HealthManagement
Promoting Management and Leadership

Blockchain Protecting Telemedicine

Telemedicine offers an opportunity for medical institutions to optimise delivery of care, especially for patients living in areas where healthcare facilities and resources are inadequate. However, there is a downside to this technology-driven approach: risks of patient data being leaked due to insecure telehealth systems.

These privacy risks are brought about by poor, or the absence of, security controls over the collection, use and transfer of data, according to Blaise Wabo, associate director at A-LIGN, who cites the potential of blockchain in protecting telehealth infrastructure against hacking threats.

The blockchain expert explains how, within a telemedicine programme, sensitive health data and other information of patients may land in the hands of unauthorised persons and/or third-party users.

You may also like: Healthcare Blockchain Company Fined for Non-Compliance

“For example, home telehealth devices and sensors may collect and transmit information on activities in the household that a patient wishes to keep private, such as substance abuse or their daily routine, including when their home is unoccupied during particular times of the day,” says Wabo.

And while smartphone apps are useful for managing one's health and fitness, these online tools also may share personal data, including the place/location of patient, allowing advertisers and third parties to store that data in third-party libraries or online servers, Wabo explains.

Blockchain to the Rescue

This distributed ledger technology, Wabo notes, can help facilitate a more efficient way to securely store and transfer data within a telehealth system, as well as sharing of data across healthcare organisations.

In addition, blockchain "allows medical records to be stored in secure, fragmented systems that can contain large amounts of data and information, enabling providers to store a more complete patient history and securely encrypt medical data,” Wabo said, adding that providers can create "a private network for their blockchain and only invite patients directly.” This means any data entered into a computer must be approved by the patient and doctor, as well as verified against a previous ledger.

Both the patient and doctor also can secure a personal copy of the ledger, rather than a single party having control over the data, according to Wabo. “When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed," he explained. This procedure ensures multiple checks are in place for protecting sensitive data and information, reducing some of telemedicine’s main security concerns.

Blockchain adoption in telemedicine, however, faces these key barriers: cost, lack of industry expertise, and the lack of standardisation.

Since blockchain technology relies on intensive computing power, it uses a lot of electricity to operate. The lack of expertise for providers, patients and even some IT professionals, is also a hurdle, which may be difficult to overcome when combined with the problem that blockchain is costly to operate, Wabo said.

Meanwhile, the lack of standardisation, or interoperability, limits the ability for platforms to connect to each other, he continued.

Lucie Robson

Source: Healthcare IT News

Image credit: iStock

Published on : Tue, 29 Oct 2019