Computers, Materials & Continua
DOI:10.32604/cmc.2021.016618
Article

Tech Science Press

HealthyBlockchain for Global Patients

Shada A. Alsalamah[1,2,3,*], Hessah A. Alsalamah[1,4], Thamer Nouh[5] and Sara A. Alsalamah[6]

[1]College of Computer and Information Sciences, King Saud University, Riyadh, 11451, Saudi Arabia
[2]Digital Health and Innovation, Science Division, World Health Organization, Geneva, CH-1211, Switzerland
[3]MIT Department of Mechanical Engineering, Massachusetts Institute of Technology (MIT), Cambridge, 02139, MA, USA
[4]College of Engineering and Architecture, Al Yamamah University, Riyadh, 11451, Saudi Arabia
[5]Trauma and Acute Care Surgery Unit, College of Medicine, King Saud University, Riyadh, 11451, Saudi Arabia
[6]College of Computer and Information Sciences, Al Imam Mohammad Ibn Saud Islamic University, Riyadh, 13318, Saudi Arabia
[*]Corresponding Author: Shada A. Alsalamah. Email: saalsalamah@ksu.edu.sa
Received: 06 January 2021; Accepted: 17 February 2021

Abstract: An emerging healthcare delivery model is enabling a new era of clinical care based on well-informed decision-making processes. Current healthcare information systems (HISs) fall short of adopting this model due to a conflict between information security needed to implement the new model and those already enforced locally to support traditional care models. Meanwhile, in recent times, the healthcare sector has shown a substantial interest in the potential of using blockchain technology for providing quality care to patients. No blockchain solution proposed so far has fully addressed emerging cross-organization information-sharing needs in healthcare. In this paper, we aim to study the use of blockchain in equipping struggling HISs to cope with the demands of the new healthcare delivery model, by proposing HealthyBlockchain as a granular patient-centered ledger that digitally tracks a patient's medical transactions all along the treatment pathway to support the care teams. The patient-centered ledger is a neutral tamper-proof trail time-stamp block sequence that governs distributed patient information across the decentralized discrete HISs. HealthyBlockchain connects patients, clinicians, and healthcare providers to facilitate a transparent, trustworthy, and secure supporting platform.

Keywords: Blockchain; eHealth; electronic health record; global patient; healthcare information system; information security; legacy system; patient-centered care; privacy; smart contract; trust

1 Introduction

Emerging eHealth models are enabling a new era of clinical care that ignites today's global modernization movement toward an individualized, holistic, and integrated healthcare delivery model. This model of care requires the flow of medical information across various healthcare information systems (HISs) to allow its seamless access by the right care team member at the

right time. Various studies in the literature reveal that current HISs interrupt patient treatment continuity, which makes them unsuitable for an individualized model of care. This results from a conflict between the information security goals needed for this new model and those already attained and enforced locally as part of the traditional disease-centered healthcare delivery models. This compromises the availability of the required medical information and places high pressure on healthcare providers to incorporate their HISs while addressing emerging privacy and information security concerns. Meanwhile, blockchain, which has been described as the "most promising technology" in today's technology realm because of the hype and optimism it has generated as an enabler of a new technological revolution, has given rise to a new generation of asset transactional applications [1]. Although most of its applications in the literature have been limited to cryptocurrencies and financial services, a wave of interest in blockchain for various other digital sectors has notably been increasing over the last couple of years, especially in the healthcare space [1–5]. Characterized as a peer-to-peer (P2P) distributed ledger technology, blockchain facilitates the tracking of assets among participants in a decentralized network [4]. At the heart of a blockchain resides trust, which is established to address consensus in entrusted networks, ensure robustness, and facilitate value migration in a decentralized manner [3].

Although several solutions have been proposed to manage legacy information systems (LISs) in general, and healthcare systems in particular [6,7], few studies have explored the use of blockchain to equip legacy HISs beyond theory. However, these solutions fall short of addressing legacy HISs' heterogeneity and inconsistency challenges. Moreover, they do not equip legacy HISs to seamlessly implement modern healthcare delivery models while maintaining their autonomous security policies and access control models. This is the gap in the literature that we intend to address in this study. We aim to study whether blockchain can enhance the ability of struggling discrete and legacy HISs to cope with the emerging cross-organizational information-sharing needs of the modern healthcare movement, which is an important aspect of delivering better patient experience and care. We believe that this topic has not been comprehensively investigated in the literature. The remainder of this paper is organized as follows. Section 2 introduces the reader to modern healthcare services. Section 3 discusses the data-sharing and protection dilemma emerging from modern eHealth services, whereas the fundamentals of blockchain technology are presented in Section 4. In Section 5, we outline the literature dealing with the use of blockchain solutions in healthcare. Section 6 presents the methodology implemented for this project. Section 7 illustrates the design of the HealthyBlockchain and a thorough analysis of how HealthyBlockchain can potentially address the challenges faced by HISs. Section 8 discusses the clinical adoption of the HealthyBlockchain. Finally, in Section 9, we present our conclusions.

2 Modern Healthcare

One of the early definitions of patient-centered care can be found in [8]:

"A collaborative effort [...] where patients and the healthcare professionals collaborate as a team, share knowledge and work toward the common goals of optimum healing and recovery."

As part of the global adoption of patient-centered care over the last couple of decades [9–11], patient treatment has shifted from a traditional [9], fragmented disease-centered approach toward an integrated individualized one [10–14]. Emerging healthcare models have utilized information communication technology (ICT) to enhance collaboration, communication, and coordination in the health sector [15,16] to provide a holistic view of the patient's condition [14,17]. This approach puts the patient at the heart of these healthcare services and integrates and tailors care around the patient's needs and current state [10,11,18,19]. While traditional disease-centered care

models emphasize record keeping [18], the patient-centered approach creates a "culture of open information" [19] emphasizing accessibility to patient information [18], teamwork and collaboration [14], and shared decision-making through regular multi-disciplinary team reviews [13,19]. The shift from disease-centered to patient-centered healthcare is illustrated in Fig. 1.

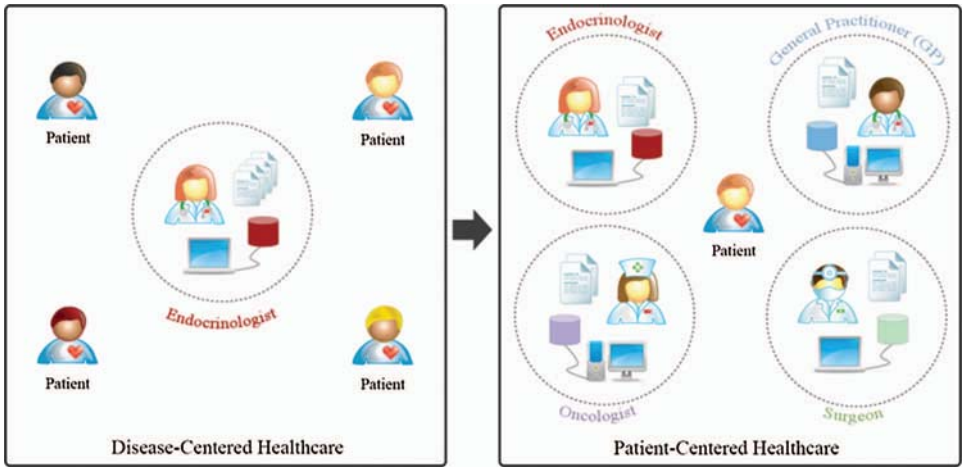

Figure 1: Shift from disease-centered care to one that is patient-centered [20]

The digital transformation of healthcare using emerging technologies, such as ICT, cloud computing, Internet of Things (IoT), and mobile and wearable devices, has the potential to enhance health outcomes by improving medical diagnosis, data-based treatment decisions, digital therapeutics, clinical trials, self-management of care, and person-centered care, as well as create more evidence-based knowledge, skills, and competence for professionals to support health care. Electronic Healthcare (eHealth) plays an increasingly significant role in shaping modern healthcare in such areas as mobile health (mHealth), ubiquitous healthcare (uHealthcare), telemedicine, and virtual healthcare. Regardless of the technology used, these models mainly aim to connect healthcare providers, clinicians, and patients to enable a seamless flow of medical information between healthcare settings to virtually form a complete electronic patient record for making informed decisions. Furthermore, they facilitate the global movement toward a holistic, integrated, and patient-centered healthcare delivery model (also known as individualized care [21], or shared care [12]) [15,18,22,23]. Such a shift is introduced to enable "a new era of clinical care [...] that empower patients, researchers, and providers to work together toward the development of individualized care" [21].

3 Data-Sharing *vs*. Protection Dilemma

According to Cancer Center's Caldicott Guardian Crosby [24], "More harm is done to the patient if his information is not available to the care team member when needed than it falling into the wrong hands." Hence, sharing patient data across heterogeneous HISs so that it is accessible to other care teams is fundamental for the successful implementation of the new patient-centered care model [25,26]. Nonetheless, the World Health Organization (WHO) Global Strategy on Digital Health 2020–2025 [27] classifies health data as sensitive personal data or personally identifiable information, which emphasizes the need for a strong legal and regulatory base to protect the privacy, confidentiality, and integrity of personal health data and to deal with

cybersecurity, trust building, accountability and governance, ethics, equity, capacity building, and data literacy issues. This is to ensure that good-quality data are collected and subsequently shared to support planning, commissioning, and transformation of services. Therefore, shared care in multiple healthcare provider settings puts acute pressure on healthcare providers to address emerging privacy and security concerns, making trust management (TM) one of the most challenging issues in this area due to the open and anonymous nature of digital environments [26,28]. This anonymous nature of our digital world undoubtedly demands reliable, trustworthy health systems and applications that can ensure that shared care is implemented securely. Information security in the context of healthcare information systems implies that only the right medical information is available to the right care team member at the right point in time [29]. This is also owing to the complicated system of global legislation that the healthcare providers must comply with. These laws include, but are not limited to, the Data Protection Act [30], Access to Health Records Act [31], Computer Misuse Act [32], Human Rights Act [33], the Health Insurance Portability and Accountability (HIPPA) Act [34], Caldicott Guardian Principles [35], the European General Data Protection Regulation (GDPR) [36], and the New York State Department of Financial Services' mandatory cyber security requirements [37]. They collectively aim to articulate how personal patient information must be handled and provide clear rules on how any processing of such information in a cross-system shared care environment should be carried out and controlled. For instance, according to the Data Protection Act 1998, Caldicott Guardian Principle 4 implementation in the UK clearly states that: "Access to patient identifiable information should be on a strict need-to-know basis" [35], and the GDPR emphasizes the patient's consent is the basis for any data processing [38], whereas the major goal of HIPPA's Privacy Rule implemented in the US is to: "Assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality healthcare and to protect the public's health and wellbeing" [39]. Therefore, healthcare providers who share patient information with other team members across their information systems have no option but to carefully balance between making the right medical information available to the right user whenever needed and maintaining information confidentiality.

Healthcare is an increasingly data-driven domain [6] that suffers from a growing collection of legacy systems, networks, and applications [6,10,29,40]. These legacy systems are often brittle, slow, and non-extensible discrete legacy information systems [29]. Such legacy systems are typically the backbone of the patient care flow, and their failure can have a serious impact on patients' care [7]. Furthermore, healthcare providers cannot afford to discard these systems as they contain historical medical data based on an aging population [29]; therefore, global efforts to modernize health care systems, including in the United Kingdom, favor an evolutionary approach over a revolutionary one that involves using legacy systems so that they are gradually replaced with newer systems [7,11,13,19,40,41]. Bisbal et al. [7] define an LIS as "any information system that significantly resist modification and evolution" [7]. In addition, this evolutionary approach is less expensive and has a lower risk of failure compared with alternative approaches [7], where the legacy systems are totally discarded and replaced with newer ones, which can have a serious impact if the information becomes unavailable or lost. Hence, it is important not to discard a legacy system, but rather to evolve it [7,10,40]. Therefore, it is not surprising that the transformation from legacy systems supporting a traditional approach to systems supporting patient-centered care is a concrete challenge the UK National Health Service (NHS) is facing [13,42]. Data in the old format are stored in standalone information silos and need to be converted into the format required by the new integrated support systems [42]. The evolutionary movement in the NHS is based on the principle of "keeping what works and discarding what has failed" [10]. This implies

that new integrated systems are built on the foundations of fragmented LISs [10]. Nonetheless, enabling information-sharing across healthcare providers with legacy systems without doubt poses several information security risks that threaten the effectiveness, dynamism, and potential of this collaboration. This has been evidenced by results from a study [29] conducted in 2016 to evaluate healthcare systems' readiness for patient-centered care at the Velindre Cancer Center [43]. Velindre, one of the largest NHS divisions and cancer centers in the UK with an annual budget of over £49 million, provides specialist cancer services to over 1.5 million people in South East Wales and beyond [43]. Using domain analysis, conceptual modeling, and 12-h observation of current practices, as well as semi-structured interviews, this study investigated three different types of cancers in-depth: hepatocellular, upper gastrointestinal, and breast cancers [29]. The results show that the studied healthcare systems fall short of meeting the minimum requirements of modern healthcare delivery models because of the availability, integrity, and confidentiality of medical information being seriously compromised, as shown in Tab. 1 [44]. Furthermore, the above threats result in legacy systems blocking the flow of medical information (see Fig. 2) [45]. This is because, first, the legacy systems were designed to meet the traditional disease-centered model [29], and hence, they cannot enforce their policies outside of their physical boundaries. Second, they lack a clear information security policy to govern exchanged patient-centered information at the collaboration level across those healthcare providers' systems.

Table 1: Information security threats posed by health care legacy systems [29]

Threat category	Threat description
Information integrity threats	Human error
	Inconsistent results in different systems
Information availability threats	Disconnected systems at major sharing points
	Inconsistent information security policies
	Inflexible balance of information security in emergency cases
	Inconsistent user-hostile information system design
	Untraceable shared information
	Manual management of referrals between health care providers
Information confidentiality threats	Improper disclosure of medical information
	Hospital-wide access control

4 Blockchain Technology: The "Internet of Individuals" [46]

Blockchain technology is being celebrated as an enabler of a new technological revolution [1]. Defined as "a peer-to-peer distributed ledger technology for a new generation of transactional applications that establishes transparency and trust." [4], Blockchain is a *distributed and sustainable* ledger, not a database solution, which is *transparent and auditable*, as it digitally tracks asset transactions between a group of networked peers. The ledger also provides a transparent tamper-proof trail of timestamps of block sequences that are algorithmically self-policed to support *secure, private, and indelible* transactions. This shifts the information-Internet into a value-Internet by addressing consensus in trustless networks, ensuring robustness, and facilitating value migration

in a decentralized manner [3]. This *consensus-based and transactional* infrastructure helps support end-to-end processes in an *orchestrated and flexible* manner.

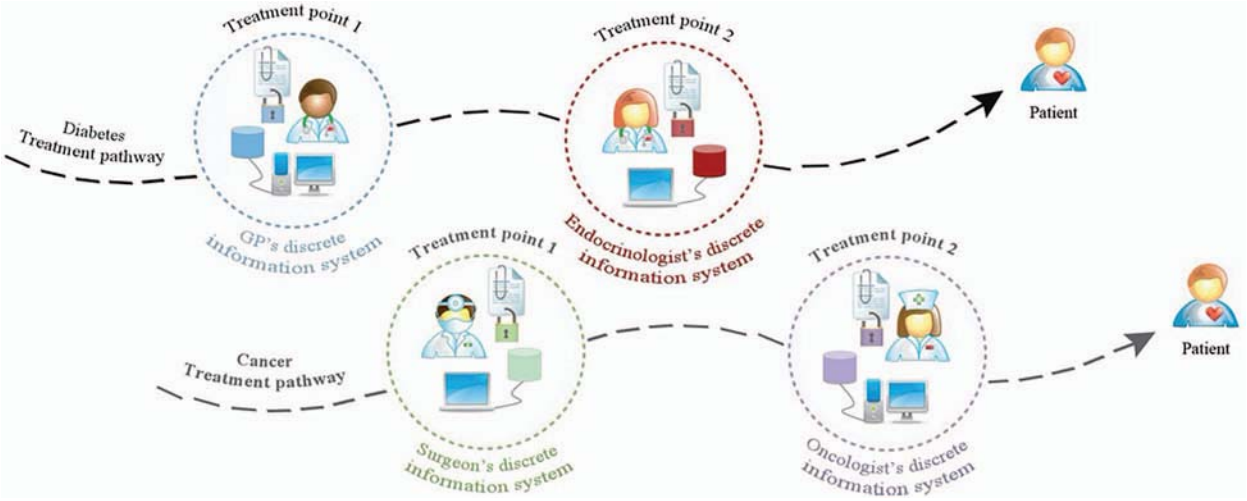

Figure 2: Health care legacy systems are blocking medical information flow [45]

Blockchain technology holds the potential to reconfigure human activity in a new disruptive computing paradigm [47]. In a World Economic Forum survey dated September 2015, 58% of all survey respondents said that they expected that by 2025, 10% of global gross domestic product will be stored using blockchain technology [5]. This anticipated revolution can be categorized into three waves: Blockchains 1.0, 2.0, and 3.0 [47]. The deployment of cryptocurrency, blockchain 1.0, was the first wave of change. Blockchain 2.0 is the next evolution of technology that enables decentralized smart contract systems. The more recent wave of interest, blockchain 3.0, demonstrates the technology's application beyond currency. The remainder of this section addresses the fundamentals of blockchain to highlight its potential to be harnessed in the healthcare domain.

The fundamental components underlying blockchain technology are distributed peer-to-peer networks, digital transactions, and shared ledgers [48]. In a blockchain a group of distributed participants are linked by a peer-to-peer communication network, where each participant houses an identical copy of the blockchain and contributes to its governance. It is *secure, private, and indelible* as participants reference each other via their public keys, and use their private key to cryptographically sign transactions. Blockchain also supports a *consensus-based and transactional* ledger in which digital transactions refer to the assets to be maintained by the blockchain, which are recorded into a shared ledger. The inclusion of new transactions into the ledger requires consensus and confirmation of participants based on a set-upon verification process. Once verified, the new transaction is propagated to all the copies of the blockchain. Transactions in the ledger have a timestamp and a unique cryptographic hash, which makes the ledger a verifiable history of the transactions in the network.

The data structure of a blockchain is an ordered sequential chain of cryptographic hash-linked blocks of digital transactions. Each block is identified by a cryptographic hash and timestamp. Each block is also linked back to the previous block, i.e., the parent block, in the chain. The hash of the parent chain is maintained in each referencing block's header, thus linking each block to its parent and achieving a temporal ordering of transactions up to the genesis block

(first block in a blockchain). Any change in the identity of the parent necessitates a change in the referencing block and hash that cascades throughout the blockchain. This ensures that the history of the blockchain remains immutable [49] through an orchestrated and flexible blockchain ledger with a lifetime process history.

The architecture of a blockchain can be categorized as either permissionless (i.e., public), permissioned (i.e., semi-public or consortium), or private. Public blockchains, such as Bitcoin [50], are often large and decentralized, where participants at any level can engage in the blockchain. Therefore, a public blockchain is completely trustless, where none of the participants are given special privileges. In permissioned blockchains, which are partially decentralized, participation can be controlled; however, permissioned blockchains are viewable to the public. Compared with public blockchains, networks utilizing a permissioned architecture have low latency and high storage capacity. A private blockchain, on the other hand, is privately shared by a trusted organization and is not viewable to the public. Transactions are quicker compared with other architectures, with almost no latency, as they are verifiable by fewer participants.

The exchange of information between participants in a blockchain is governed by a decentralized consensus. This consists of a series of standards and rules that direct transactional contributions or exchanges to ensure an unambiguous, immutable ordering of transactions to guarantee the integrity and consistency of the blockchain among trustless participants in a scalable setting [47]. In a permissionless architecture, any participant can take part in the consensus process, whereas a consortium of participants in a permissioned or private architecture governs the consensus process. As the nature of blockchain transactions varies, various models are used for creating consensus. The choice of a consensus model is often dependent on the expected threat to the network and the degree of trust in the participants operating the blockchain. For instance, Bitcoin operates a consensus model called "proof of work" to prevent malicious attacks on trade histories and permissionless ledgers. Several other consensus models have been proposed, for example, proof of stake, variants, and hybrid. The efficacy of a consensus model is determined by three key properties: safety, liveness, and fault tolerance. A consensus model guarantees safety by maintaining a consistent shared state, liveness by producing a consensus from non-faulty participants, and fault-tolerance by recovering from a participant's failure [51].

Immutability is one of the defining features of blockchain technology. The immutability mechanisms of blockchain also imply that they are auditable, as the authenticity of every transaction is recorded in the blockchain. This means that blockchain design supports a systematic and independent examination of transactions to determine their temporal validity and thus enforce accountability [52]. For instance, Bitcoin's economic accountability is made possible via its proof-of-work consensus model, which makes corruption prohibitively expensive and immediately detectable, which means the Bitcoin is tamper-resistant [51]. A transaction's audit trail further supports provenance tracking, where the history of ownership, source, or origin is transparent and tractable. One of the earliest applications of blockchain for the provenance tracking of physical goods was the provenance of diamonds [53].

5 Related Work

ICT is enabling an emerging generation of intelligent healthcare delivery models that are integrated, holistic, personalized, and even mobile [44]. However, patient-centeredness requires informed decision-making processes that are shared among care providers. This can only be achieved through seamless access to relevant siloed information held in discrete electronic medical record (EMR) systems [44]. Nevertheless, current systems fall short because of their heterogeneity

and inconsistencies across EMR systems in terms of security policies and access control models [44]. Blockchain technology is seen as offering promising possibilities for the healthcare sector. Although few studies have explored the potential of blockchain in healthcare, there still are a number of promising proposals that may contribute to enabling personalized care through blockchain-based EMR solutions. Azaria et al. [54] proposed MedRec to overcome the existing barriers to effective cross-organizational information-sharing caused by legacy HISs or traditional EMR systems. This should eventually address miscommunication issues between patients and healthcare providers; this is to prioritize a patient's involvement in their care and reduce direct third-party involvement. MedRec handles a unified patient-centered EMR using a decentralized blockchain-based record management system, integrated with the patient's healthcare providers. Using permission management, it sustains and secures the network via proof-of-work by various medical stakeholders with the incentive to become blockchain miners. As a reward, MedRec provides access to aggregated and anonymized data. The proof-of-work algorithm is based on a trustless model that is used to secure the content from tampering, where individual nodes must compete to solve computations before the next block unit is added. This creates a comprehensive, immutable, accessible log to the patient's medical information across providers and treatment sites. Conceição et al. [55] proposed the implementation of an integrated blockchain-based large-scale architecture to access EMRs. They utilize a blockchain smart contract to enable secure access to EMRs. Abdelkhalek et al. [56] suggested a roadmap to improve the performance of EMR using blockchain in the health sector. The authors suggested connecting all health facilities to a unified network using blockchain technology. The road map touched many technical and non-technical aspects that should be considered, including improving the current EMR, unifying medical terminologies, introducing awareness programs to public and medical societies, and developing laws, legislations, and health procedures. Tanwar et al. [57] proposed an access control policy architecture and algorithm to facilitate access to EMRs, supporting the simulation of environments to implement the hyperledger-based EMR sharing system that uses the concept of a chain-code.

Furthermore, Yue et al. [58], AlOmar et al. [59], and Xia et al. [60] revolutionized EMR systems by enforcing tighter security countermeasures for access control. Yue et al. [58] proposed a healthcare data gateway (HGD) as a blockchain solution that gives patients control and access rights to their medical data. Access in HGD is more controlled than in MedRec because it is based on a stricter purpose-based information access scheme. The EMRs in HGD are managed using a blockchain-based storage system that authenticates all data access requests based on a purpose-centered information security principle. In addition, it utilizes a secure multiparty computation (MPC) mechanism to allow third parties to process patient data without risking patient privacy. Meanwhile, AlOmar et al. [59] proposed MediBchain, which is similar to HGD in that it revolutionizes EMR systems by using secure countermeasures for authentication, but with an extra focus on the identification of participants. Xia et al. [60] proposed MeDShare, which adds an extra layer of protection by monitoring entities that access data for malicious use from a data custodian system. This is achieved by employing smart contracts and an access control mechanism to effectively track the data behavior. Although the solutions may vary in their approach or security aspect, they share commonalities in terms of the content and type of blockchain used. All frameworks aim to store transactions in relation to a patient's medical information that needs to be accessed to make an informed decision about the best treatment options. This blockchain is distributed among EMR systems at various healthcare settings based on permissioned blockchain solutions that allow access to only invited, and hence verified, users.

This complies with the information security and data protection laws and regulations for medical records [58].

6 Methodology

Using a mixture of qualitative research methods, we, first, conceptually modeled the information flow between different treatment points along a well-defined and globally accepted breast cancer treatment pathway and implemented using business process modeling. This pragmatic approach was necessary to fully understand the challenges posed by LISs, as we had to define a scope while using real systems to achieve our goals. Second, we studied the implementation of individualized care using current discrete information systems. Third, we identified the challenges hindering the full implementation of the discrete information system by mapping the results with the conceptual model. Finally, we designed a blockchain that would address these challenges and equip the LISs to fully implement personalized care. The results of the above steps can be found in multiple publications (for details, see [44,45]). This paper focuses on the final step, as explained in the following section.

7 HealthyBlockchain: Refurbishing Health Care Services Using Blockchain Technology

A block is the smallest unit in a blockchain, and is conceptually similar to a database primary index. A block does not store the data, but keeps track of where data can be found. Therefore, it is effectively a bookkeeper of all the treatment points that the patient is undergoing. As the patient goes down his or her treatment plan, each block is initiated and completed by a single care team member, and links back to a previous block within the list (i.e., a chain in our context). All blocks within a patient's chain should have the same data structure. Each block unit represents a new transaction of value (patient medical information collected or processed in a treatment in this context) and has a *block header* and *block content*. The block header keeps track of the blockchain details to relate this block to the chain whereas the block content keeps track of the patient's medical information generated at each treatment point. This information is then associated with the layers of metadata to put the details of the treatment point in context. The metadata details include the team member originating from this treatment point, treatment session details, the hospital where this information has been collected and processed, and, finally, the owner keys details (see Fig. 3A).

To implement an access control model that can govern the patient data on HealthyBlockchain at the global level, an 8-level fine-grained information classification scheme is designed, as illustrated in Fig. 3B.

Access control authorization is managed through public and private keys. *HealthyBlockchain* manages the private and public keys of each patient's care team members in the following two scenarios.

Private Data-Sharing: This scenario aims to share information privately between two specific health care professionals, let us say between a patient's general practitioner (GP) and her psychologist after the recent suicide attempt by the patient. The GP does not want to share the patient's personal and psychological details with her surgeon. Hence, the GP uses the psychologist's public key to sign the report and pass it along to the psychologist, who then decrypts the report using his private key.

Public Data-Sharing: This scenario aims to share information publicly with the remaining care team members while clearly showing the report originator (i.e., owner) for ensuring data integrity

and authenticity. In this scenario, the GP would like to share with her care team the details of a recent follow-up visit at his clinic after the patient has successfully completed a treatment plan. The GP uses the GP's public key to decrypt the report and see it.

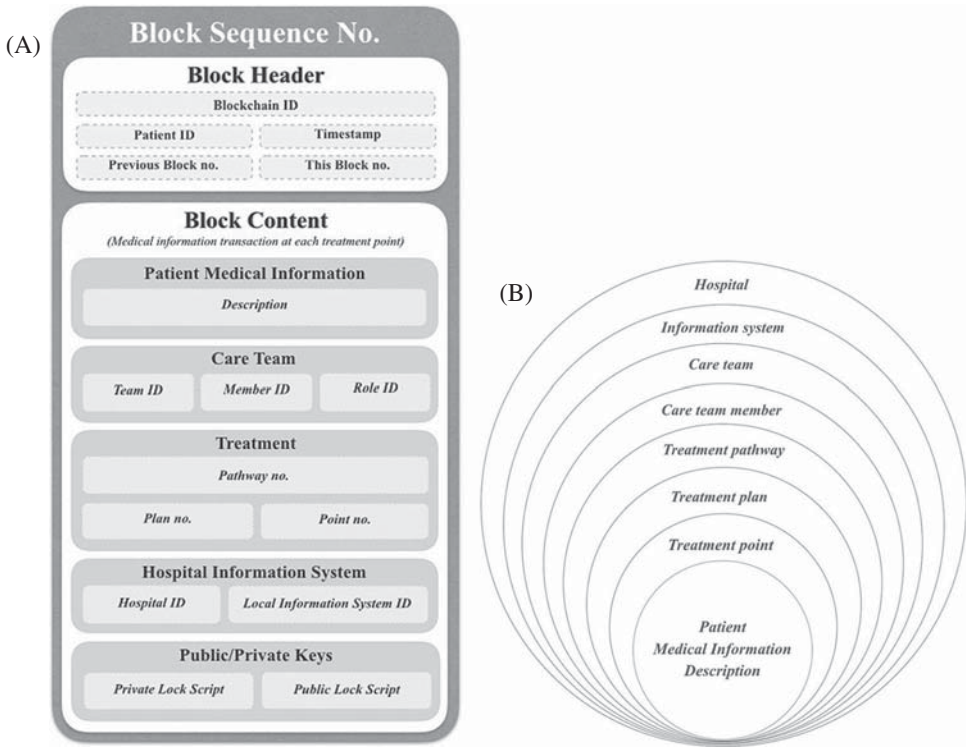

Figure 3: (A on the left) Anatomy and granularity of HealthyBlockchain's unit of block. (B on the right) Fine-grained information classification scheme of eight layers for HealthyBlochain data governance

Fig. 4 illustrates an instance of a HealthyBlockchain that is patient-centered in action and digitally signed by each care team member with their private key before releasing to the patient's blockchain following the patient-specific treatment pathway. Eventually, the sequence of blocks is added into a ledger presents the complete scenario.

Putting It All Together

HealthyBlockchain uses private and permissioned blockchains, the former to comply with jurisdictional, international health data protection acts and the latter to implement role-based accessed control to allow only those participants allowed to write on the blockchain. The Healthy-Blockchain backend solution comprises two key components: a local hospital information system for off-chain data and a patient-centered ledger for on-chain data (see Fig. 5). The former component handles the off-chain data stored in the local EMRs by the care team all along the treatment plan. Once a record is created or updated in the local hospital information system, the smart contract is invoked to create a new treatment transaction record based on the treatment point details following the information classification scheme.

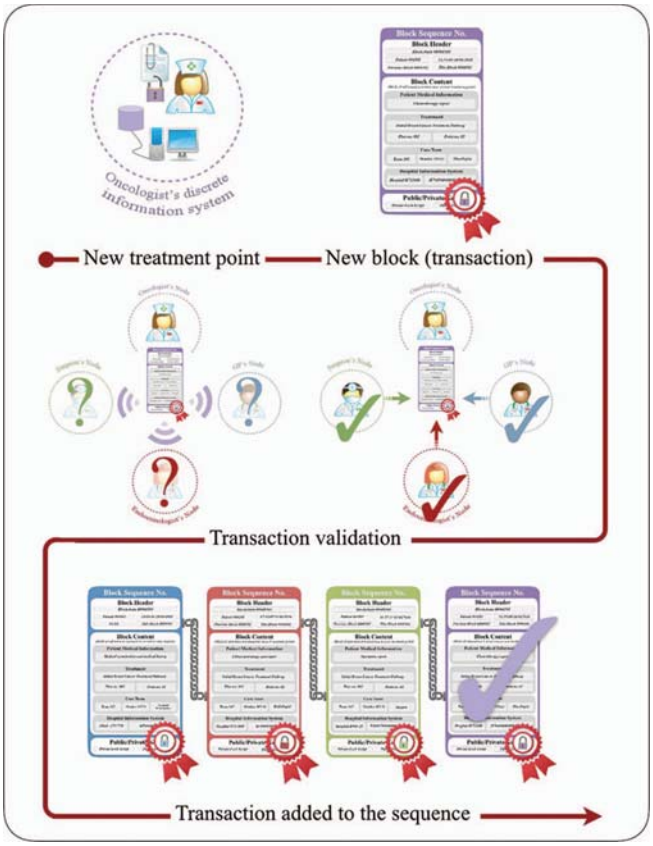

Figure 4: HealthyBlockchain in action and digitally signed by each care team member with their private key before releasing it to the remaining care team to validate the new treatment transaction (block unit) before it is added to the patient's blockchain sequence

In this paper, we propose *HealthyBlockchain* as a fine-grained, comorbidity-oriented, patient-centered ledger that digitally tracks each patient's medical transactions along all followed treatment pathways and for all the involved care teams while they keep using their local systems. At each treatment point, a block with 8-levels of granularity is automatically generated with a description of the recorded information in the local system on a digitally signed block. This is to provide a unified block sequence for patients with tamper-proof trail time-stamps, which is a neutral, conflict-free information policy implemented through a smart contract that governs patient-centered information across decentralized ledgers. *HealthyBlockchain* connects patients, clinicians, and healthcare providers to facilitate a transparent, trustworthy, and secure patient-centered healthcare delivery model required to cope with the demands of today's global patient healthcare needs. This should be incorporated into this modernization movement rather than being a burden that needs to be discarded; this is intended to build a better quality of care for a better tomorrow. See Fig. 6 below.

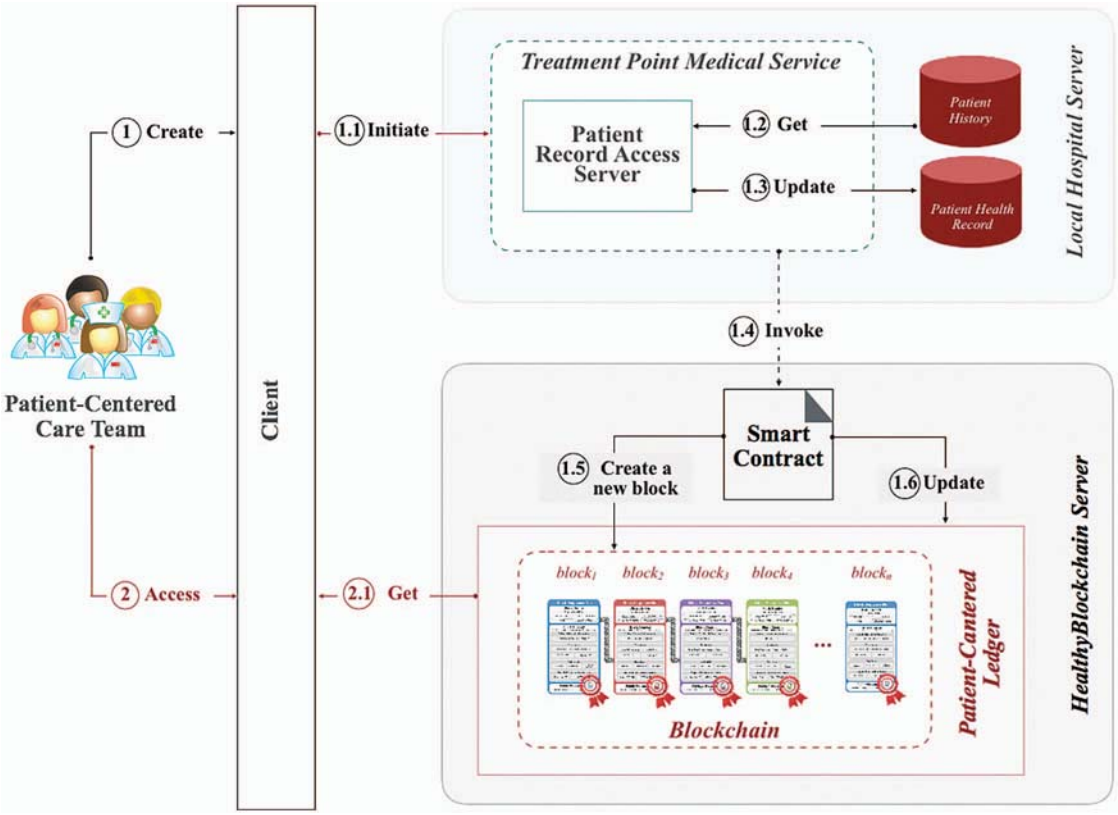

Figure 5: HealthyBlockchain software components and data flow

As identified earlier, the information security threats posed by healthcare legacy systems include: integrity, availability, and confidentiality (explained in section three). HealthyBlockchain addresses these threats as follows (and summarized in Tab. 2):

Information Integrity. Preserving the accuracy of patient medical information systems is one of the challenges in LISs. Restoring the right level of information integrity to suit modern care delivery, medical information needs to be organized in a chronological order so that owners can track the origin of invalid information resulting from a human error incident and act upon it. HealthyBlockchain is transparent and auditable, as all transactions and participants are verified in near real time when a block is added. Thus, transactions are time-stamped and tamper-proof and are represented in a block sequence, each representing a treatment point. Moreover, an important requirement in the healthcare domain is that medical data collected along patient treatment points should never be deleted; it simply has to become a part of the medical history. This is owing to the fact that this data are the basis for treatment decisions and hence any required updates to this data will imply going back to all decisions made on invalid data and trying to fix it. Therefore, any updates made to the data need updating the history to track the timeline. HealthyBlockchain is secure, private, and indelible in this regard as all medical history and decisions made based on them are recorded and never deleted. In addition to the treatment details, each block is digitally signed by the care team member participating as the owner to ensure the authenticity of the data provided. Validation following any signed block implies that everyone will be aware of all updates to a particular patient's data, leaving very little scope for human error not being spotted.

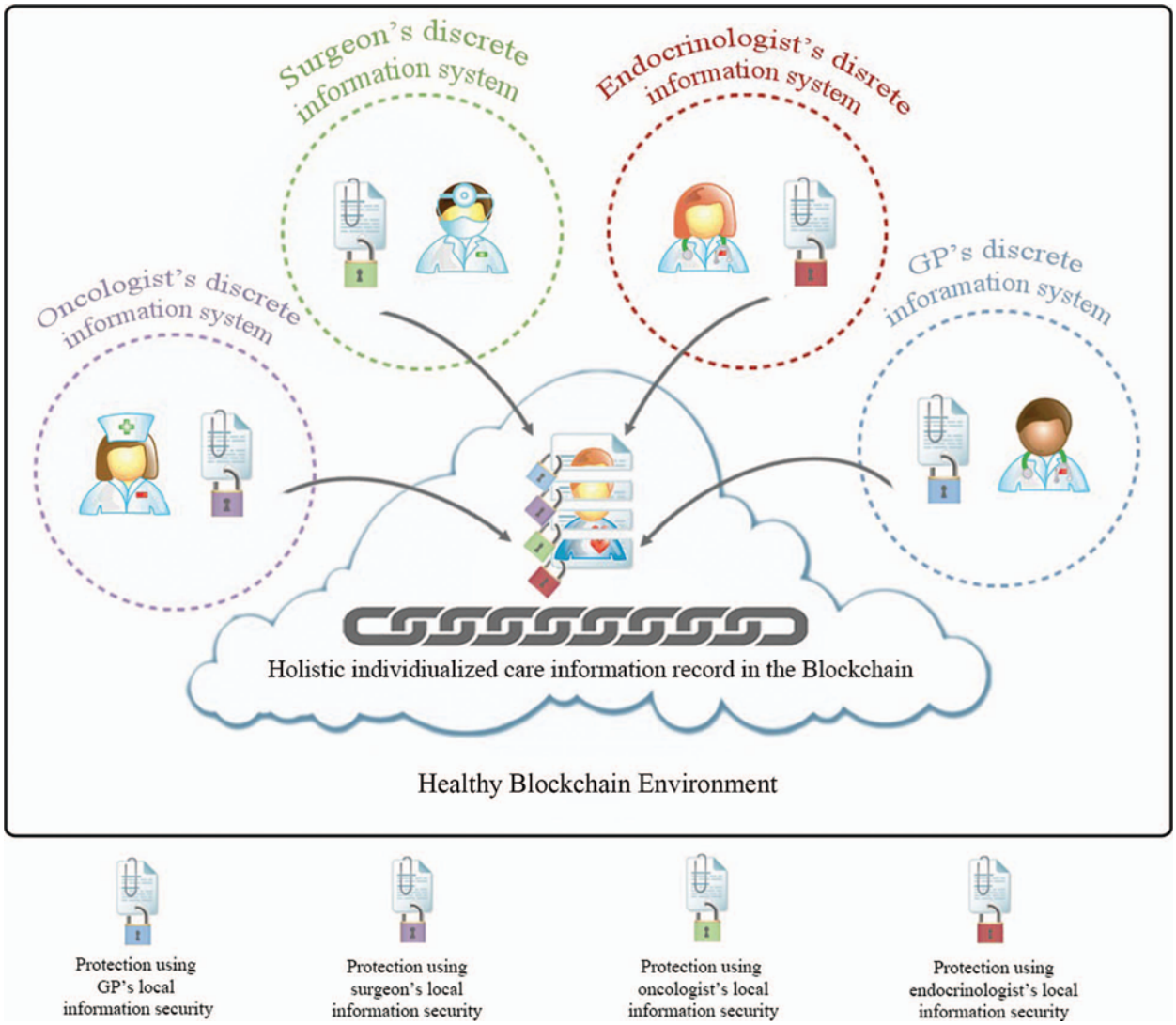

Figure 6: Incorporating blockchain technology into patient-centered care movement

This is also recorded in the HealthyBlockchain ledger that summarizes the chronological order of treatments and care team members involved without the need for any replications in different systems, which may cause inconsistencies.

Information Availability. Access to medical information across distributed and heterogeneous hospital legacy systems is currently not supported in HISs. Therefore, a common collaboration-driven information access to overarching local organization-driven policies is required. Healthy-Blockchain is distributed and sustainable, which allows access to medical information through its neutral decentralized consensus.

It is also orchestrated and flexible to include historical lifetime treatment stages and support end-to-end treatment flow. Information security policies within the medical information legacy system are also inconsistent, which also hinders information-sharing. HealthyBlockchain governs the visibility of the medical information, according to the permission rules set by its owner, as it

is secure, private, and indelible. It uses cryptographic techniques to present selected views of the ledger to participants and to the fine-grained layers in each block.

Table 2: HealthyBlockchain addressing threats posed by health care legacy systems

Threat	Distributed	Secure	Transparent	Consensus	Orchestrated
Human error		YES	YES		
Inconsistent results in different systems	YES				YES
Disconnected Systems	YES				YES
Inconsistent security policies	YES	YES			
Inflexible balance of information security in emergency cases			YES	YES	
Inconsistent user-hostile information system design	YES				
Untraceable shared information			YES		
Manual management of referrals between healthcare providers	–	–	–	–	–
Improper disclosure of medical information			YES	YES	
Hospital-wide access control			YES		YES

A consistent information organization that provides a patient-centered holistic view and allows easy access to patient clinical information is needed within the modern healthcare delivery landscape. Within HealthyBlockchain, this is supported by the data structure of the ordered sequential chain of cryptographic hash-linked blocks. Each block is also linked with a cryptographic hash and time stamp. Moreover, the sequence of the blocks is added into a shared ledger, which provides a lifetime history of all transactions. Thus, the ledger within the distributed and sustainable HealthyBlockchain is comorbid-oriented and presents the full picture of each patient's medical case. Further, the gathering and filtering of relevant information to avoid overwhelming the care team members with irrelevant information is required to increase the chances of finding the right information at the right time. HealthyBlockchain allows participants to join the chain

as its architecture permits this, and each participant governs the visibility of the information they add through the smart contract, including the owner's key details. This could also be filtered throughout the 8-layers of granularity within each block. The resilience of emergency cases is a crucial requirement that speeds up access to information for decision-making in a life-or-death situation. The central point of information governance within HealthyBlockchain supports the release of the private keys as the emergency case requires. This is again controlled by having a consensus-based and transactional blockchain to grant access as per the situation and also a transparent and auditable blockchain that tracks every transaction. HealthyBlockchain does not address automated referral among different healthcare providers with the right information. However, it is proposed as a future work through the use of business process management to support predefined clinical pathways.

Information Confidentiality. Common collaboration-driven information access needs define the line between the two conflicting information security goals: availability and confidentiality. The comorbid-oriented and fine-grained digitally signed block by care team members supports this in the HealthyBlockchain.

Information security policy awareness in a culture of open information is required to raise the awareness of care team members in terms of how to look at another member's information so as to help preserve the confidentiality of shared information. The digital signature supports hospital-wide access control, whereas the smart contract supports it across hospitals. This is due to the transparency and auditability of HealthyBlockchain for in-house information exchange, and the orchestrated and flexible platform is supported by the HealthyBlockchain for cross-organizational exchange.

8 Clinical Adoption of HealthyBlockchain

Healthcare providers utilize multiple IT solutions to deliver medical care (documentation, laboratory, imaging). Information is exchanged freely between these systems within the confines of the healthcare provider following an information security policy that allows free flow of information between systems while protecting aggregated medical information from external threats and maintaining access to healthcare providers according to their security privileges. Although this system works well, it might benefit from blockchain technology. There is a clear need for the incorporation of HealthyBlockchain in healthcare when the patient moves from one level of care to another that is external to the security zone of his/her healthcare provider. When the patient moves from primary to secondary, tertiary, or quaternary care, the medical information is currently not well shared and is through a written medical report or the patient's verbal narrative. The difficulties faced by the healthcare system with this approach is that a medical report "summarizes" all the medical data in a couple of pages, and this does not grant the receiving provider access to all of the original data (physician documentation, nursing documentation, imaging, laboratory, pathology), wherein there is a deficiency in the medical report or further information that was not included in the medical report is needed. Moreover, relying on the patient's account provides another challenge as patients differ in their ability to communicate the correct information based on their understanding, memory, preference, or benefit. To overcome this, many healthcare providers and institutions rely on evaluating the patient as if new to the system, having to redo many of the assessments because of their inability to access the patient's file from the previous institution and driven mostly by genuine patient care needs and sometimes to address potential medicolegal areas of care.

HealthyBlockchain can eliminate these security concerns as it allows the seamless flow of clinical information from the security zone of one care provider to the other in a secure traceable manner. This will cause a massive reduction of waste in healthcare expenses and the prevention of potential complications, delays, and mismanagement due to the lack of information flow, by maintaining the patient at the center of healthcare without compromising information security. One of the very important concerns in the HealthyBlockchain process relates to the control of the blockchain. HealthyBlockchain can be designed to be controlled by healthcare providers, payers, patients, or the government (if not in the roles of provider or payer). Each option has its advantages and drawbacks. Ideally, the provider generates a blockchain for a patient's entire medical record. The control for allowing other health care providers (institutions or individual physicians) would be with the patient. In this way, patients are empowered and assured that their medical information is accessible by legit care providers, and the providers can conveniently access the medical record its entirety without any constraints on the selection of information.

9 Conclusions

This paper asserts the blockchain technology to be an enabler for the transformation of the healthcare sector rather than a hindrance if the migration is conducted with the absolute minimum risk. HealthyBlockchain has been proposed to support collaboration among healthcare providers in modern healthcare with the use of legacy systems. HealthyBlockchain could act as a top layer to evolve their operation to support distributed, secure, consensus-based, transparent, and flexible transactions across healthcare organizations. We propose the HealthyBlockchain architecture to illustrate how it will operate technically with the existing infrastructure. In terms of the clinical adoption of HealthyBlockchain, we describe the flow of data among software components to address integrity, availability, and information security threats within legacy healthcare systems. Regardless of technological hiccups, blockchain has every opportunity, with minimal risks, to transform the health of aging nations and to facilitate limitless personalized care to patients globally.

Funding Statement: This work received funding from Ibn Khaldun Fellowship for Saudi Women in partnership with the Center for Clean Water and Clean Energy at MIT, and the Deanship of Scientific Research at King Saud University through research Group No. RG-1438-002.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th Int. Conf. on e-Health Networking, Applications and Services (Healthcom)*, Munich, Germany, pp. 1–3, 2016.

[2] A. Tandon, A. Dhir, A. K. M. N. Islam and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Computers in Industry*, vol. 122, no. 12, pp. 103290, 2020.

[3] H. Zhao, Y. Zhang, Y. Peng and R. Xu, "Lightweight backup and efficient recovery scheme for health blockchain keys," in *IEEE 13th Int. Symp. on Autonomous Decentralized System*, Bangkok, Thailand, pp. 229–234, 2017.

[4] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health IT and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States, pp. 1–10, 2017.

[5] World Economic Forum, "Deep Shift Technology Tipping Points and Societal Impact, Global Agenda Council on the Future of Software & Society: Survey Report," 2015. [Online]. Available: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.

[6] T. Paparella, "Healthcare Legacy Systems: How to retire them, reduce costs and maintain access to all the data using active data archiving," *HIMSS Weekly Insider*, pp. 1–4, 2013.

[7] J. Bisbal, D. Lawless and J. Grimson, "Legacy information systems: Issues and directions," *IEEE Software*, vol. 16, no. 5, pp. 103–111, 1999.

[8] International Alliance of Patients' Organizations (IAPO), *What is Patient-Centred Healthcare? A Review of Definitions and Principles*, 2nd ed. London, United Kingdom: International Alliance of Patient' Organizations, 2004.

[9] G. Ellingsen and K. Røed, "The role of integration in health-based information infrastructures," *Computer Supported Cooperative Work (CSCW)*, vol. 19, no. 6, pp. 557–584, 2010.

[10] Department of Health, *The New NHS: Modern, Dependable*. London, United Kingdom: The Stationary Office, 1997.

[11] O. Allam, "A holistic analysis approach to facilitating communication between general practitioners and cancer care teams," Ph.D. dissertation, Cardiff University, United Kingdom, 2006.

[12] E. Smith and J. H. Eloff, "Security in health-care information systems-current trends," *International Journal of Medical Informatics*, vol. 54, no. 1, pp. 39–54, 1999.

[13] A. Skilton, "Using team structure to understand and support the needs of distributed healthcare teams," Ph.D. dissertation, Cardiff University, United Kingdom, 2011.

[14] H. Al-Salamah, W. A. Gray and D. Morrey, "Velindre healthcare integrated care pathway," In: L. Fischereds (Ed.) *Taming the Unpredictable Real World Adaptive Case Management: Case Studies and Practical Guidance*, Lighthouse Point: Future Strategies Inc., pp. 183–196, 2011.

[15] G. Eysenbach, "What is e-health?," *J. Med. Internet Research*, vol. 3, no. 2, pp. e20, 2001.

[16] J. Powell, "Integrating healthcare with ICT," In: W. Currie, D. Finnegan (Eds.) *Integrating Healthcare with Information and Communications Technology*, 1st ed. Oxford: Radcliffe Publishing Ltd., pp. 85–94, 2009.

[17] G. E. Deng, B. R. Cassileth, L. Cohen, J. Gubili, P. A. Johnstone *et al.,* "Society for integrative oncology executive committee, integrative oncology practice guidelines," *Journal of the Society for Integrative Oncology*, vol. 5, no. 2, pp. 65–84, 2007.

[18] J. Dawson, B. Tulu and T. A. Horan, "Towards patient-centered care: The role of e-health in enabling patient access to health information," In: E. V. Wilson (Ed.) *Patient-Centered E-Health*, London, United Kingdom: IGI Global, 2009.

[19] Department of Health, *Equity and Excellence: Liberating the NHS*. London, United Kingdom: The Stationary Office, 2010.

[20] S. Alsalamah, "Information classification scheme for next generation access control models in mobile patient-centered care systems," in *12th Int. Conf. on Cyber Warfare and Security*, Dayton, USA, pp. 1–9, 2017.

[21] D. Kotz, C. A. Gunter, S. Kumar and J. P. Weiner, "Privacy and security in mobile health: A research agenda," *Computer*, vol. 49, no. 6, pp. 22–30, 2016.

[22] S. Lopriore, A. LeCouteur, S. Ekberg and K. Ekberg, "Delivering healthcare at a distance: Exploring the organization of calls to a health helpline," *International Journal of Medical Informatics*, vol. 104, no. 4, pp. 45–55, 2017.

[23] J. Brunner, E. Chuang, C. Goldzweig, C. L. Cain, C. Sugar *et al.,* "User-centered design to improve clinical decision support in primary care," *International Journal of Medical Informatics*, vol. 104, no. Suppl. 3, pp. 56–64, 2017.

[24] Dr T. Crosby, "Caldicott guardian for the cancer centre, chair of the cancer service management board, clinical director of the velindre cancer centre, and consultant oncologist treating UGI cancer," *Personal Communication*, 2013.

[25] Healthcare Information and Management Systems Society (HIMSS), *The Evolution of Patient Engagement: Rethinking How to Best Engage Patients*. HIMSS Media Lab: Himss17 In Focus, 2017.
[26] J. Goldwater, *The Use of a Blockchain to Foster the Development of Patient-Reported Outcome Measures*. Washington, D.C., United States: National Quality Forum, 2016.
[27] World Health Organization, *Global Strategy on Digital Health 2020–2025*. Geneva, Switzerland: World Health Organization, 2020.
[28] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ and A. Abd-alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *International Journal of Medical Informatics*, vol. 142, pp. 104246, 2020.
[29] S. Alsalamah, H. Alsalamah, A. W. Gray and J. Hilton, "Information security threats in patient-centred healthcare," In: A. Moumtzoglou (Ed.) *M-Health Innovations for Patient-Centered Care*. Hershey: IGI Global, pp. 298–318, 2016.
[30] UK Public General Acts, *Data Protection Act 1998*. London, United Kingdom: The Stationery Office, 1998.
[31] UK Public General Acts, *Access to Health Records Act 1990*. London, United Kingdom: The Stationery Office, 1990.
[32] UK Public General Acts, *Computer Misuse Act 1990*. London, United Kingdom: The Stationery Office, 1990.
[33] UK Public General Acts, *Human Rights Act 1998*. London, United Kingdom: The Stationery Office, 1998.
[34] Office of the Assistant Secretary for Planning and Evaluation, "Health insurance portability and accountability (HIPPA) act of 1996," *Public Law*, pp. 104–191, 1996.
[35] Department of Health, *Department of Health Annual Report and Accounts 2010 to 2011*. London, United Kingdom: The Stationery Office, 2011.
[36] The EU General Data Protection Regulation, "GDPR portal," *GDPR*, 2017. [Online]. Available: http://www.eugdpr.org/.
[37] New York State Department of Financial Services, *New York Cybersecurity Requirements for Financial Services Companies*. Albany, New York, United States: New York State Department of Financial Services, 2017.
[38] The EU General Data Protection Regulation (GDPR), "Article 7 EU GDPR conditions for consent," *EU*, 2016. [Online]. Available: https://www.privacy-regulation.eu/en/7.htm.
[39] The U.S. Department of Health and Human Services (HHS), *Summary of the Health Insurance Portability and Accountability (HIPPA) Act for 1996 for Professionals*. Washington, D.C., United States: HHS, 1996.
[40] Dr D. Morrey, "Former head of clinical information unit at velindre NHS Trust," *Personal Communication*, 2013.
[41] Department of Health, *The NHS Plan: A Summary*. London, United Kingdom: The Stationary Office, 2000.
[42] Department of Health, *Delivering 21st Century IT Support for the NHS: National Strategic Programme*. London, United Kingdom: The Stationary Office, 2002.
[43] Velindre NHS Trust, "Velindre cancer centre-about us," 2017. [Online]. Available: http://www.velindrecc.wales.nhs.uk/about-us.
[44] S. Alsalamah, H. Alsalamah, A. W. Gray and J. Hilton, "Information security threats in patient-centred healthcare," in *Health Care Delivery and Clinical Science: Concepts, Methodologies, Tools, and Applications*. Pennsylvania, United States: IGI Global, pp. 1531–1552, 2018.
[45] S. Alsalamah, "Achieving a secure collaborative environment in patient-centred healthcare with legacy information systems, Cardiff University, United Kingdom, Ph.D. dissertation, 2015.
[46] M. Swan, *Blockchain: Blueprint for a New Economy*, In: T. McGovern (Ed.) Sebastopol: O'Reilly Media, Inc., 2015.

[47] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly Media, Inc., 2015.
[48] L. Linn and M. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States: ONC/NIST, 2016.
[49] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol: O'Reilly Media, Inc., 2014.
[50] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2020. [Online]. Available: klausnordby.com.
[51] A. Baliga, *Understanding Blockchain Consensus Models*. Colombo, Sri Lanka: Persistent Systems Ltd., Tech. Rep, 2017.
[52] Bifury Group, *On blockchain auditability: White paper* . Washington, DC, US: Bitfury Group Ltd., 2016.
[53] G. Volpicelli, "How the blockchain is helping stop the spread of conflict diamonds," *Wired UK*, 2017. [Online]. Available: http://www.wired.co.uk/article/blockchain-conflict-diamonds-everledger.
[54] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Int. Conf. on Open and Big Data*, Vienna, Austria, IEEE, pp. 25–30, 2016.
[55] A. Conceição, F. Silva, V. Rocha, A. Locoro and J. Barguil, "Eletronic health records using blockchain technology," ArXiv abs/1804.10078, 2018.
[56] I. A. Abdelkhalek, R. A. Salha and M. A. El-Hallaq, "Blockchain-based quality of service for healthcare system in the Gaza strip," *Journal of Engineering Research and Technology*, vol. 7, pp. 45–57, 2020.
[57] S. Tanwar, K. Parekh and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, pp. 102407, 2020.
[58] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 218, 2016.
[59] A. Al Omar, M. S. Rahman, A. Basu and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *Int. Conf. on Security, Privacy and Anonymity in Computation, Communication and Storage*, Guangzhou, China, Springer, pp. 534–543, 2017.
[60] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du *et al.,* "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.