Your World First

C/M/S/
Law.Tax

Dubai Healthcare City - Health and Pharma Overview

November 2019

TABLE OF CONTENTS

1. INTRODUCTION

Up until recently, there were no explicit laws or authorities that dealt specifically with privacy and data protection in the UAE (excluding the Dubai International Financial Centre ('DIFC') and Abu Dhabi Global Market). The concepts of privacy and data protection were considered in a variety of federal laws and industry specific regulations set out below.

However, the introduction of Federal Law No. 2 of 2019 ('the Healthcare Data Protection Law') (only available in Arabic here) to the Dubai Health Care City ('DHCC') marks the first occasion where a specific law dealing with the protection of individuals' data has been specifically addressed in the UAE, and highlights a growing trend towards the development of more specific legislation to deal with personal data, cybersecurity and privacy issues across the Gulf Cooperation Council economies.

Furthermore, companies based in the UAE will need to consider the extent to which they may need to comply with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). Whilst the GDPR applies to companies located within the EU that hold personal data, it also applies to companies located outside the EU, such as the UAE, provided that such companies:

- offer (or envisage offering) goods or services to data subjects in the EU; or
- monitor the behaviour of data subjects in the EU.

Currently, 'personal data' is not defined under the laws of the UAE. Consequently, references to the same in this chapter are in its broader sense, and generally refer to data pertaining to individuals' private and family life, as such reference is set out to what pertains to be protected data under current UAE legislation, as set out under the Penal Code 1987 (Federal Law No. 3 of 1987) ('the Penal Code').

1.1 Legislation

- the Healthcare Data Protection Law
- the Health Data Protection Regulation 2013 (DHCC Regulation No. 7 of 2013) ('the DHCC Data Protection Regulation')
- the Federal Law No. 5 of 1985 Issuing the Civil Transactions Law (only available in Arabic here) ('the Civil Code')
- the Electronic Transactions and Commerce Law 2002 (Dubai Law No. 2 of 2002) (only available in Arabic here)

- the Federal Decree-Law No. 5 of 2012 on Combating Cybercrimes ('the Cybercrime Law')

1.2 Supervisory authorities

- the Ministry of Health and Prevention ('MOHAP')
- the Dubai Healthcare City Authority – Regulatory ('DHCR')
- the Customer Protection Unit at the Center of Healthcare Planning and Quality at Dubai Healthcare City Free Zone ('the Customer Protection Unit')

1.3 Guidelines

There are no relevant guidelines to date. However, guidelines will shortly be issued to support the Healthcare Data Protection Law.

1.4 Definitions

The Healthcare Data Protection Law provides the following key definitions:

Data: Whichever that may be stored, processed, generated and transformed through the information and communication technology, such as numbers, letters, codes, images and the like.

Health Information: Health data which has been processed and has visual, audio or legible meaning, and is characterised by the health feature, whether related to the health or insurance establishments, authorities or to the beneficiary from the health services.

Process: Information creation, introduction, amendment, update or deletion electronically.

Circulation of Health Information: Accessing, exchanging, copying, photocopying, transforming, storing, publishing, disclosing or sending health data and information.

Information and Communication Technology: Technological and electronic tools or systems or other means allowing the possibility of processing all types of information and data, including the possibility of storing, recovering, publishing and exchanging them.

The DHCC Data Protection Regulation provides for the following key definitions:

Patient Health Information: Information about a patient, whether spoken, written, or in the form of an electronic record, that is created or received by any licensee, that relates to the physical or mental health, or condition of the patient, including the reports from any diagnostic procedures and information related to the payment for services.

Process: Any operation or set of operations which is performed on patient health information, whether or not by automatic means such as collection, recording, organisation, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, erasure or destruction.

2. CLINICAL RESEARCH AND CLINICAL TRIALS

2.1 Data collection and retention

Data Collection

Healthcare Data Protection Law

As a general rule, it is prohibited for those who have access to individual's personal data to disclose or publicise that information without obtaining the individual's express consent.

Under the Healthcare Data Protection Law, the MOHAP will develop a central healthcare IT system ('the Central IT System') responsible for keeping, exchanging, collecting health data and information to enable healthcare entities to access data in a secure manner, subject to any control and/or supervision by the UAE Government. Only organisations authorised by the local health authority will have access to the Central IT System.

From a practical perspective, access to data through the Central IT System will need to be managed and controlled, and only authorised individuals may be given access to such information. Procedures will need to be put in place by the organisations in the healthcare sector to ensure integrity and accuracy of data. Implementing regulations to the Healthcare Data Protection Law ('the Implementing Regulations') are expected to add further detail to clarify the metrics around who will be authorised to use and access the Central IT System and how this will be managed and controlled. However, the Implementing Regulations are yet to be published.

DHCC Data Protection Regulation

The DHCC Data Protection Regulation provides that, in the event of collection of data, patients and/or their representatives must be aware of the following:

- the fact that their information is being collected;
- the purpose for which the information is collected;
- the name and address of the healthcare professional or entity which is collecting the information and/or holds such patient information;

- whether or not supply of patient information is voluntary or mandatory; consequences (if any) for that patient if all or part of the requested patient health information is not provided; and
- the right of access to and correction of patient health information.

It is not necessary for the healthcare professional and/or entity to make the patient or representative aware of the above information where compliance would prejudice either:

- the interests of the patient; or
- the purposes of the collection of such information.

Data Retention

Healthcare Data Protection Law

The Healthcare Data Protection Law currently provides that healthcare bodies need to retain health data for at least 25 years following the last point of contact with the patient.

DHCC Data Protection Regulation

The DHCC Data Protection Regulation provides that a healthcare professional and/or healthcare entity must retain patient health information in a secure environment for the following periods:

- medical and dental records of UAE national and expatriate patients - 10 years after the date of last entry into the record;
- medical and dental records of children – 10 years after the person has reached the age of 18 years old;
- medical and dental records of medico-legal cases – 20 years after the date of last entry into the record;
- medical and dental records of deceased patients – 10 years after the date of last entry into the record; or
- for any longer periods of time as may be specified by the Central Governance Board or relevant agency from time to time.

The above does not apply to:

- actual photographs, films, scans, recordings and other such images, unless necessary for purposes of a medical treatment or surgical procedures; or
- where holding any document is necessary or describable for providing healthcare services to the patient.

Organisations operating in the healthcare space should also be aware of the limitation periods for raising a claim in the event of dispute under UAE law, currently set out in the Civil Code and Federal Law on Commercial Transactions 1993 (Federal Law No. 18 of 1993) as follows:

- 15 years for breach of contracts;
- 10 years for breach of commercial contracts; and
- three years for any claims under tort/negligence.

2.1.1 Consent

Under UAE Federal Law, consent of an individual is required before processing personal data to the extent that such data is related to an individual's private life. Consent must be expressly given, in an easily accessible form, with details of the purpose for the processing of their data clearly set out. The data subject must have the right to expressly withdraw such consent at any point. Online consent will be acceptable under local laws as long as it is clear and freely given and capable of being recorded and reproduced in a hard copy format.

The permission of a parent or legal guardian is required to allow the processing of a minor's personal data. A minor is anyone under the age of 21. However, it is common practice for minors' data to be processed using the same consent mechanisms as adults. The validity of this mechanism has not yet been tested by the local courts.

Under the Penal Code, the requirement to obtain the individual's written consent can be waived where:

- a UAE official or public authority has required the transfer of the data to it; or
- the transfer serves public interests or national security.

2.1.2 Data obtained from third parties

The Penal Code stipulates that data subjects should provide consent to the transfer of personal data to third parties inside or outside the UAE.

The Healthcare Data Protection Law prohibits storage and processing of data related to services provided within and outside of the UAE. It is yet to see whether this will be lifted by the MOHAP.

3. PHARMACOVIGILANCE

Not applicable.

4. BIOBANKING

Not applicable.

5. DATA MANAGEMENT

UAE laws do not have specific definitions for data controllers and data processors. To date, there are no specific Federal Laws in the UAE that impose obligations on data controllers to ensure data is processed properly.

Sectoral laws and regulations, such as the Cybercrime Law, require service providers to take measures to prevent the unauthorised use or disclosure of personal data.

Security

As a matter of good practice, entities which process or store health data should notify data subjects whose data is at risk of compromise in order to avoid potential legal action.

The DHCC Data Protection Regulation provides that a healthcare professional and/or entity is responsible for the security of its information systems and networks and should:

- act in a cooperative manner to prevent, detect and respond to security incidents;
- review and assess security of information systems and networks and put relevant policies and measures in place on a regular basis;
- disclose security incidents to the Customer Protection Unit;
- ensure that patient health information is stored in a manner that ensures accuracy and easy removal of information as and when required;
- ensure that patient health information is protected by ensuring appropriate security safeguards are in place to prevent misuse, loss, destruction, theft, use and modification;
- where information is no longer necessary, ensure that the document is disposed in a secure manner that preserves the privacy of the information contained in a document; ensure that information is not disclosed to any person other than the intended recipient;
- ensure that patient health information is only disclosed by facsimile in accordance with the DHCC Data Protection Regulation, once the healthcare professional and/or entity has verified its identity, and confirmed that the facsimile number is correct; and
- ensure that patient health information is only disclosed electronically as stipulated by the Central Governance Board of the DHCR.

6. OUTSOURCING

Not applicable.

7. DATA TRANSFERS

The Penal Code provides that the data subject's consent is required to transfer personal data to third parties inside or outside the UAE.

Healthcare Data Protection Law

The Healthcare Data Protection Law expressly prohibits the storage and processing outside the UAE of health information related to services provided within the UAE.

This prohibition can only be lifted by a resolution issued by the local Emirate health authority in coordination with the MOHAP, providing permission for this transfer. The Implementing Regulations were due to provide further detail around this process and the types of transfers which are and are not permissible. However, as mentioned above, the Implementing Regulations are yet to be published.

On the basis of the Healthcare Data Protection Law, organisations will need to assess two key components when considering whether or not a transfer of data will be prohibited:

- whether the data collected is related to services provided in the UAE; and
- whether such data comprises health information.

DHCC Data Protection Regulation

The DHCC Data Protection Regulation provides that patient health information may only be transferred to a third party located in a jurisdiction outside Dubai Healthcare City Free Zone if:

- there are laws in place that ensure an adequate level of protection for such information; and
- the patient has consented to the transfer of information or such transfer is necessary for the ongoing provision of healthcare services to that particular patient.

A jurisdiction shall be considered to have an adequate level of protection if that jurisdiction is listed as an acceptable jurisdiction under the Data Protection Law (DIFC Law No. 1 of 2007), or has the written approval of the Central Governance Board of the Dubai Healthcare City Free Zone Authority.

8. BREACH NOTIFICATION

Not applicable.

9. DATA SUBJECT RIGHTS

Data subjects' express consent is required before the collection and processing of any of their personal data. If consent is not obtained in such circumstances, the penalties listed under section 6 below may apply.

10. PENALTIES

UAE law requires employers to take measures to prevent the unauthorised use or disclosure of personal data. Companies may be vicariously liable for failure to take action against or stop employees known to be involved in the unauthorised disclosure of personal data. The relevant provisions of UAE law are detailed below.

Healthcare Data Protection Law

Chapter 3 of the Healthcare Data Protection Law sets out various disciplinary actions for violating the law, including written notice, warning letters, a monetary penalty (not less than AED 1,000 (approx. €247) and not exceeding AED 1 million (approx. €247,000)), suspension or permanent withdrawal from the Central IT System, which may impact the way in which business is run.

Cybercrime Law

Article 2 of the Cybercrimes Law prohibits the disclosure, publication and republishing of any information that was obtained by unauthorised access to websites or electronic information systems or networks.

Article 4 of the Cybercrimes Law provides that any person who enters, without permission, into any electronic site for the purpose of obtaining confidential information of a financial trade or economic establishment shall be punished by temporary imprisonment and/or a fine of not less than AED 250,000 (approx. €62,000) and not exceeding AED 1,500,000 (approx. €370,000). The penalty is increased if such data is changed, copied, deleted, disclosed, or published, which includes a fine of not less than AED 250,000 and not exceeding AED 1,500,000, and/or imprisonment for a period not less than five years.

Article 21 of the Cybercrimes Law prohibits the invasion of privacy of an individual by means of a computer network, and/or electronic information system, and/or information technology, without the individual's consent, and unless otherwise authorised by law. Any individual in

breach shall be punished by imprisonment for a period not less than six months and/or a fine not less than AED 150,000 (approx. €37,000) and not exceeding AED 500,000 (approx. €124,000). The Article further sets out examples of assaulting the privacy of person including transferring and transmitting or disclosure of conversations, communications.

Article 17 of the Cybercrimes Law provides that companies may be vicariously liable for failure to take action against or stop employees known to be involved in any of the activities prohibited by the law.

Article 22 of the Cybercrimes Law prohibits disclosing confidential information obtained in the course of, or because of, work, by means of any computer network, website or information technology. Any individual found in breach shall be imprisoned for not less than six months and/or fined not less than AED 50,000 (approx. €12,400) and not exceeding AED 1 million (approx. €247,000).

Penal Code

Article 378 of the Penal Code provides for imprisonment of up to 1 year and/or a fine of up to AED 10,000 (approx. €2,470) for any individual found to have published any news, pictures or comments with the intention of revealing secrets of an individual's private or family life, without that individual's consent regardless of whether such publications are true.

Article 379 of the Penal Code provides for imprisonment of up to 1 year and/or a fine of up to AED 20,000 (approx. €4,940) for any individual entrusted with a secret due to his/her profession and who is found to have disclosed it in cases other than those lawfully permitted, or who is found to have used such a secret for his/her own private benefit or for the benefit of another person, without the individual's consent.

Corporate entities can also be guilty of the offences established by the Penal Code through their directors, agents or other representatives.

Criminal sanctions may also be enforced by the police against the offender for violations of the Penal Code and/or the Cybercrime Law, and prosecuted by the public prosecutor. Additionally, the data subject can lodge a claim under civil courts or even attach a civil claim to the criminal proceedings.

11. OTHER AREAS OF INTEREST

Ministerial Resolution No. 430 of 2007 on the Regulation of Health Advertisements (only available in Arabic here) sets a range of requirements on the advertisement and registration of medical devices insofar as such devices are marketed or sold in the UAE.

ABOUT THE AUTHORS

Rob Flaws
CMS UAE

Robert is a partner in the Technology, Media & Telecommunications Department with over 10 years of international experience supporting the delivery of private and public sector technology and communications projects. Since relocating to the Middle East in 2011, Robert has been engaged on numerous projects including mobile network procurements and rollouts, managed services outsourcing for mobile operators, business process outsourcings and tower sale and lease-back initiatives. Most recently, Robert spent time on secondment working with one of the largest mobile, telecoms and media services providers in the UAE, as a key part of their technology and procurement legal team. Robert is a regular participant at industry events and enjoys sharing trends, experiences and best practices with participants in MENA's vibrant and ever changing telecoms industry.

rob.flaws@cms-cmno.com

RELATED CONTENT

NEW POST

Germany: BSI issues guidelines on safety of medical devices

NEW POST

Pakistan: SBP issues regulations on digital on-boarding of merchants

LEGAL RESEARCH

Special category data (November 2019)

NEW POST

UK: ICO publishes guidance on special category data processing

NEW POST

Spain: AEPD publishes guide for patients and users in health sector