IDC TECHNOLOGY SPOTLIGHT

Brought to you by Tech Mahindra, Powered by IDC

This paper examines how Tech Mahindra is using blockchain and distributed ledger technology to improve the consent management process, which will enhance the patient experience and physician satisfaction with improved — and compliant — access to patients' protected health information.

Improve Patient Experience Using a Seamless Consent Management Process Engineered with Blockchain Technology

August 2018

Written by: Lynne A. Dunbrack, Research Vice President, IDC Health Insights

The Process of Managing Patient Consent Is Cumbersome

Patients have grown accustomed to signing Health Insurance Portability and Accountability Act (HIPAA) forms before they seek treatment. However, they often find the process confusing and frustrating, especially when it is repeated each time they see another healthcare provider in the same health system. Care can often be delayed while office staff search for the necessary paperwork to confirm that patients have provided consent or authorization to access their protected health information (PHI).

HIPAA prohibits covered entities (e.g., payers and providers as well as their business associates) from disclosing PHI unless authorized by the patient or if the disclosure is related to treatment, payment, or healthcare operations activities. Covered entities may provide only the minimum necessary information for payment and healthcare operations. U.S. Department of Health and Human Services (HHS) recommends that covered entities establish role-based policies and procedures that limit disclosures, including data that an organization's workforce has access to on a need-to-know basis to do a job.

AT A GLANCE

KEY STAT

42.2% of providers are researching, piloting, or deploying blockchain technology.

KEY TAKEAWAYS

» Blockchain ledgers of secure, immutable, and sequential data and records can be shared as a "single version of the truth" for managing consent.

» Consent management is a good first blockchain project to get a "quick win on the scoreboard" because it's a self-contained project.

Covered entities may opt to obtain the individual's consent to use and disclose PHI for treatment, payment, and healthcare operations. While patients can request restrictions on how covered entities may use or disclose this information, covered entities are bound to meet those restrictions only when they agree to do so. For example, PHI access may be limited to a certain period or shared only with specific healthcare providers. It should be noted that consent should not be confused with authorization. Even if the covered entity has obtained patient consent for treatment, payment, and healthcare operations, authorization must be obtained for disclosure for other purposes such as for the use and disclosure of psychotherapy notes, marketing, and any disclosure involving the sale of PHI.

To streamline the consent management process, healthcare organizations (HCOs) are deploying electronic consent management systems. However, they face a variety of challenges that inhibit the creation of a seamless consent process and improved patient experience, such as:

- **Interoperability.** The healthcare industry still struggles with health information exchange across the enterprise and to external third parties. Scanned consent forms stored in the patient's electronic health record (EHR) lack machine-readable, structured data, thus making electronic consent management more difficult. Where (which module) and how (which technical standard) consent is managed will vary by EHR vendor, increasing the level of complexity in transferring consent between healthcare organizations.

- **Compliance complexities.** The HIPAA Privacy Rule sets forth privacy protections; it does not create a national standard. Thus, if state or local laws provide greater privacy protections, they preempt the federal requirements. State preemption becomes particularly complicated for healthcare organizations whose catchment area spans multiple states that may have different consent models (e.g., opt-in, opt-out, full, or with restrictions) and when additional authorization is required to share sensitive information, such as HIV status or substance abuse.

- **Visibility.** Most clinicians and patients lack visibility into what data the consent covers as well as who can see the patient's data and for how long. For example, the patient's primary care physician can see the patient's full EHR, while the orthopedic surgeon can see only the most recent records related to the orthopedic injury being treated and not the decade-old records related to a mental health crisis the patient experienced. Even with electronic consent management systems, it is difficult to track consent expiration.

Blockchain technology, including distributed ledger technology (DLT), and smart contracts will play a key role in managing the electronic consent process by enabling trusted relationships between healthcare professionals, patients, and their family caregivers. Patients define what PHI they want to share, with whom, and for how long; that information is then recorded using DLT and smart contracts. Healthcare providers participating in the patients' care can securely access this information to confirm that consent (or authorization) was provided by patients and that they are accessing and disclosing PHI according to any restrictions agreed upon between the healthcare organization and patients. Patients need to record their consent (or authorization depending upon the scenario) only once. Access to this information is distributed to healthcare providers participating in the consent management blockchain, a great improvement upon the current cumbersome consent management process.

Distributed Ledgers in Healthcare

IDC defines blockchain as a digital, distributed ledger of transactions or records. The ledger, which stores the information or data, exists across multiple participants in a peer-to-peer network. There is no single central repository that stores the ledger. DLT allows new transactions to be added to an existing chain using a secure, digital, or cryptographic signature. The underlying processes supporting blockchain ledgers are the blockchain protocols that aggregate, validate, and relay transactions within the blockchain network. New blocks of transactions can be added to existing blockchains and dispersed to other parts of the blockchain network. Blockchain technology allows the data to exist on a network of instances or "nodes" rather than being managed in one centralized instance, as seen in many traditional systems. Nodes within the network contain a complete copy of the entire ledger, making it available to those who can access the network. Blockchain is designed to be an incorruptible, decentralized network with enhanced security properties, allowing data and transactions to be transparent to members of the distributed ledger.

Increasingly, enterprises across various industries are investing in blockchain ledgers that can be distributed to (or shared with) multiple parties to help provide "one version of the truth" that can be shared with internal lines of business and with customers, suppliers, counterparties, and intermediaries. DLT is gaining momentum as HCOs look to aggregate data that can be shared among multiple users. According to IDC's 2018 *Industry IT and Communications Survey,* 42.2% of providers are researching, piloting, or deploying blockchain technology. Distributed blockchain ledger use cases in healthcare include consent management, product track and trace, interoperability, identity management for people and things, and insurance claims processing.

Private Ledgers

Our research suggests that most enterprise users seek to deploy private or permissioned ledgers, where consent must be given in advance to read and write to the ledger. This is particularly useful in healthcare because HCOs must comply with stringent state and federal privacy and security regulations or face stiff penalties for noncompliance and data breaches.

Private ledgers can have one owner or many owners. However, only those with permission have access to information about transactions and the identities of the individuals and businesses accessing the private ledger. The ledger's integrity and security are provided for through limited access, and monitoring of the ledger can be done by trusted partners such as payers, providers, and intermediaries. Private ledgers can also include digital signatures, which can be viewed by the counterparties that belong to the private ledger. Private ledgers are the preferred model for HCOs and regulators because access can be granted to the identities and transaction histories, which helps with HIPAA compliance by ensuring appropriate access to patient records by authorized personnel and producing an audit trail showing who accessed the blockchain of records or transactions and when.

Public Ledgers

Public or unpermissioned ledgers do not have a single owner, and anyone can access and contribute data. IDC Health Insights believes healthcare organizations will remain reluctant to use public blockchain ledgers because of their open nature, which could violate HIPAA's privacy and security provisions and lead to latency from processing a huge number of transactions for all participants. We believe it is more likely that governments and agencies may use public blockchains to post public records (e.g., birth certificate information and property ownership records) versus personally identifiable health information, claims transactions, account balances, and contracts.

Smart Contracts

Smart contracts are designed to execute automatically when conditions set by both the healthcare provider and the payer are met. For example, if the conditions to properly adjudicate a claim are met (e.g., eligibility, authorization, and plan benefit design), then smart contracts adjudicate the claim and process real-time (or near-real-time) payments. Similarly, if the patient's consent has been recorded on the blockchain, access to the PHI is provided according to the provisions defined in the smart contract. Advantages include greater transparency and lower transaction costs because once set, contracts execute automatically, and transaction data is recorded in the ledger, enabling faster transaction processing. However, HCOs are looking closely at the risks associated with relying on program logic, the legal and computing issues related to blockchain technology, and the required resources necessary to execute and record smart contracts as directed.

The Benefits of Using Blockchain Technology to Manage Patient Consent

Secure, aggregated immutable records describing consent enable HCOs to build direct connections between healthcare providers, patients, lines of business, suppliers, and the supply chain. Direct connections between these players help simplify business processes, such as consent management, and improve data security and data reconciliation. Benefits of using blockchain technology to manage patient consent include the following:

- **Consent is under the complete control of the consumer.** Consumers (or delegated family members for minors or those with cognitive issues) define who can see what data and for how long. This information is then stored in a smart contract.
- **Third parties have greater visibility into what kind of consent was provided.** DLT and smart contracts provide a single source of the truth regarding what restrictions have been requested by the consumer and agreed to by the HCO.
- **Ready access to health information is available.** Blockchain technology–enabled consent management reduces the time it takes to confirm that consent was (or will be) provided by the patient. Without consent, care can be delayed, resulting in potentially poor patient outcomes. There are also financial and staffing implications when appointments must be rescheduled. In the United States, an open time slot costs a practice an average of $200.
- **Regulatory compliance is increased.** Many HCOs use a combination of manual and semi-automated processes to manage patient consent. A more efficient process will facilitate complying with local privacy and security regulations, including HIPAA and the General Data Protection Regulation (GDPR).
- **Monetization opportunities may exist.** Patients may decide to allow third parties not directly related to their care (such as research organizations) to access their data, provided they are compensated for this data access. Blockchain's distributed nature creates a new marketplace where patients can "sell" or monetize their PHI because they — not the HCO — own the keys to it.
- **The patient experience is improved.** Nothing frustrates patients more than providing the same information over and over again. Delays in receiving care while consent is confirmed only make matters worse for patients and their family caregivers. A more efficient process with faster access to consent information reduces friction and improves the patient experience. Reducing friction in the consent management process will also improve staff and clinician satisfaction.

Considering Tech Mahindra's Blockchain Practice for Healthcare

Tech Mahindra provides IT services and consulting along with business process outsourcing to organizations in a wide range of industries, including healthcare providers, payers, and life science organizations. The company has more than 115,000 professionals across 90 countries serving more than 900 global customers, including Fortune 500 companies.

The company began its foray into blockchain in 2016 following conversations with 90 CXOs and other senior leaders from a variety of industries about the role blockchain could play in solving industry-specific challenges. A key finding was that enterprises — regardless of industry — needed platform capabilities and staff with blockchain expertise. Tech Mahindra developed a core team of technical resources trained on major blockchain protocols such as Corda, Hyperledger, and Ethereum as well as emerging protocols such as Postchain, which offers a consortium database.

Close partnerships forged with more than 15 protocol and niche blockchain application development companies keep Tech Mahindra staff abreast of the rapidly evolving blockchain landscape. The company has also invested several million dollars in BlockRx, a series of initiatives developed by startup iSolve to address counterfeiting in the pharmaceutical supply chain. Investments and grants in BlockRx and other companies provide Tech Mahindra customers with access to new blockchain capabilities and the assurance that these solutions will scale from both a technical resources perspective and a professional resources perspective.

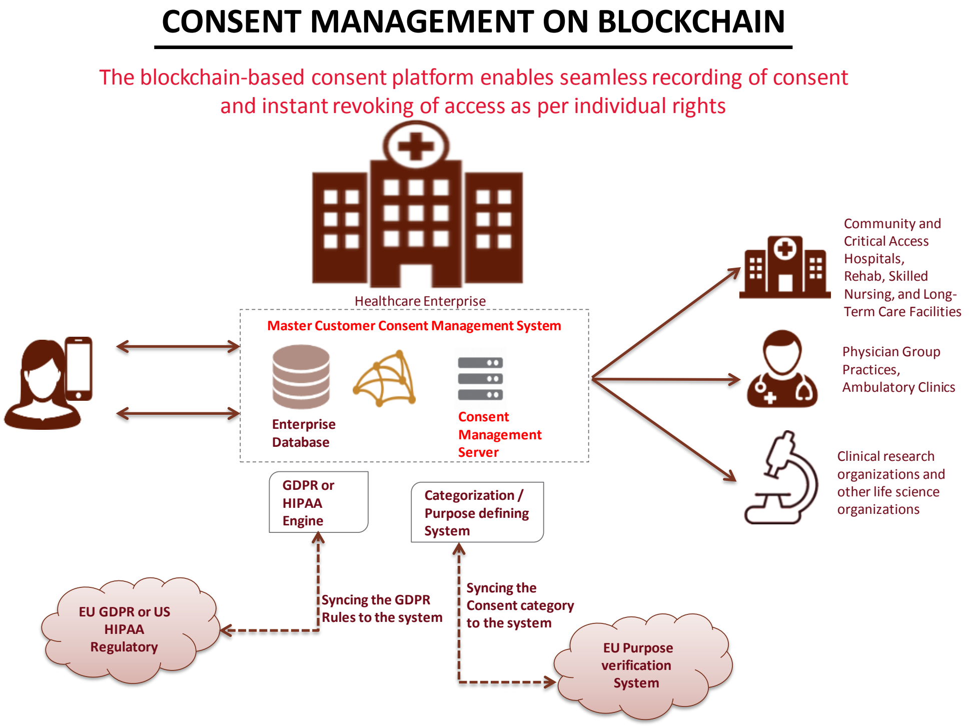
Tech Mahindra is also creating a core team of blockchain technical resources with the right skills to build off of its expertise in back-end server integration. The company launched its BlockGeeks program, in which staff will undergo intensive training to gain blockchain technology proficiency. The first class of 20 will be trained by fiscal year 2019.

Additionally, Tech Mahindra's Blockchain Design Studio combines deep domain experience in healthcare (and other industries) with a blockchain platform and services offering in the Tech Mahindra cloud. (IBM and Microsoft Azure cloud services are also options.) The company has built out the following healthcare and life science blockchain use cases in Blockchain Design Studio: patient health records, patient and hospital "know your customer" (KYC), provider benefit management, and consent management.

Tech Mahindra's Blockchain Consent Management Solution

Tech Mahindra is building out the blockchain-based consent management solution as part of the blockchain work it is doing in patient health records. Patients first enroll in the network. A unique blockchain wallet (or locker) is created to store patients' PHI and consent on the blockchain in compliance with local privacy and security laws. Data on the blockchain is encrypted for additional security. Patients are in full control of their data. They define who can see what data, when, and for how long. Using a mobile or web browser–based app, patients can remotely change their consent or authorization definitions. Participating healthcare providers will have access only to the PHI they are allowed to see based on patient consent and local privacy and security laws (see Figure 1).

FIGURE 1: ***Tech Mahindra Blockchain Consent Management***


CONSENT MANAGEMENT ON BLOCKCHAIN
The blockchain-based consent platform enables seamless recording of consent and instant revoking of access as per individual rights
Healthcare Enterprise
Master Customer Consent Management System
Enterprise Database
Consent Management Server
GDPR or HIPAA Engine
Categorization / Purpose defining System
Syncing the GDPR Rules to the system
Syncing the Consent category to the system
EU GDPR or US HIPAA Regulatory
EU Purpose verification System
Community and Critical Access Hospitals, Rehab, Skilled Nursing, and Long-Term Care Facilities
Physician Group Practices, Ambulatory Clinics
Clinical research organizations and other life science organizations

Source: Tech Mahindra, 2018

Consent management is a good first project for those considering blockchain technology because it is self-contained and demonstrates blockchain use between HCOs. As a proof-of-concept (POC) project, it provides a "quick win on the scoreboard" to demonstrate the value and best practices associated with deploying blockchain technology.

Challenges

The market challenges facing Tech Mahindra and its customers also present opportunities:

» **Blockchain technology is relatively new and hasn't been widely embraced by HCOs.** Most organizations are still absorbing massive investments in EHRs and balancing the shift from fee-for-service reimbursement with its steady revenue stream to value-based care, which requires additional investment in analytics, population health management, and patient engagement solutions. HCOs will need guidance from blockchain technology and service providers in identifying and prioritizing use cases.

» **There is a dearth of blockchain talent.** Firms are challenged to recruit and retain staff with blockchain expertise to establish teams with the appropriate business and technical skills to build distributed ledgers and smart contracts.

- **Compliance complexity exists.** Laws, agency rules, and regulatory frameworks are either evolving or under development worldwide. The GDPR, which went into effect May 25, 2018, represents a significant expansion of personal privacy rights for European Union residents. HIPAA privacy laws became more stringent when the HIPAA Omnibus Rule went into effect in 2013; the HHS Office for Civil Rights has since stepped up enforcement of HIPAA compliance by covered entities and their business associates.
- **Critical mass is essential for success.** Like health information exchange initiatives, collaboration across the healthcare ecosystem to build critical mass is essential to the success of blockchain projects — even for pilots. Partnerships with information technology and services providers, other HCOs, and consortia will play an important role in the development and deployment of blockchain-based applications, especially those based on data sharing.

Conclusion

HCOs are beginning to experiment with blockchain technology, as evidenced by their participation in blockchain consortia dedicated to the health and life science industries; they are also partnering with information technology and services providers on pilot and POC projects. With any new initiative, especially an initiative that relies on new and evolving technology, picking the right POC project is important for future project success.

Deploying blockchain can help improve patient experience and engagement, thus leading to improved outcomes.

Consent management is a good initial POC because it is a shared challenge across the health ecosystem and a process that HCOs typically do not compete on. A self-contained project, consent management can provide a quick win. Making the consent management process more efficient not only improves the patient experience but also encourages greater engagement between patients and their providers because it is easier to share electronic health information. Facilitating access to patients' health information will also improve physician satisfaction because it reduces the friction involved with the process of patient referrals.

Collaboration will be key given the pace of innovation and shortage of talent. HCOs should collaborate with partners, including other healthcare organizations, looking to solve the same problem. To augment their own IT staff, HCOs should also look for information technology and services providers with deep health domain and blockchain expertise and the means for further developing blockchain teams.

IDC believes the market for blockchain technology and services will continue to grow, and to the extent that Tech Mahindra can address the challenges described in this paper, the company has a significant opportunity for success.

About the analyst:

Lynne Dunbrack, *Research Vice President*

Lynne Dunbrack is Research Vice President for IDC Health Insights responsible for the research operations for IDC Health Insights. She manages a group of analysts who provide research-based advisory and consulting services for payers, providers, accountable care organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads the IDC Health Insights Connected Health IT Strategies program.

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.