: 2184-4305

of outcomes and care benefits and agendas for assistance activities planning;

Community Resources: connection to territorial and hospital resources for the training of the assisted and for the reporting of care managers;

Health Care Organizations: connection to the organizational structure, objectives and values of the health system that takes care of the patient.

To date, within the CCM, adequate information systems have not yet been defined that can support patients in all their needs and actively involve them in the care process. Indeed, it was noted that most of these patients were marginalized if not even excluded from any initiative of active involvement (Marmot et al., 2012). These cases have led to a substantial worsening of care outcomes and to an increase in care costs compared to the average (Coulter et al., 2018) and to a worsening of the quality of the assistance given to disadvantaged patients (Mackert et al., 2016). Difficulties have also been encountered in the exchange of data in a secure and scalable manner between the various system actors, in the support of clinical communications especially in the cases of patients living in remote areas, producing in this case also a deterioration in efficacy and quality of care services that should be supported by adequate information systems (Zhang et al., 2018; Castaneda et al., 2015; Berman and Fenaughty, 2005).

In general, the process of clinical information retrieval is slow as health data, when not present in the Electronic Health Record, must be recovered from various sources, prepared in order to respect certain schemas and sent to the recipient through appropriate channels characterized by high levels of security and reliability (Nourie, 2015). The process of clinical information retrieval is also incomplete precisely because of the extreme fragmentation of produced data and the lack of those produced by the same patient, and it is decontextualized because all the data are provider-centred and not patient-centred. Furthermore health information systems do not allow patients to know how and by whom data is processed and do not allow to govern access policies to them (Schoenberg, 2013). The data are also not updated in real time (Ash et al. 2004).

In assisting patients suffering from chronicity, and therefore also in CCM, remote patient monitoring (RPM) is of fundamental importance, because it allows to move some care services outside the traditional clinical setting (typically at home care recipients). The use of RPM can help to further reduce the cost of assistance and improve the outcomes achieved. The currently used tele-monitoring devices have now become unobtrusive, user-friendly and equipped with advanced features such as alerting and patient feedback collection systems directly implemented at the device level.

Currently no solutions have been defined that allow secure management of the data in Internet of Medical Things (IoMT) networks (Linn and Koo, 2017) and the sharing of data between authorized devices in order to provide a complete information framework to allow them to carry out automatic operations safely through their actuators (Bolduc, 2017).

Finally, precisely because of the innumerable sources of health data (most of which derive directly from IoMT devices and the direct feedback of patients), it is particularly difficult to bring them all back into a single framework to generate a valuable population level insight (Asokan and Asokan, 2015).

The blockchain technology (BC) can provide a viable implementation solution that guarantees secure access to health data, system scalability, privacy of clinical data, and data collection to conduct evidence-based studies of population medicine.

The aim of this article is to suggest a possible solution for the implementation of a CCM support information system which is based on the BC technology. After a rapid examination of the main characteristics of this technology (Section 2), the main applications of the BC in medical and healthcare field will be reviewed, with respect to the management and sharing of clinical and remote control devices information (Section 3). The architecture of CCM support platform designed by ASUR will then be illustrated together with a business case related to the context of AV2 local health system of Marche Region (Section 4).

2 BLOCKCHAIN TECHNOLOGY MAIN FEATURES

A BC system can be considered as a distributed and potentially incorruptible cryptographic database, where it is possible to store sensitive and health data. Technically it is essentially a peer-to-peer network with an open and distributed ***ledger***, whose updating is based on appropriate consensus rules for the transfer of ***blocks*** of information between entities that can be people, organizations and devices.

BCs can be ***permissionless*** and ***permissioned***. A permissioned BC limits the number of actors who can participate in the consensus validation process.

The data related to a new block contained in the ledger spread through the peer-to-peer network as soon

as it is possible to establish a communication between each couple of authorized nodes. Each of the authorized nodes, following the one that generated the block, has the right to verify the validity of the block and the correspondence with the network policies. If the transaction is accepted, it is digitally signed and stored in the distributed ledger. All rejected transactions are entered into a temporary archive.

A register can be seen as an ordered sequence of transactions divided into blocks. Each block can represent a set of transactions (for example the transfer of clinical data or information) and contains two elements. The first is the ***header*** that includes a timestamp and the hash code of the header of the previous block. The second is the ***body*** that contains all the transaction data properly encrypted.

The link that connects a header to the previous one (starting from the first chronologically inserted that is called "Genesis") allows to set up the BC ensuring that nobody can tamper the inserted data. The only way to do this would be to control more than 51% of the nodes before modifying the data in the distributed ledger. This situation is attributable to the Byzantine Generals Problem (BGP) (Melnyk et al., 2018). In these cases the protocol to be used to manage the consent must be ***Byzantine Fault Tolerant*** (BFT).

The distributed register can also contain smart contracts (Szabo, 1997) that can help to regulate the access to the data contained in the blocks and to validate them. For example a smart contract can be used to define privacy policies or to define appropriate alerting rules linked to certain data-driven conditions.

3 RELATED WORK

With regard to the processing of personal and sensitive data in the health field, there has always been a conflict between ***data privacy*** (Pavlou, 2011) and ***data accessibility*** that is the sharing of data between the professionals who take charge of the patient (Culnan, 1984).

In contexts such as the CCM, professionals from different fields and disciplines should be able to access the contents of clinical records they need (Reti et al., 2010). In the operative reality, interoperability between information systems belonging to different healthcare organizations or based on different technologies is often not guaranteed (Detmer et al., 2008). This problem is well known in the health field under the name of ***care coordination*** (Klein et al., 2015).

In general, in the health sector there is a need to implement secure and scalable systems capable of ensuring access to data on a large scale, guaranteeing trust and the compliance with the policies on sensitive and personal data.

The first solutions for the management of health data privacy and accessibility in the presence of multi-professional teams or multiple health organizations resort to multi-agent solutions (Isern and Moreno, 2016; Barrue et al., 2015; Wimmer, 2014). More recently, solutions based on BC technology based on the Electronic Health Record model have begun to be considered. Some first implementations make use of the distributed ledger of the BC, of a secure management system of encryption keys and of a characteristic system for blocks validation (Wood et al., 2016), other solutions resort to the so-called ***miners***, or groups of nodes of the peer-to-network peer that constitutes the BC, which are given the task of validating new transactions (Azaria et al., 2016; Ekblaw et al., 2016). Other more recent implementations make use of BC cloud services to ensure the secure and unalterable exchange of information between multiple healthcare organizations, in order to constantly update the patient's clinical picture and to ensure continuity of care (Xia et al., 2017). Such systems prove to be particularly effective in contexts such as the treatment of patients suffering from chronic disorders (e.g. HIV and cancer). For chronic patients, permissioned BC-based solutions have also been adopted, especially to ensure privacy and data security (Dubovitskaya et al., 2017). Also characteristic is the choice made by (Benchoufi et al., 2017) to manage the patients' informed consent through a CB to make it unfalsifiable.

In general, however, for the management of clinical data by multidisciplinary teams of professionals, the tendency is currently to resort to the Personal Health Record model where patients themselves or their representatives are responsible for managing the access policies to their data, monitoring constantly their accesses and the uses made of them (Chen et al. 2018; Yue et al., 2016; Ivan, 2016). This choice is well suited to the CCM model, which provides for a high level of involvement of the patient who actively and consciously participates in the choice of the therapeutic path.

With regard to remote monitoring systems using IoMT devices, in recent times there has been the choice of implementing solutions based on the BC (Griggs et al.,2018; Wu et al., 2019).

For RPM through IoMT devices, it is generally not recommended to use computationally heavy algorithms such as Proof of Work (PoW) for block validation and symmetric-type encryption algorithms are used (Dorri et al. 2016, Dorri et al. 2017).

Furthermore smart contracts for data processing are implemented in order to identify critical situations and to send alerts to the nodes associated with health professionals (Griggs et al., 2018).

Overall, what emerges from the literature seems to validate the choice of the BC for the safe and reliable management not only of the communications between professionals who take care of chronic diseases but also of communications coming from or exchanging IoMT devices (Dwivedi, 2019).

4 ASUR CCM MANAGEMENT FRAMEWORK

A patient-centred CCM management framework (CCMMF) will be implemented at the Area Vasta 2, throughout the territory that revolves around the community hospitals of Jesi, Loreto and Chiaravalle.

The CCMMF will interface with other systems already used at regional level such as the regional authentication system called FedCohesion, the Policy Manager and the Regional Attribute Authority to give the actors involved in the CCM the appropriate access rights to the CCMMF platform. The regional reference database for patients anagraphical data called ARCA will be used together with the Electronic Health Record called SIRTE and the regional catalogs containing the updated data of the organizational structures.

The CCMMF will consist of a ***permissioned*** blockchain (BC) based on the HyperLedger Fabric (HLF) platform. The various nodes must first undergo an authentication procedure before performing the creation or validation of new blocks. The approval (***endorsement***) of a set of transactions (sending multiple clinical information) present in a new block will follow a process characterized by various phases (proposal, approval, ordering, validation and commit) and will follow certain approval policies. In particular these policies will identify which nodes must give the endorsement for a given transaction class, while the chaincode will guarantee that these policies have been implemented.

Before committing, peers will execute the chaincode to ensure that there are sufficient endorsements and that they have been obtained from the appropriate entities (those defined at the policy level). In the end, a check will also be carried out on the version of the registry before inserting the new blocks to avoid attacks such as double spending operations. Each transaction in a block contains its read/write set or the set of cryptographic keys that have been read or written at endorsement time.

The HLF framework introduces the ***channel*** element. In HLF the channels are the first level of segregation and information confinement. A ledger is logically associated with a channel (a register itself replicated as many times as there are peers associated with that channel). Therefore peers that do not participate in a channel do not have visibility on the data written in it.

For a more accurate management of access within a channel it is possible to define ACLs (Access Control Lists). Access policies are written in blocks but on a separate channel from the application data. Writing within a channel the authorization logics there remains an indelible auditable trace over time of all the definitions made and all their modifications.

In this way it is possible to solve the problem of managing access policies in a lightweight and scalable manner, complying with the current provisions of the GDPR (General Data Protection Regulation, 2016). By accessing the channel dedicated to data access policies produced by the peer-to-peer network, the patient, or a person in charge thereof, can modify these policies at any time, guaranteeing the traceability of accesses, the data obscuration as well as the obscuration of obscuration. In other words, not only unauthorized nodes will not be able to access the contents of a file, but they will also ignore their existence. It will also be possible to recover all the health information produced by the peer-to-peer network by going back along the chaincodes associated with the various channels, storing them in an exportable format and it will also be possible to process all the information made available by the client for statistical purposes.

The chaincode, at the time of accessing the data, will perform a check on the authorization criteria currently available and will apply them in response to a request for a node. For the encryption of clinical data, symmetric algorithms will be used to facilitate transactions with and between IoMT device nodes.

In the CCMMF solution implemented by the ASUR, smart contracts will also be used for the purpose of processing data, and implementing alerting systems in order to proactively alert caregivers and all professionals who have taken care of the client of important changes in the relative clinical picture.

The activities of the professionals operating within the CCM will be managed through a workflow management system (WMS). Thanks to this WMS through an app that can be installed on the smartphone, the assisted and its caregivers will have a complete picture of the care path to follow and will receive alerts on scheduled events (such as taking a drug, carrying out an outpatient visit or of a therapeutic treatment) or on critical events to be managed promptly by following

the appropriate guidelines prepared by the multidisciplinary team that took care of the client.

The CCMMF will initially be tested on care pathways aimed at patients suffering from chronic cardiovascular diseases and will provide real-time monitoring of some vital parameters of the patient (heart rate, blood pressure, ECG) using IoMT devices.

The figure shows a typical scenario relating to the CCM. The main actors are the ***cardiac patient***, the ***general practitioner*** (GP), the ***family nurse practictioner*** (FNP), the ***local professional*** (dietitian, nutritionist, social worker, geriatrician, physiatrist, wellness coach etc.), the ***drugstore*** (which can also provide services in addition to the administration of drugs, counselling services or registration of parameters such as weight, body mass index, pressure etc.), ***IoMT monitoring devices*** wearable by the patients and any ***affiliated shops*** where patients can purchase food monitoring the ingredients and quantities purchased to check if the purchased product is in line with the diet that patients must respect.

All these actors can create blocks or access blocks belonging to their own channel, in compliance with the access policies to the data established by the patient.

To ensure that the CCM is effectively applied, the workflow of the entire care process must follow the so-called ***'5As' model*** (Glasgow et al., 2006). Following the recruitment of the assisted by the GP, the path followed by the CCM is started. The first phase (***1.assess***) consists in the recovery, through appropriate questionnaires, of the knowledge of the patients about their chronicity, of their behavioural habits and of their expectations of improvement. This phase mainly involves the patient and the FNP who administers the questionnaires. In the second phase (***2. advise***) the FNP helps the client to understand what are the possible therapeutic and pharmacological pathways that can be followed. The ultimate aim is to allow the patient to make an informed choice of the care pathway registering it in the third phase (***3.agree***) within a specific smart contract. This will allow the entire assistance system to safeguard itself also from the legal point of view. In the smart contract, the consent will also be recorded in relation to the data processed in the various channels activated, released in an informed manner by the user.

In the fourth phase (***4.assist***) assistance is provided following the pathway agreed with the patient. The vital parameters of patient are also monitored in order to verify whether the chosen care pathway is giving rise to objectively verifiable improvements. In this patient-centred record patients can incorporate patient-reported experience measures (PREM) and patient-reported outcome measures (PROM) in addition to data

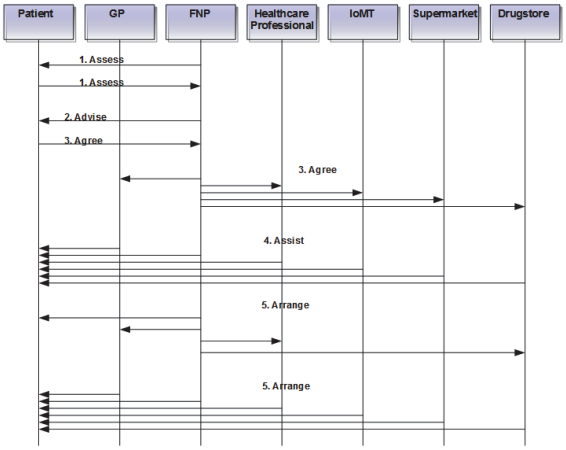

Figure 1: CCMMF communication diagram.

provided by wearable monitoring devices [16].

In the fifth phase (***5.arrange***) the FNP, in agreement with the multidisciplinary team (GP, dietician, nutritionist, social worker, geriatrician, physiatrist, wellness coach etc.) who takes care of the client, decides the modalities in which to conduct any follow-up activities.

The main actors presented in the communication diagram of Figure 1 will interface to an Enterprise Service Bus which has the task of managing communications between the healthcare IT platforms used in the regional context and the main IT systems that make up the backbone of the platform to be realized.

The system components are shown in figure 2. The circles represent the interfaces used by the system actors. The professionals who take charge of the care recipient have been divided into two groups consisting of regional health personnel (who authenticate themselves through the FedCohesion regional authentication system) and non-healthcare personnel operating in the regional territory (physiatrist, social worker, dietician, nutritionist, wellness coach etc.) that uses another strong authentication system included in the interface.

The interfaces used by the main actors (with the exception of the IoMT devices) have an adequate GUI that guarantees adequate levels of usability / accessibility considering the relative user categories.

The blockchain is implemented using the open source framework HLF, which also allows the channel mechanism to be implemented.

For the management of consent data, a special channel must be used within the network that constitutes the blockchain. A node must be created and managed for each of the types of actors involved in the business process of Figure 1.

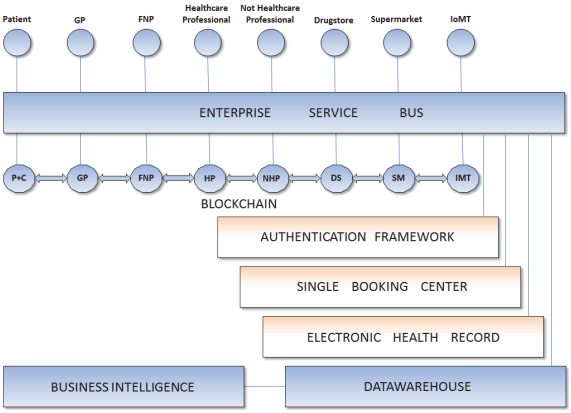

Figure 2: CCMMF architecture.

At the end of the route, all the sensitive and health data produced must be recovered using the chaincode associated with the route, in order to ensure its completeness and validation.

5 CONCLUSIONS

After a brief summary of the BC technology features and an examination of the main implementation solutions relating to the IT support systems for care activities aimed at patients suffering from diseases and chronic disorders, a possible computerization solution of the CCM based on BC technology was presented.

This platform will be used on an experimental level for a year in a restricted territorial reality of the Marche Region, and if it will present concrete and encouraging levels of results it will soon be extended to the whole regional territorial reality.

The outcome measures collected at the end of the trial period will be used to evaluate the effectiveness of the technological solution chosen to support the care activities related to the CCM.

REFERENCES

Ash, J.S., Berg, M., Coiera, E.: Some unintended consequences of information technology in health care: the nature of patient care information system-related errors, Journal of the American Medical Informatics Association,, 11, (2), pp. 104-112 (2004).

Asokan GV, Asokan V.: Leveraging “big data” to enhance the effectiveness of “one health” in an era of health informatics. J Epidemiol Glob Health 2015 Dec;5(4):311-314 (2015).

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: Medrec: Using blockchain for medical data access and permission management. In Open and Big Data (OBD), International Conference on, pages 25–30. IEEE (2016).

Barrue, C., Cortes, A., Moreno, J., Cortes, U. Using multiagent systems to mediate in an assistive social network for elder population. In Artificial Intelligence Research and Development: Proceedings of the 18th International Conference of the Catalan Association for Artificial Intelligence, volume 277, page 120. IOS Press. (2015).

Batalden, M., Batalden, P., Margolis, P., Seid, M., Armstrong, G., Opipari-Arrigan, L., Hartung, H.: Coproduction of healthcare service. BMJ Qual. Saf., 25, 509–517 (2016).

Benchoufi, M., Porcher, R., Ravaud, P.: Blockchain protocols in clinical trials: Transparency and traceability of consent. F1000Research 2017, 6, 66 (2017).

Berman, M., Fenaughty, A.: Technology and managed care: Patient benefits of telemedicine in a rural health care network. Health Econ., 14, 559–573 (2005).

Bodenheimer, T., Lorig K, Holman H, Grumbach K.: Patient self-management of chronic disease in primary care. JAMA: the journal of the American Medical Association. ,288:2469–2475 (2002).

Bolduc, M., The future of medical wearables, available online: https://www.mpo-mag.com/issues/2017-06-01/view_columns/the-future-of-medical-wearables 2017 , accessed on 13th Jun 2019 (2017)

Castaneda, C., Nalley, K., Mannion, C., Bhattacharyya, P., Blake, P., Pecora, A., Goy, A., Suh, K.S.: Clinical decision support systems for improving diagnostic accuracy and achieving precision medicine. J. Clin. Bioinform., 5, 4 (2015).

Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S.: Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J. Med. Syst., 43, 5 (2018).

Coleman K., Austin B.T., Brach C., Wagner E.H.: Evidence on the chronic care model in the new millennium, Health Aff. 28 (1) (2009).

Coulter, A., Parsons, S., Askham, J.: World Health Organization. Regional Office for Europe, European Observatory on Health Systems and Policies. Where Are the Patients in Decision-Making about Their Own care?. available online: www.who.int/management/general/decisionmaking/WhereArePatientsinDecisionMaking.pdf, accessed on 10th September 2018 (2018).

Culnan, M. J.: The dimensions of accessibility to online information: Implications for implementing office information systems. ACM Transactions on Information Systems (TOIS), 2(2):141–150 (1984).

Detmer, D., Bloomrosen, M., Raymond, B., Tang, P.: Integrated Personal Health Records: Transformative Tools for Consumer-Centred Care. BMC Medical Informatics and Decision Making, 8(1) (2008).

Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in internet of things: Challenges and solutions., arXiv:1608.05187 (2016).

Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the IEEE International Conference on Pervasive Computing and

Communications Workshops (PerCom 2017), Kona, HI, USA, 13–17, 618–623 (2017).

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: Secure and trustable electronic medical records sharing using blockchain. In AMIA Annual Symposium Proceedings; American Medical Informatics Association: Washington, DC, USA, 2017; Volume 2017, p. 650 (2017).

Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors,19, 326 (2019).

Ekblaw, A., Azaria, A., Halamka, J. D., Lippman, A.: A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data. In: Proceedings of IEEE Open & Big Data Conference, Vol. 13, p. 13 (2016).

General Data Protection Regulation, available online: https://gdpr-info.eu/, accessed on 13th Jun 2019 (2016).

Glasgow R.E., Emont S., Miller D.C.: Assessing delivery of the five 'As' for patient-centered counseling, Health Promotion International, Volume 21, Issue 3, 245–255, available online: https://doi.org/10.1093/ heapro/dal017, accessed on 13th Jun 2019 (2006)

Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J. Med. Syst., 42, 130 (2018).

Isern, D. and Moreno, A.: A systematic literature review of agents applied in healthcare. Journal of medical systems, 40(2):43 (2016).

Ivan, D.: Moving toward a blockchain-based method for the secure storage of patient records. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop; ONC/NIST: Gaithersburg, MD, USA, (2016).

Klein, D. M., Fix, G. M., Hogan, T. P., Simon, S. R., Nazi, K. M., Turvey, C. L.: Use of the Blue Button Online Tool for Sharing Health Information: Qualitative Interviews With Patients and Providers. Journal of Medical Internet Research, 17(8):e199 (2015).

Kushniruk, A., Nøhr, C.: Participatory Design, User Involvement and Health IT Evaluation. Stud. Health Technol. Inform, 222, 139–151 (2016).

Linn, L.A., Koo, M.B.: Blockchain For Health Data and Its Potential Use in Health IT and Health Care, available online: https://www.healthit.gov/sites/ default/files/11-74-ablockchainforhealthcare.pdf , accessed on 24th Nov 2017 (2017).

Mackert, M., Mabry-Flynn, A., Champlin, S., Donovan, E.E., Pounders, K.: Health Literacy and Health Information Technology Adoption: The Potential for a New Digital Divide. J. Med. Internet Res., 18, e264 (2016).

Marmot, M., Allen, J., Bell, R., Bloomer, E., Goldblatt, P.: WHO European review of social determinants of health and the health divide. Lancet, 380, 1011–1029 (2012).

Melnyk, D., Wang, Y., Wattenhofer, R.: Byzantine preferential voting, arXiv:1803.02720 (2018).

Nourie, C.E. (Ed.). (2015, February). Your Medical Records, available online:, from http://m.kidshealth.org/en/teens/medical-records.html, accessed on March 01, 2018 (2015).

Pavlou, P. A.: State of the information privacy literature: where are we now and where should we go? MIS Quarterly, 35(4):977–988 (2011).

Reti, S. R., Feldman, H. J., Ross, S. E., Safran, C.: Improving personal health records for patient-centered care. Journal of the American Medical Informatics Association, 17(2):192–195 (2010).

Schoenberg, R.: Bridged patient/provider centred method and system, in Editor (Ed.)^(Eds.): 'Book Bridged patient/provider centred method and system' (Google Patents, 2013, edn.) (2013).

Szabo, N.: Formalizing and Securing Relationships on Public Networks. First Monday, [S.l.], sep. 1997. ISSN 13960466. available at: <https://firstmonday. org/ojs/index.php/fm/ article/view/548/469>. Accessed on Jun. 2019 (1997).

Wagner, E., Austin, B., Von Korff, M.: Organizing care for patients with chronic illness. Millbank Q. (74):511-544 (1996).

Wagner, E.H., Davis C., Schaefer J., Von Korff M., Austin B.: A Survey of Leading Chronic Disease Management Programs:Are They Consistent with the Literature? Managed Care Quarterly7(3): 56-66 (1999).

Wagner, E.H., Glasgow R., Davis C., Bonomi A., Provost L., McCulloch D., Carver P., Sixta C.: Quality Improvement inChronic Illness Care: A Collaborative Approach, Journal on QualityImprovement 27(2): 63-80 (2001).

Wimmer, H. A multi-agent system for healthcare data privacy. In AMCIS (2014).

Wood, C., Winton, B., Carter, K., Benkert, S., Dodd, L., and Bradley, J.: How blockchain technology can enhance EHR operability. Available online: https://www.hyperledger.org/wp-content/uploads/2016/10/ARKInvest_and_GEM_ Blockchain_EHR_Final.pdf. Accessed on 13th Jun 2019 (2016).

Wu, L., Du, X., Wang, W., Lin, B.: An out-of-band authentication scheme for internet of things using blockchain technology, IEEE Access, vol.7, 58381-58393 (2019).

Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M.: MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757–14767 (2017).

Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: Found healthcare intelligence on Blockchain with novel privacy risk control. J. Med. Syst., 40, 218 (2016).

Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: Fhirchain: Applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J., 16, 267–278 (2018).