



## Client Alert

March 2019

### **UAE issues law to protect health data and restrict its transfer outside the country**

*Important changes are coming for anyone who collects, processes or transfers electronic health data originating in the UAE. Besides a host of new data protection measures and new rules around use of a centralized database managed by the United Arab Emirates (UAE) Ministry of Health, a general prohibition on transferring health data outside the UAE may have a significant impact on healthcare service providers and life sciences companies operating locally. Cloud based health solutions which involve collection, storage and processing of health data, such as wearables and health monitoring apps, may be particularly affected. While the full extent of the new requirements is still not clear, it is imperative for companies operating in the sector to carefully monitor developments.*

On 6 February 2019, the President of the UAE issued Federal Law No. 2 of 2019 (the **Law**) which regulates the use of information technology and communications (ITC) in the healthcare sector. This eagerly anticipated Law:

- aims to raise the minimum bar for protection of health data and to introduce certain concepts which are on a par with best international practice in information law;
- continues the legislative trend towards localization of sensitive categories of data; and
- paves the way for centralized health data capture and analysis to support public health initiatives conducted by the UAE Ministry of Health.

The Law has been published in the Federal Gazette on 14 February 2019 and will come into force three months from publication. The implementing regulations which will provide further details on its application are to be issued within six months from the date of publication.

#### **Which entities does the Law apply to?**

The Law applies to all entities operating in the UAE, whether onshore or from one of its free zones (including Dubai Healthcare City), which provide:



- healthcare services;
- health insurance services (including insurance brokers or providers of related administrative services);
- healthcare IT services; or
- any other services, directly or indirectly, related to the healthcare sector, or engaged in activities that involve handling of electronic health data.

In this alert we refer to these parties collectively as **Healthcare Service Providers**.

### **What are the new requirements of the Law?**

#### **1. Regulation of health data**

The scope of the Law is broad - it regulates the processing of all electronic health data regardless of its form, including names of patients, information collected during consultation, diagnosis and treatment, alpha-numerical patient identifiers, common procedural technology (CPT) codes, images produced by medical imaging technology, and lab results among other types of data.

#### **2. Prohibition on storage of health data outside of the UAE**

The Law formalizes the longtime informal regulatory policy that health data must be processed and stored inside the UAE. Critically it provides that such data may not be transferred outside of the UAE, except where an exception is issued by the relevant health authority. The Law also prohibits the creation of health data outside of the UAE which relates to health services provided inside the UAE. Accordingly, cloud solutions hosted out of country, outsourcing of IT services to overseas locations, remote IT support from other departments within multi-national Healthcare Service Providers and remote collection and monitoring of patient information within the UAE, such as heart rate, sleep patterns, or steps walked, from outside the UAE through apps and wearables may be significantly impacted.

The Law envisages certain exceptions to the default data localization requirements. These will be set out in subsequent ministerial resolutions or the implementing regulations.

#### **3. Minimum standards for processing of health data**

In addition to reinforcing the duty of Healthcare Service Providers to maintain the confidentiality of health data, the Law introduces a number of concepts familiar from overseas data protection frameworks. For example:

- **Purpose limitation:** Patient information must not be used other than for the purpose of the provision of health services, except with the prior consent of the patient;



- **Accuracy:** Healthcare Service Providers must ensure that the health data processed is accurate and reliable;
- **Security measures:** Healthcare Service Providers must put in place measures to protect health data and to prevent its unauthorized processing, damage, alteration, deletion or amendment; and
- **Non-disclosure/patient consent:** The Law reiterates existing obligations not to disclose patient data to any third party without the prior consent of the patient.

#### 4. Retention period

Health data must be retained for a minimum period of 25 years from the date on which the last procedure on the patient was conducted, or as long as is necessary if longer.

#### 5. Centralized data management system

A new centralized data management system (**DMS**) will be established and operated by the UAE Ministry of Health to facilitate access to, storage and exchange of health data. Healthcare Service Providers are required to register to access the DMS and identify all members of personnel who are authorized to access it.

#### 6. Website blocking for advertisement or licensing violations

The UAE Ministry of Health is entitled to instruct the relevant local or federal health authorities to block any website, whether inside or outside of the UAE that does not comply with the regulations applicable to healthcare advertising or which provides healthcare information without a license or permission from the UAE Ministry of Health.

### Are there any permitted exceptions to the general rules?

The only circumstances in which a patient's information may be used or disclosed without the patient's consent are:

- to allow insurance companies and other entities funding the medical services to verify financial entitlement;
- for scientific research (provided that the identity of the patient is not disclosed and applicable scientific research standards and guidelines are complied with);
- for public health preventive and treatment measures, for example. in the case of a public health crisis;
- at the request of a competent judicial authority; or
- at the request of the relevant health authority for public health purposes including inspections.



### **How does the Law address data anonymization?**

The role of 'big data' in the prevention and early detection of serious conditions and in research and development has been an area of focus and collaboration between major players in the IT and healthcare sectors in recent years. There is a delicate balance to be struck between the potential benefits of this practice and the protection of each individual's right of privacy. Where to draw the line in this assessment remains a topic of discussion between industry stakeholders and regulators, particularly in light of high profile breaches in recent years such as the collaboration between the Royal Free London NHS Trust and Google Deep Mind to identify patients at risk of kidney disease, or in the context of using health data for secondary research purposes. In January 2019 the European Data Protection Board issued its opinion on the European Commission's draft Q&A on the interplay between data protection under the EU General Data Protection Regulation and clinical trials regulation. We will need to wait for the Law's implementing regulations to see what position the UAE authorities will take on this sensitive issue.

### **What are the penalties for non-compliance?**

As well as certain penal sanctions for breach of key requirements, such as the data localization obligations, the Law sets out a number of overarching disciplinary sanctions for breach of its provisions. These sanctions range from warnings to fines of AED 1 million and/or cancelling the breaching company's permit to use the DMS.

### **What's next?**

While the Law sets out the basic framework to establish DMS and to formally regulate the processing of health data and patient information, there are a number of important details that still need to be addressed by the implementing regulations and/or in further ministerial resolutions. These include, most notably, the rules and process for registering to access the DMS and the exemptions from data localization requirements.

Healthcare Service Providers are likely to be granted a grace period to achieve compliance with the Law. We will continue to monitor developments closely and will issue further updates as subsequent regulations are released.

***To speak to us in relation to any healthcare data issues in the UAE, please feel free to contact one of the lawyers below, or your usual Baker McKenzie contact.***



## Contacts



**Zahi Younes**  
Partner, Corporate/Healthcare  
Regulatory, UAE/KSA  
Zahi.Younes@  
bakermckenzie.com



**Els Janssens**  
Senior Associate  
Healthcare Regulatory, UAE  
Els.Janssens@  
bakermckenzie.com



**Kellie Blyth**  
Head of IT &  
Communications, UAE  
Kellie.Blyth@  
bakermckenzie.com



**Ghada El Ehwany**  
Counsel, Corporate/Healthcare  
Regulatory, UAE  
Ghada.ElEhwany@  
bakermckenzie.com

[www.bakermckenzie.com](http://www.bakermckenzie.com)

Abu Dhabi  
Level 8, Al Sila Tower  
Abu Dhabi Global Market Square  
Al Maryah Island  
P.O. Box 44980  
Abu Dhabi, UAE

T: +9712 6123700  
F: +9712 6581811

Dubai - Business Bay  
Level 14, O14 Tower  
Al Abraj Street  
Business Bay  
P.O. Box 2268  
Dubai, UAE

T: +9714 4230000  
F: +9714 4479777

Dubai - DIFC  
Level 3, Tower 1  
Al Fattan Currency House  
DIFC  
P.O. Box 2268  
Dubai, UAE

T: +9714 4230005  
F: +9714 4479777

Baker & McKenzie Habib Al Mulla is a member firm of Baker & McKenzie International, a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

© 2019 Baker & McKenzie Habib Al Mulla