Healthcare data protection in the UAE

A new federal law

pwc

With Europe leading the charge on data privacy and protection in the form of the General Data Protection Regulation (**GDPR**) and the latest draft of the EU e-Privacy Regulation, the feeling in the Middle East in recent times is that it would be a positive move for Gulf nations to introduce specific local data protection and privacy regulations. The UAE Free Zones, such as the Dubai International Financial Centre, Abu Dhabi General Market and Dubai Healthcare City, do have specific data protection regimes in place that are largely modelled on, and inspired by, the privacy and data protection principles and guidelines contained in the 1995 Data Protection Directive and 1980 OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. What has been noticeably absent in the UAE to date however, has been a specific federal data protection law – until now.

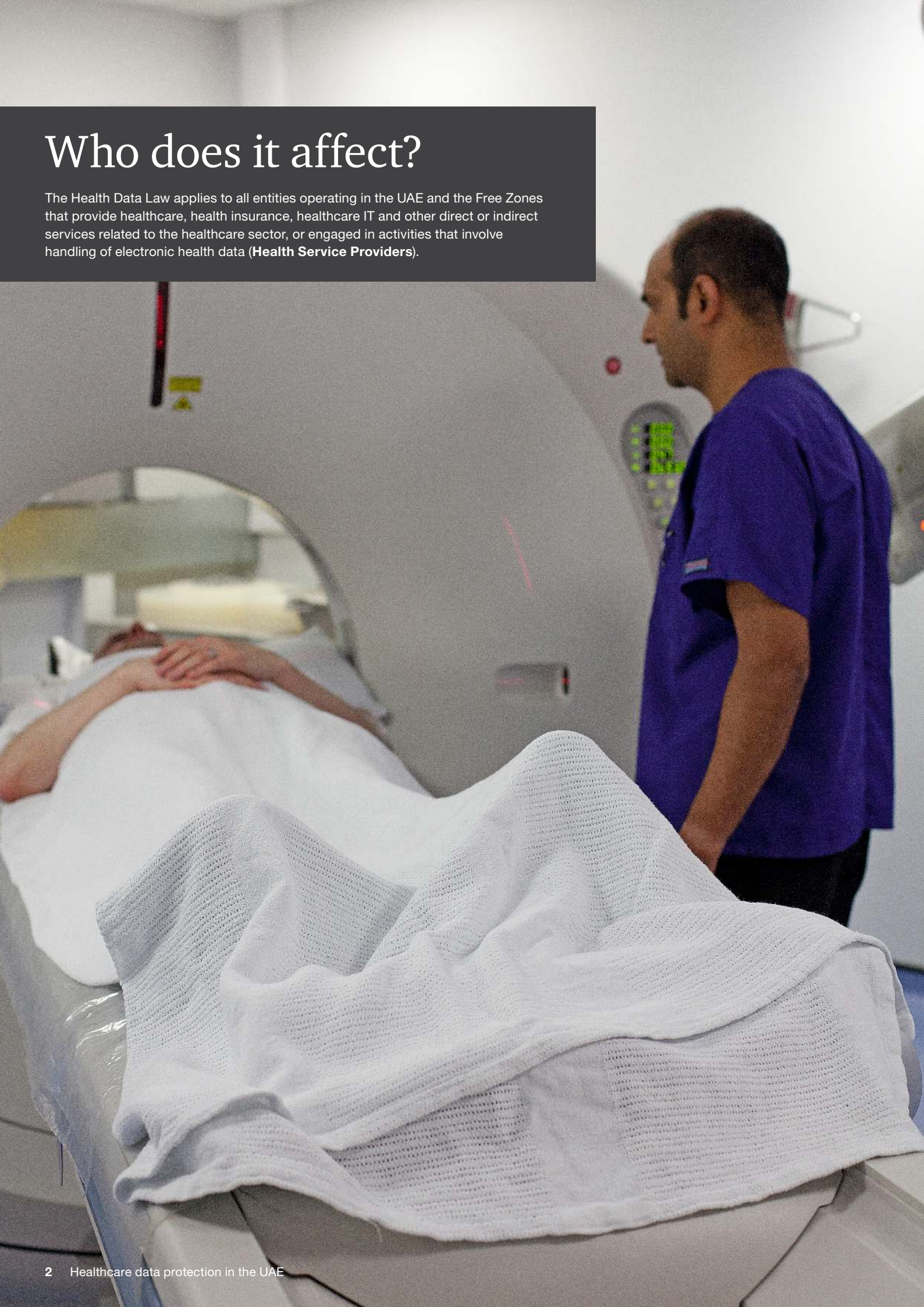
In February 2019, the President of the UAE issued Federal Law No 2 of 2019 (**Health Data Law**) which regulates the use of information technology and communications (**ITC**) in the healthcare sector. This is the first piece of federal legislation in the UAE that directly addresses data protection principles. The law introduces familiar data protection concepts such as purpose limitation, accuracy, security measures and consent to disclosure, similar to the GDPR.

The law is also timely in that it comes on the heels of a recent Opinion of the European Data Protection Board on the interplay between the GDPR and the EU regulation relating to clinical trials and a Recommendation from the Council of Europe on the protection of health-related data by EU Member States.

Contents

Who does it affect?

The Health Data Law applies to all entities operating in the UAE and the Free Zones that provide healthcare, health insurance, healthcare IT and other direct or indirect services related to the healthcare sector, or engaged in activities that involve handling of electronic health data (**Health Service Providers**).



What are the key components of the law?

Data processing

The Health Data Law regulates the processing of electronic health data originating in the UAE, including patient names, consultation, diagnosis and treatment data, alpha-numerical patient identifiers, common procedural technology codes, medical scan images and lab results **(Health Data**).

The law also introduces familiar data privacy and protection concepts:

- **Accuracy** – Healthcare Service Providers must ensure that the Health Data they process is accurate and reliable;
- **Purpose limitation** – Health Data must not be used other than for the purpose of the provision of health services, except with the prior consent of the patient;
- **Consent to disclosure** – Health Service Providers cannot disclose patient data to any third party without the prior consent of the patient or as permitted by law; and
- **Security measures** – Health Data must be kept safe from unauthorised damage, amendment, alteration, deletion or addition using appropriate security measures.

Data security

Article 4 of the Health Data Law mandates that all Health Service Providers that use ICT on Health Data ensure that such information will be kept confidential and will not be shared without authorisation. In terms of security, the law is faithful to the principles of the GDPR, requiring the 'validity and credibility' of the Health Data to be ensured by keeping it safe from 'non-authorised damage, amendment, alteration, deletion or addition.'

The law also requires Health Service Providers to ensure the availability of Health Data and facilitate the access to it by those authorised to have such access. This includes allowing access only to those authorised personnel who understand the need for patient confidentiality.

In keeping with international data protection standards and best practices, the Health Data Law requires entities to introduce technical, operational and organisational procedures to ensure the integrity and security of Health Data.

Data localisation

One of the most impactful aspects of this new law will be the general prohibition on transferring health data outside the UAE unless authorised by the relevant health authority in coordination with the government ministry (Article 13). This provision represents a codification of the long-time informal regulatory policy that Health Data must be processed and stored inside the UAE.

From a practical perspective, the requirement will have a significant impact on businesses currently relying on data storage solutions or data processors outside the UAE (e.g. via cloud or hosting services). Article 13 will equally impact those providers currently offering such services into the UAE.

Whilst some relief may be provided (as the law envisages certain exceptions to this data localisation requirements), this will only come down the line in subsequent ministerial resolutions or the implementing regulations.

Data retention

Under Article 20, Health Data must be retained for as long as it is required but in any event not less than 25 years from the date on which the last procedure on the patient was conducted. The Health Data Law departs from the GDPR in this respect, with the latter requiring personal data be kept for no longer than is necessary for the purposes for which the personal data are processed. This represents a significant compliance burden for Health Service Providers who must ensure that they have the capabilities and data storage systems to comply.

Centrally controlled healthcare IT system

A centralised Health Data management system, controlled by the Ministry of Health and Prevention, will be developed. The system will house the Health Data collected by Health Service Providers and will enable them to access and exchange this data in a uniform and secure way, subject to any controls determined by government.

Exceptions to disclosure restrictions

Under Article 16, Health Service Providers may use or disclose Health Data without the consent of the patient:

- to allow insurance companies and other entities funding the medical services to verify financial entitlements;
- 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;
- to comply with a request from a competent judicial authority; or
- to comply with a request from the relevant health authority for public health purposes including inspections.

Sanctions

The law contains a regime of sanctions for non-compliance including disciplinary actions and monetary fines which may be imposed by a disciplinary committed within each health authority. These sanctions may be imposed, for example, for violating the data localisation rules.

Specifically, sanctions include:

- the potential suspension or withdrawal of the licence to use the central IT system;
- a formal notice or warning from the relevant health authority; and/or
- fines ranging from AED 1,000 to AED 1,000,000.

What do you need to do?

Entities operating in the healthcare sector should begin looking at how they will comply with the Health Data Law. As the law relates to the processing of Health Data, a practical first step would be for entities to conduct a data discovery exercise to create an inventory of all data in scope for the law. In order to comply with the law, entities will also need to make changes to their policies, procedures, controls and systems. To do this, entities should first conduct a gap assessment against the Health Data Law to build up an implementation roadmap.

Below is PwC's suggested approach to compliance with the Health Data Law.

Assess current capabilities

Risk analysis and data discovery

How we can help

- Stakeholder engagement and communications plan
- Personal data inventory
- Data flow maps showing the movement of personal data from collection through to disposal

Gap assessment

How we can help

- Control gap analysis
- Risk assessment based on current and planned future uses of personal data

Design the future state

Target operating model and programme design

How we can help

- Detailed remediation project plan with identified organisational impact
- Cross-functional working group established

Programme implementation

How we can help

- Strategy and governance
- Policy management
- Cross-border data strategy
- Data life-cycle management
- Individual rights processing
- Privacy by design
- Information security
- Privacy incident management
- Data processor accountability
- Training and awareness

Operate and sustain

Ongoing operations and monitoring

How we can help

- Defined ongoing monitoring programme
- Tracking and retesting of non-compliance
- Protocols for changes to policies and procedures

Conclusion

As the Health Data Law was only published in February 2019, the full extent of its requirements remain to be seen. The law will come into force in May 2019 but will amount to only a basic framework to set initial rules and establish the central IT system. Further implementing regulations detailing its application will follow by August 2019, which will provide important clarity in areas such as the rules and process for registering to access the centralised Health Data management system and any exceptions to the data localisation requirements.

It is expected that Health Service Providers will be provided a grace period in which to achieve compliance with the new law.

Contact us

For more information on how this affects your organisation, please get in touch.

Matthew White
Partner, Digital Trust Leader

M: +971 (0)56 113 4205
E: matthew.white@pwc.com

Hamish Clark
Partner, Health Industries Consulting Leader

M: +971 (0)50 634 6943
E: hamish.clark@pwc.com

Phil Mennie
Director, Digital Trust

M: +971 (0)56 369 7736
E: phil.mennie@pwc.com

Richard Chudzynski
Senior Manager, PwC Legal

M: +971 (0)56 417 6591
E: richard.chudzynski@pwc.com

Gordon Wade
Manager, PwC Legal

M: +971 (0)50 143 5619
E: gordon.wade@pwc.com

190403-101052-PB-OS