How Does Bahrain's New Personal Data Protection Law Impact Patient Privacy?

Andrew Fawcett - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi

How patient data is processed in the Kingdom of Bahrain has been altered by Law No. 30 of 2018 promulgating the Personal Data Protection Law ('PDPL'), which came into effect on 1, August 2019.

While the PDPL affects almost all businesses in the Kingdom, the health sector will be particularly impacted as, by its very nature, healthcare involves the collection of significant amounts of personal data to deliver services to patients.

Our Law Update article entitled "Catching the wave: New Data Protection Law in Bahrain" regarding the PDPL's general applicability can be found in the 2018 June/July Law Update edition. In this article, we focus on the healthcare sector.

We understand that Bahrain's National Health Regulatory Authority ('NHRA') expects that the general framework on data processing provided for in the PDPL be followed in relation to patient data.

Patient Data is Sensitive Personal Data

Under PDPL any data related to a person's health is categorised as 'sensitive personal data' and is subject to specific processing conditions.

The PDPL expressly allows sensitive personal data to be processed without the consent of the data subject where the processing is necessary for:

> *"preventive medicine, medical diagnosis, provision of healthcare or treatment, or for the management of healthcare services which is carried out by a licensed member of a medical profession, or by any other person who is bound by a duty of confidentiality as imposed by law".*

However, this exception is not a complete exemption from the PDPL's requirements. Here are some examples of PDPL's requirements with which health organisations in Bahrain now need to comply.

Rights of Patients as Data Subjects

The PDPL includes provisions that require a data controller to, amongst other things, notify data subjects of certain information, including the purpose and location of any data that is collected. Further, the data subject now has a statutory right to access their personal information and to object to processing of their data in certain circumstances.

With patient health data collected at points ranging from doctors' offices to specialised healthcare facilities, the data footprint of an individual patient can be highly fragmented. Under the PDPL, healthcare organisations must better understand how their patient information is collected and where it is stored.

Explicit Consent

Under the PDPL, even where a data subject has consented to the processing of their personal data, for consent of the data subject to be considered to be valid, the consent has to meet certain perquisites including that:

- it must be written, explicit, clear, and specific; and
- it must be issued based on the patient's free will and consent after he/she is fully informed about the purpose or purposes of the processing of the data, and informed, when necessary, of the consequences that will arise from his/her failure to grant approval.

Security Measures

Data controllers are legally compelled to have in place appropriate technical and organisational measures to protect patient data against unauthorised or unlawful processing and against accidental loss, destruction of, or damage. Such measures have to be commensurate with the harm that might result and the nature of the data to be protected, whilst having regard to the state of technological development and

the cost of implementing any measures.

Data Processing Agreements

Where the healthcare organisation is a data controller and uses a third party service provider to act as a 'data processor' to process data on their behalf, the processing must be subject to a written contract that stipulates that the data processor will:

- only engage in processing in accordance with the data controller's instructions; and
- comply with the same security and confidentiality requirements prescribed for the data controller.

In addition, the healthcare organisation needs to ensure that the data processor gives sufficient guarantees regarding the technical and organisational measures it applies to protect the patient data it is processing. Further the healthcare organisation needs to take reasonable steps to verify the data processor's compliance with those measures (e.g. conducting an audit).

Transfer of Data outside of the Kingdom

Healthcare organisations will need to comply with Articles 12 and 13 concerning the transfer of personal data outside of Bahrain. It is a criminal offence to breach these provisions. It needs to be understood that the intent of the law is not to require that patient data is localised in Bahrain, rather that patient data is not to be sent to another country, the laws of which do not provide sufficient protection for that personal information.

Currently, healthcare organisations sending patient data outside of Bahrain would need to fall within an exception in Article 13 (e.g. the transfer is with consent of the data subject or the transfer is needed to perform a contract that the data subject is either a party to or beneficiary of). Importantly, one can transfer data outside of Bahrain if it is in the patient's vital interests (and it is assumed that such provision of healthcare and treatment will be in the patient's vital interest).

The need to fall within an Article 13 exception will change once the implementing regulation is issued; it will identify the names of countries deemed to offer adequate protection of personal data, so that that transfer can be made to such countries under Article 12 without needing any exception.

Clarifying the Current Status of the Law

Some clarification is needed regarding the status of the PDPL as currently not all provisions of the PDPL have come into effect. This is because, under the resolution issuing the PDPL, it is provided that Board of Directors of the Personal Data Protection Authority ('Authority'), will issue the necessary decisions for the implementation of the provisions of the PDPL.

However, as it currently stands no implementing regulations have been issued as the Authority had not yet been established. We expect that this position will change in the near future, as it was recently announced, under Decree No. 78 of 2019 that the Ministry of Justice, Islamic Affairs and Awqaf will assume the responsibility of the duties and powers of the Authority, until such time as the financial budget for the Authority has been allocated within the overall budget of the State, and a Decree forming the Board of Directors of the Authority is issued.

Consequently, at present there are many provisions of the PDPL including, importantly, the need to notify/register with the Authority before processing personal data under Article 14, have not actually been implemented and cannot be complied with immediately (as there have been no decisions on the necessary rules and procedures).

Nevertheless, this does not mean the PDPL does not have legal effect right now. There are provisions of the PDPL that affect healthcare providers that do not require the implementing regulations to be effective. These include all the requirements referred to above.

Although there may not be criminal liability for breaching these provisions, anyone who suffers damages/harm arising from the processing of their personal data in breach of the PDPL is entitled to compensation in order to make reparation for the damage/harm, under Article 57 of the PDPL. This right to compensation appears to have come into effect on 1, August of this year.

There are also criminal penalties under Article 58 of the PDPL that do not require implementing regulations. These are:

- processing sensitive information in violation of Article 5;
- transferring personal data outside of the Kingdom of Bahrain in violation of either Article 12 or 13; and
- unnecessarily disclosing data in violation of the provisions PDPL.

The penalty in each case is imprisonment for a period not exceeding one year and/or a fine of not less than BHD1,000 (approximately US$2,650) and not exceeding BHD20,000 (approximately US$195,000). As these are criminal matters, the public prosecutor can take action in the absence of the Authority.

What Needs to be Done?

If it has not already been done, health organisations in Bahrain must review their policies, procedures, and practices with regard to how they process patient data so as to ensure compliance with the PDPL.

In particular, as it now stands, the PDPL requires that health organisations should:

- have a privacy notice notifying patients of information, as required by Chapter V of the PDPL, including the patient's right to access their personal information and to object to the processing of their data in certain circumstances;
- ensure their patient consent processes meet the requirements of the PDPL;
- have data processing agreements with data processors that contain the stipulations prescribed by the PDPL; and
- currently, only transfer patient data outside of Bahrain if the transfer falls within one or more of the exceptions set out in Article 13 of the PDPL that permit such a transfer.

Once the implementing regulations have been issued there will be additional actions (including making notifications to the Authority) that will likely be required.

Al Tamimi & Company's Technology Media & Telecommunications team and its Healthcare Practice in Bahrain regularly advise on laws and regulations impacting the healthcare sector. For further information please contact healthcare@tamimi.com.