

Upscaling critical medical technologies with IoMT secures data integrity and interoperability

24 January 2024 | Analysis

By Genie Yuan, Regional Vice President APAC Japan, Couchbase



Healthcare in Singapore is at a crossroads. A rapidly ageing population - the government [estimates](#) that one in four of the population will be over 65 years old by 2030 - has carers on the ropes.

On top of that, the Ministry of Health ([MOH](#)) found that diseases are on the rise between 2017 and 2022. In particular, the percentage of adults suffering from hyperlipidaemia has grown from 35.5% to 39.1%, and the same can be said for hypertension, from 24.2% to 37%. These findings underscore the need for always-available healthcare to ensure that citizens continue to enjoy a high quality of life.

For this reason, Singapore's healthcare sector is going digital. Elderly monitoring systems, for example, are being looked at to respond faster to emergencies and provide more accurate diagnoses anytime and anywhere. These technologies work best by leveraging patients' data generated from Internet of Things (IoT) devices. Capturing this data is crucial, and it is one of the reasons why healthcare providers need to integrate the right database into their tech stacks.

Databases are the heart of healthcare

Choosing a database with cloud capabilities that is compatible with a distributed edge infrastructure can help healthcare professionals gain insight into patients' conditions and how to cure them. For instance, data collected from surgical devices can automatically be summarised into reports, allowing surgeons to review certain procedures and determine the best post-op care. Upon being discharged from the hospital, patients can also read through recovery instructions at a convenient time, such as pain expectations and medication prescriptions.

During periods of network interruptions, such a database allows critical medical technologies, like endoscopic camera systems, to continue functioning normally. Then, once connections are restored, new data can be captured and synced with other devices across the entire organisation. This feature ensures that healthcare professionals can continue to treat their patients while minimising complications brought on by data discrepancies.

Inherent security concerns around patient data

With data being the lifeblood of healthcare operations, it is imperative that organisations protect them from cybersecurity threats and maintain compliance with local and global privacy regulations. In November, Internet users were unable to access the websites of several public health institutions due to a distributed denial of service (DDoS) attack. Imagine how much worse the damage would have been if data theft was added to the mix. Not only would this jeopardise healthcare organisations' reputations, but it could also expose their patients to more attacks.

Preventing these incidents starts by installing role-based access controls. This will allow healthcare organisations to limit employees' access to only the files and assets necessary for their duties. These controls can be reinforced with Transport Layer Security ([TLS](#)) encryption that prevents attackers from eavesdropping or tampering with data, whether at rest or in transit.

Healthcare organisations that operate with a distributed architecture also need to take the following features into account when choosing their database:

- **Native support with various operating systems:** Databases must be able to operate in a variety of OS environments, including Linux and Windows Server, to ensure smooth-running processes.
- **Flexible data models:** Healthcare organisations need to transport medical information to various devices so that professionals are better prepared to operate on their patients. Integrating a non-relational database is necessary to achieve this, as they can adapt their architectures to accommodate different [data types](#), including NoSQL and JSON documents.
- **Reliable operations:** Maintaining accurate, high-quality data is crucial for healthcare organisations looking to create new medical innovations that can add years to patients' lives.
- **Data replication:** A database that is capable of pairing standalone devices with other hospital systems and tools can sync medical information across various components. Not only will this ensure data consistency, but it can also prevent the loss of crucial information if a data centre suddenly breaks down.

Consistent and reliable information is key to saving lives, especially those of elderly citizens living alone. Activating these capabilities requires healthcare organisations to break down silos, minimise operational errors, and mitigate security risks. With a modern database powering their devices, healthcare professionals leveraging the same medical information can work together to keep their patients alive and well without inviting in threats.