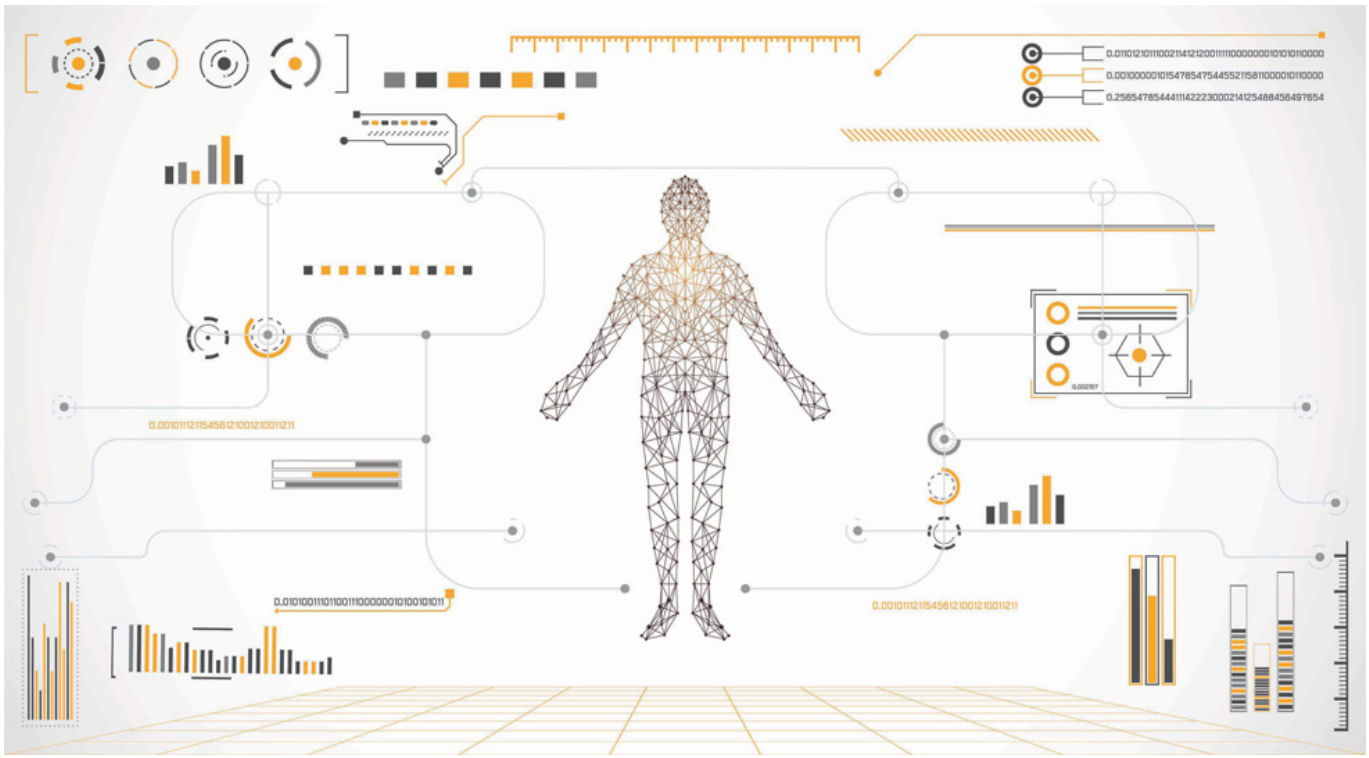
# The Saudi Health Information Exchange: Data and technology enabling improved healthcare management in Saudi Arabia

**Nick O'Connell** - Partner, Head of TMT - Saudi Arabia - Technology, Media & Telecommunications / Intellectual Property

n.oconnell@tamimi.com - Riyadh

Amy Land-Pejoska - Associate - Technology, Media & Telecommunications - Riyadh



In 2000 a World Health Organisation paper on measuring overall health system performance ranked Saudi Arabia highly (26th out of 191) in terms of overall efficiency across all WHO member states. In 2017, consistent with the Vision 2030 plan, King Salman announced that government hospitals and health centres will be converted into public sector companies and decentralised so as to compete on the basis of quality, efficiency, productivity and waste reduction. Vision 2030 specifically identifies improved efficiency and effectiveness of the healthcare sector through the use of information technology and digital transformation as a key focus.

Saudi Arabia's Ministry of Health has published a suite of policies relating to the Saudi Health Information Exchange ("SHIE") initiative (may also be referred to as Saudi eHealth Exchange ("SeHE")), which is broadly aimed at the use of health information, including patient data, in the context of the increased adoption of technology and digitalisation in the health system. While the exact legal status of the policies and the programme is not entirely clear, the policies provide a good indication of what the Ministry of Health expects in terms of the use of data in a healthcare context.

Under the SHIE framework, the implementation of ongoing technological improvements to the healthcare system is contemplated on two main fronts. The first is the adoption of secure technology solutions to enable streamlined patient care via online health records. The second is making available de-identified

patient data that can inform research. This can be used by both the public sector, for example, by guiding public health policy responses (e.g. containment and prevention of epidemics, or targeting health awareness programmes), and by the private sector, for example, by developing new treatments and pharmaceuticals. Researchers in both the public and private sector can also benefit.

## Use of the SHIE system

Broadly speaking, the SHIE policies contemplate the use of the SHIE system, for certain required purposes as well as certain permitted purposes, by participating healthcare subscribers (being healthcare providers that have executed a participation agreement with SHIE), their business associates and sub contractors, and SHIE infrastructure providers.

Uses of the SHIE system that are specifically permitted include:

- patient treatment (including informing patients of their own interests) and the support of that treatment by the healthcare provider;
- operational purposes, involving health service management and quality assurance; and
- public health purposes, such as public health surveillance for disease control, public safety emergencies, and for providing information to policymakers).

It may be permitted to use the SHIE system for research, education, market studies and payment administration, but it is not permitted to use the system for legal or forensic investigations, or for purposes that are not disclosed.

## Information security

The SHIE policies include provisions relating to information security.

Participating healthcare providers are required to have comprehensive policies in place to ensure that health information is protected from misuse. These include policies relating to access control, audit logs, and encryption. Certain minimum requirements are set out in the SHIE policies, and others may be added pursuant to the data use agreement to be entered between participants and the SHIE.

Minimum information security requirements specified in the SHIE policies include:

- infrastructure needs to be managed in accordance with ISO 27000 or SAS70/SSAE 16, relating to access and core secure management practices;
- contingency and disaster recovery plans need to be implemented to ensure availability and integrity of data held in the SHIE system;
- the exchange of information from or via the SHIE system needs to be encrypted, and the encryption must support either AED or 3DES data encryption standards;
- intrusion detection measures need to be implemented; and
- personnel handling health information involved in the support of SHIE systems need to receive proper training in privacy and confidentiality, and a sanctions policy for inappropriate use, transmission, copy or disclosure of data needs to be implemented.

There is an expectation that SHIE systems be managed to conform with the ISO/TC 215 standard: ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002, as well as an expectation that participants appoint a privacy/information security officer.

The SHIE policies go into significant detail on aspects relating to identity management and authentication. They also include specific details with regard to security audits, reportable events and breach investigations, as well as data breach notification obligations. These include categorisation of events warranting review, as well as details on circumstances in which reportable events constitute privacy breaches.

## Patient rights

Healthcare providers are required to provide patients with a clear notice relating to the impact of the use of the SHIE system on their patient health information. Such notices need to include specific details, including information regarding the purpose and benefit of the SHIE system, benefits, how data is protected in the SHIE system, how data may be used, and contact information through which to seek further information. The notice also needs to provide patients with details on how to opt out of the SHIE system.

Relevant personal health information contained within the SHIE system should be available to patients in a convenient and affordable manner, and without the need to use physicians or healthcare institutions as an intermediary. Patients should be able to add to, or amend, their information in a convenient and affordable manner. There should be appropriate mechanisms for vetting the identity of the patient when accessing his or her records, as well as for vetting and recording the identity of any person making annotations or amendments to the records. Patients need to be advised as to how their personal health information could be used, by whom it could be accessed, and in what circumstances it might be disclosed.

It is not permitted to disclose patient health information held in the SHIE system other than for the treatment, patient use, operational and public health purposes specified in the policies. The patient care rights section of the SHIE policies provides for a mechanism for patient complaints, including in respect of data breach incidents (in respect of which there is an obligation to notify affected persons), as well as a mechanism by which patients may seek a report of any disclosure of information about them via the SHIE system.

# ‘Healthcare technology providers seeking to introduce their solutions to the Saudi market need to familiarise themselves with the legal and regulatory framework relating to the use of patient data.”

## Conclusion

There is clearly interest in the use of technology and data to deliver better health outcomes for patients in the Kingdom. We expect to see continued investment in this sector. It is important that healthcare technology providers seeking to introduce their solutions to the Saudi market familiarise themselves with the legal and regulatory framework relating to the use of data, including patient data, in the Saudi healthcare context.

Al Tamimi & Company’s Technology, Media and Telecommunications team regularly advises on technology and data issues in the healthcare sector. For further information, please contact Nick O’Connell, Partner (n.oconnell@tamimi.com) or Amy Land Pejoska, Associate (a.pejoska@tamimi.com).