HIMSS

Considerations for Policymakers: The Application of Blockchain Technology in Healthcare

December 2019

Table of Contents

Background

Blockchain technology is a subset of distributed ledger technology (DLT), where the data are distributed across computers or nodes within a network, and nodes in the network store a copy of the ledger. The term "blockchain" comes from the characteristics of the technology where each item, or block, on the ledger contains information regarding the previous block within hash, creating a chain and limiting the tampering of the data. Given this new infrastructure, DLT and more specifically, blockchain-enabled solutions, prompt new questions about access, exchange, and ownership of data.

The 2019 HIMSS Blockchain in Healthcare Task Force, a team of HIMSS members with blockchain expertise, completed an assessment of the ethical considerations of blockchain. As a result, HIMSS provides the below recommendations on cross-sector issues related to the application of blockchain-enabled solutions in healthcare as a means to further educate the public and help guide the work of policymakers and regulators. Further rationale to support these considerations is also available.

Policy Considerations

1. ***Benefits & Risks: Empower healthcare organizations and individuals to understand how to maximize the benefits and manage the risks.***

   Blockchain has both benefits and risks for the healthcare enterprise. This kind of technology enables healthcare organizations to drive forward the values of the quadruple aim. However, if not implemented appropriately, the technology has the potential to create privacy, security, compliance, and performance risks as well as post-implementation concerns if processes are not maintained. Weighing these potential outcomes is critical when assessing the appropriateness of blockchain for any use cases identified by an organization. These benefits and risks may also shift and evolve as these solutions mature, adoption increases, and throughputs improve, as well as when new threats, vulnerabilities and compliance requirements emerge.

   Rationale: *Cybercrime and Related Vulnerabilities, Environmental Impacts*

2. ***Test, Pilot & Evaluate: Facilitate an environment that encourages robust testing, piloting and evaluation before implementation.***

Blockchain-enabled solutions may streamline and improve many processes within the clinical and administrative settings, *but they are not panaceas*. Policymakers should encourage the following activities for an enhanced understanding of the potential impact of blockchain in healthcare:

(1) An assessment of use case(s) and associated business value of the solution to both clinicians and end-users, including but not limited to administrative, financial and executive teams;
(2) A review of security, privacy, interoperability, and identity management considerations as part of the solution selection process.
(3) Robust testing and piloting of such a solution within a healthcare consortium in a real-world setting before "go live" implementation occurs, and
(4) Continuous evaluation of blockchain-enabled solutions, threats, vulnerabilities, compliance requirements, and performance indicators.

Where appropriate, government policymakers and regulators should explore setting standards and minimum testing requirements for implemented solutions. It is imperative that healthcare stakeholders be involved in testing to provide understanding around the specific needs and sensitivities of healthcare data, leveraging a use case approach to help identify key criteria to measure success in a pilot phase.

Rationale: *Data Subject Ownership and Control*, *Data Subject Monetization*, *Cybercrime and Related Vulnerabilities*, *Disintermediation and Disruption*

3. ***Awareness & Education: Encourage broader education to create an informed workforce around blockchain-enabled solutions and empower individuals to understand data ownership, access and privacy.***

HIMSS recognizes governments have explored the creation of work groups or task forces to encourage knowledge sharing on blockchain and training for the broader healthcare community. As the technology continues to mature and gain traction in healthcare, research, education and training are necessary to ensure blockchain is applied appropriately, and a skilled and more informed workforce is developed. Key decision-makers will need the knowledge to understand how blockchain could be integrated meaningfully into existing or new solutions before exploring implementation.

There is also a need to educate data subjects (i.e. individuals about whom data is being collected) and end-users on ownership, access and privacy considerations. Data subjects and end-users need to have a basic understanding of the full data lifecycle -- what happens to their personal data from collection, throughout its storage, use, disclosure, and disposal. Furthermore, data subjects and end-users need to be educated on what their shared responsibility is regarding the privacy and security of their personal data.

Rationale: *Data Subject Ownership and Control*, *Data Subject Monetization*, *Cybercrime and Related Vulnerabilities*

4. ***Integration: Consider blockchain-enabled solutions in relation to existing systems and technologies.***

Today, healthcare organizations and government policymakers are exploring solutions to address healthcare's biggest challenges. Blockchain may be part of that solution, as it can facilitate new business relationships and data access opportunities. However, it is not a universal remedy and may not be the appropriate approach for all use cases. Even when it does provide opportunities to address these issues, it will need to complement and integrate with legacy systems and follow standards-based interoperability to ultimately be successful. Policymakers and decision-makers have a fiscal and ethical responsibility to ensure blockchain technology is an appropriate solution for the particular circumstances in question and is integrated appropriately in a manner that provides value and does not contribute unnecessary burden to the end-user or implementing organization(s).

> ***Rationale:*** *Cybercrime and Related Vulnerabilities, Disintermediation and Disruption, Reorienting the Clinician's Role*

5. ***Regulatory Alignment: Align blockchain-enabled solutions with existing, applicable regulations and data protection laws.***

As new policy is considered for the use of this technology, blockchain-enabled solutions must comply with applicable local, national, and international laws and regulations. Various laws and regulations would apply, as some are broadly-construed, and others regulate a specific use case or segment of the industry. These considerations present even greater complexity when looking to scale a solution across several geographical regions, where disparate laws and regulations may apply.

Because new privacy regulations may unintentionally impede the progress of blockchain-enabled solutions, policymakers should work closely with market suppliers to gain mutual understanding of the existing regulatory and legal environment and its effect on piloting efforts and adoption. As appropriate, policymakers have a responsibility to ensure regulation encourages, and does not unintentionally impede, the adoption and proliferation of solutions that may benefit the current ecosystem. The current compliance and regulatory environment is complex and burdensome at all levels for healthcare organizations, clinicians, market suppliers and patients. If this technology can help simplify implementation and enforcement of some of these regulations, the industry should consider how to thoughtfully move it forward. Review further Regulatory and Compliance Considerations here.

> ***Rationale:*** *Data Subject Ownership and Control, Data Subject Monetization, Reorienting the Clinician's Role, Hyper-efficiency and Potential Job Loss, Cybercrime and Related Vulnerabilities, Environmental Impacts*

6. ***Approach to Data: Adopt a "minimal but sufficient" approach to data on the blockchain.***

Blockchain technology was not designed to be a storage mechanism for data and should not be leveraged as such, for security, privacy, compliance and performance reasons. Information added to the chain may be transparent to permitted network participants and difficult to remove

without affecting the entire chain. Therefore, we strongly recommend that regulators and policymakers promote that organizations leveraging blockchain-enabled solutions employ a "minimal but sufficient" strategy for the data that should be included on-chain. This strategy should be guided by the use case's data needs, and implementers should keep in mind not only the privacy and security risks but also the performance of blockchain transactions when deciding the amount of data and/or personally identifiable information (PII) included on the chain. Whenever possible, privacy-enhancing technologies should be used to secure private data on the blockchain.

Rationale: *Disintermediation and Disruption, Reorienting the Clinician's Role, Cybercrime and Related Vulnerabilities*

7. ***Security and Compliance: Build a robust security and compliance strategy for blockchain-enabled solutions.***

Blockchain-enabled solutions are not impenetrable and have vulnerabilities that can be exploited. For example, such solutions may be compromised through phishing, network-based attacks, weak ciphers, or poor key management. Accordingly, it is important to implement appropriate defense in depth measures. Many security and compliance requirements are related to people and processes, irrespective of the underlying technology. Immutability, encryption, and robustness are true strengths of blockchain technology, though such characteristics can also be its weaknesses. Its use should improve and not compromise the compliance with existing security requirements for healthcare organizations and market suppliers. To explore potential security strategies, click here.

Rationale*: Data Subject Ownership and Control, Cybercrime and Related Vulnerabilities*

These policy considerations were framed by discussions with the HIMSS Blockchain in Healthcare Task Force members around the opportunities and challenges blockchain's use may present. Explore the next section to review these topics in further detail.

Rationale for Policy Considerations

The following information provides a rationale for the policy considerations listed above. Each consideration poses a scenario this technology may enable as well as examines potential opportunities and challenges that may arise from its use.

Data Sovereignty

Blockchain-enabled solutions may provide opportunities for the data subject to own or control their data and identity. Identity and access management, which keeps information of what is accessed, at what time, and by whom, may help achieve this ownership and control. This, in turn, helps ensure the integrity of the data and metadata on the blockchain.

Healthcare Organization Ownership and Control

Opportunities: With greater access and knowledge of metadata, such as records on who created or accessed data, and the hashes of data sets, clinicians may be better equipped to review, reconcile, and update data. This metadata provides information on data sources and changes to the data, allowing stronger trust in using this data to inform care.

Challenges: With greater access to and control of the information, technical solutions may increase in complexity and may malfunction more often. Dealing with technology that does not work properly may detract from patient care. Instead of taking care of the patient, the clinician's focus may be pulled toward addressing technical challenges to try to make it work accurately.

Universal Accessibility of Healthcare Data

Opportunities: By offering more opportunities for access via blockchain-enabled solutions, there is greater potential for healthcare organizations and individuals to leverage their data in a way to have more informed interactions within the healthcare system.

Challenges: Technically, healthcare data can be made available for access to a wider array of individuals. However, individuals may face challenges such as access to technology, or barriers like language, age, education, economics, mental and physical disorders, or disabilities. Thus, while the healthcare data may be technically available, it may not be actually available to a wide range of individuals.

Empowering Individuals with Data Control

Opportunities: When individuals (data subjects) are provided with the means to review their data, amend access permissions, make authorizations of uses and disclosures of their data, and revoke consent for sharing of their data with other parties, individuals may be empowered to control where their data move and how the information may be used. Consortia may work on such matters to provide more uniformity around an individual's access to and control over their own data.

Challenges: While the means for individuals to review their data may be technically feasible, individuals may not be sufficiently informed about their rights to review and amend their healthcare data. At times, providers may not know that the patient has such rights. Thus, there may need to be a substantial effort to educate individuals on the right to review and amend their healthcare data as well as the need to educate providers about individuals' rights.

Existing laws and regulations may pose additional challenges around data access and ownership that may cause confusion if substantive education isn't provided to both providers and patients. For example, health providers may be obligated to report certain data to public health authorities, law enforcement, and others. Also, state statutes may require healthcare organizations and providers to be custodians (or co-custodians) of the health records for an extended period of time, which would need to be communicated. Furthermore, if a data subject is deceased, there must be an understanding of how this legally dictates future use of that data within constraints mandated by the U.S. Health Insurance Portability and Accountability Act (HIPAA) E.U. General Data Protection Regulation (GDPR) and other applicable laws and regulations.

Data Subject Monetization and Direct Benefits of their Data

Opportunities: While not all blockchain solutions leverage cryptocurrency or tokens, certain use cases involve patients monetizing data to incentivize participation in clinical trials that fit their specific needs. Besides offering cryptocurrencies or crypto-token rewards, participation rewards may include direct notification of important findings with their data. Incentives may encourage greater participation, thus increasing the data available to inform clinical research and ultimately care delivery and population health.

Informed consent protocols may be made more transparent and efficient with the use of blockchain-enabled processes. Blockchain technology audit trail capabilities can be leveraged to ensure patients' informed consent is collected, trackable, and securely stored. Additionally, the processes should allow for withdrawal of informed consent, should the patient choose to do so. [Source]

Challenges: Not at all individuals may be able to monetize their healthcare data in matching with clinical trials. Barriers such as language, age, education, physical and mental disorders and disabilities, and other factors may deter some individuals from seeking such clinical trial opportunities.

Additionally, even for individuals who would be able to monetize their healthcare data in matching clinical trials, such individuals may not fully understand the consequences of participating in the clinical trial and sharing their healthcare data. The potential privacy concerns and impact may either not be known or communicated across to the individual.

There are also challenges with identifying the monetary value of data, so variables in value may arise between organizations and within the industry. It is a question as to whether the government and/or broader market guides how this data is valued.

Disintermediation and Disruption

Opportunities: Blockchain shifts away from a centralized "hub and spoke" architecture, with single points of failure and greater vulnerability failures and attacks, to a decentralized, federated network. It enables autonomous, automated processing of transactions, eliminating traditional intermediaries in these transactions. Decentralizing the transaction process has the potential to reduce costs, delays, and single points of failure. Automating transactional processes has the potential to decrease unnecessary administrative work on behalf of the clinicians, increasing time for more meaningful interactions across the care continuum. The distributed network also eliminates a single point of failure, improving resilience of the information on the blockchain.

Challenges: Blockchain technology is meant to operate on the back end and should avoid, where possible, adding additional steps for the end user. If this technology is poorly implemented without a strong federated approach, workflow may be negatively impacted, potentially affecting the quality of care.

A strong identity management strategy and sufficient federation abilities are needed for successful disintermediation, both of which are currently lacking within our current healthcare ecosystem.

Hyper-efficiency and Potential Job Loss

Opportunities: Blockchain has the potential to eliminate redundant maintenance and inconsistencies of data across centralized silos. Greater efficiency has enormous potential to reduce many of the administrative costs in healthcare. Breaking down silos can improve health information management across both the administrative and clinical data domains, eliminating friction, delays and costs from previously redundant and siloed data records. The introduction of a new technology also creates education opportunities for a new skilled workforce to fill the employment gap.

Challenges: As seen in other industries, increased efficiency may make certain jobs unnecessary. Organizations may reduce staff expenditures as a result of increased efficiency resulting from blockchain-enabled processes. As with any technical advancement, these new efficiencies may lead to displacement of parts of the workforce. New technologies, such as blockchain, could also lead to major business process reengineering. This progression requires change management and advanced planning to minimize any negative impact on the organization and its employees.

Environmental Impacts of Data Mining

Some public blockchains require the mining of cryptocurrency or data as part of the process used to validate data added to the blockchain.

Opportunities: The majority of healthcare blockchain solutions thus far use private consortium blockchains, not public blockchains, so considerations around mining may not be needed. In most cases to date, private blockchain networks leverage consensus algorithms that do not require mining and therefore impose much less energy or hardware demand. In a case where healthcare organizations use public blockchains, the requirements of mining may offset the benefits of full decentralization and automation of transactions on the blockchain. Also, as the technology

advances, new solutions are being tested to minimize the requirements of energy and resources necessary. These advancements may also improve scalability.

Challenges: Some mining may require a great deal of electricity and hardware. This resource drain can be a deterrent for public blockchain solutions and use. However, this may change with advances in blockchain algorithms, cloud computing, and other disruptive technology. Stakeholders need to be educated on the advancements in mining so potential environmental misconceptions don't become a deterrent in exploring blockchain as a solution.

Cybercrime and Related Vulnerabilities

Opportunities: Blockchain technology's characteristics may provide additional security components that can be incorporated into an organization's security strategy. The ability to use blockchain-enabled solutions with existing systems and technology as well as using specific identifiers on the blockchain that reference PII and PHI stored wherever possible in secure enterprise systems, helps reduce risk and ease compliance requirements. Blockchain also has the potential to mitigate fraud.

Challenges: As with any other technology, blockchain-enabled solutions are not free from vulnerabilities. To the extent that there are weaknesses in design or implementation of this kind of technology, market suppliers, purchasers, and users need to address such issues. Communication among the market suppliers, purchasers, and users is key; those who procure and/or use blockchain-enabled solutions must be cognizant of any updates or new information. Ideally, this information will enable purchasers and users to understand the significance of the information/updates conveyed and what steps, if any, may be taken in light of the new information or update.

Reorienting the Clinician's Role back to Care

Since the shift to health IT accelerated in the early 2000s, there has been a growing issue of overburdening clinicians with data entry and navigational issues around accessing data of optimal quality and integrity, which impedes a clinician's ability to deliver care.

Opportunities: When a blockchain-enabled solution is implemented correctly, it should provide seamless integration to enable easier access to and secure storage of information and the transactions involved. The blockchain-enabled solution should not interfere with the end user's workflow or access to other technology solutions. Given its current nascence in healthcare, there is an opportunity to get ahead of the challenge of seamless integration in a way that does not negatively impact care.

Challenges: Adding a blockchain-enabled solution without considering its applicability to a use case, potential value, or relationship with a partnering stakeholder, could add a layer of complexity to an already convoluted health IT ecosystem. Furthermore, if this complexity detracts from the end goal of sound care, ethical and other questions may arise from the implementation of this kind of solution that is not well suited for the coordination and delivery of care.