

Privacy in a UAE Healthcare Context

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data
n.oconnell@tamimi.com - Riyadh

February 2014

Privacy also has practical significance in an efficient, modern healthcare system. In this article, we consider the importance of privacy in a healthcare context, and touch on some of the laws in place in the UAE to protect patient privacy.

Reliable personal data is an essential part of modern healthcare. It allows public health authorities, researchers and healthcare providers, to improve knowledge, efficiency and quality, resulting in better use of limited resources and the delivery of better healthcare solutions to patients.

Underpinning the use of personal data in a healthcare context is trust. Patients need to be able to trust their healthcare providers and medical practitioners. In the absence of trust, patients are less likely to regularly use the same providers or practitioners, and more likely to withhold personal information or provide personal information that is inaccurate. Where there is no trust, patient data becomes less reliable, and treatment outcomes may suffer as treatment decisions are based on incomplete or incorrect information. In this type of environment, healthcare operations are less efficient, and reputations suffer as providers or practitioners are seen as responsible for less-than-ideal outcomes. Where personal data is unreliable, public health suffers as researchers and policy-makers base their theories and projections on incorrect assumptions, and resources are used inefficiently.

The importance of reliable personal data in a healthcare context cannot be underestimated. This is one of the reasons that many jurisdictions have introduced data protection laws aimed at ensuring compliance with certain principles when collecting and using personal data, providing data subjects with some degree of control over their personal information, and establishing a framework for addressing inappropriate handling of personal data.

Data protection in the UAE

The UAE does not have a modern data protection law of the type found in member states of the European Union, for example. Data protection issues are generally assessed with reference to privacy-related provisions found in legislation and regulations not specifically focused on data protection or privacy. Of primary relevance is Article 379 of the Penal Code, which relates to the use or disclosure of "secrets" without the consent of the person to whom the secret relates:

[...] Any individual who, by reason of his profession, craft, circumstance or art is entrusted with a secret and who discloses it in cases other than those permitted by the law, or who uses it for his own advantage or another person's advantage, shall be [punished] unless the individual to whom the secret pertains has consented that it be disclosed or used.

Whether the subject personal information is 'secret', will be a question of fact. There is no clear judicial guidance on the meaning of the term 'secret'. Without needing to come to a clear conclusion as to whether or not the subject information is likely to be considered 'secret' by a UAE court, it is clear that obtaining the consent of the person to whom the information relates would eliminate the risk of breaching this Penal Code prohibition. When gathering personal information, it would be important to ensure that such consent encompasses the proposed scope of use of such personal information.

Additionally, there are other provisions that apply specifically in a healthcare context. By way of example, we set out below brief descriptions of some patient privacy related laws, regulations, and guidelines.

Confidentiality obligations of healthcare practitioners

Obligations of confidentiality on healthcare practitioners can be found in a number of documents.

- Federal Law No. 7 of 1975 Concerning the Practice of Human Medicine Profession, governing doctors licensed in the UAE, provides that, in the absence of the patient's consent, no doctor has the right to divulge a private secret, either if the patient has directly confided it to him or he has come to know it by himself in the course of his work.
- The Ministry of Health Code of Conduct 1988 governing medical practitioners, pharmacists and other healthcare professionals licensed in the UAE (nurses and laboratory technicians, for example), requires complete confidentiality of information related to patients (including medical records, health problems and personal information related to the patient) and prohibits disclosure without the patient's prior informed consent.

Obligations relating to the confidentiality of patient information can also be found in other sources, including local health insurance laws and regulations applicable in certain jurisdictions.

DHCC Health Data Protection Regulations

Dubai Healthcare City Governing Regulation No. 7 of 2008 regulates the use and disclosure of "Patient Health Information" (including personal information and medical information relating to a patient's physical or mental health) by entities licensed in the Dubai Healthcare City - a healthcare-related free zone in the Emirate of Dubai.

The Regulations provide a number of 'Health Data Protection Principles'. These address aspects including the manner and purpose of collection of patient health information, the source of such information, the storage and security of such information, access and correction, retention, and limits on use and disclosure. Licensed entities are required to identify one or more individuals to act as Data Protection Officers within their organisations, and the Regulations provide for the establishment of a Health Data Protection Ombudsman responsible for the administration of the Regulations and for investigating complaints made under the Regulations. The Regulations also provide a procedure for the transfer of patient health information to places outside Dubai Healthcare City, as well as procedures for patients to request access to, and correction of, Patient Health Information. The Regulations can be seen as quite similar to the type of data protection legislation found in European countries.

It is important to note that a general review of the Dubai Healthcare City Regulations occurred in 2013. The impact of that review on the Regulations relating to Patient Health Information is not yet known. There is some likelihood that changes to the regulatory regime for Patient Health Information may be announced in the near future.

HAAD Data Standard

The Health Authority Abu Dhabi's Data Standard dated 24 January 2008 (and revised most recently on 19 February 2013) requires that partners involved in healthcare delivery in the Emirate of Abu Dhabi develop and institute policies and procedures relating to "Confidential Health Information", which includes information that can be used to identify a patient. Policies developed pursuant to HAAD's Data Standard are required to ensure that only the minimum necessary personnel have access to Confidential Health Information, and such information must be kept from unauthorized access. Policies must specify sanctions applicable for breach, and external breaches will be subject to investigation and prosecution by appropriate law enforcement authorities. The policies and procedures must be available for inspection and demonstrable upon request, and HAAD has indicated that it will make default policies and procedures available.

Information security

'Data protection' and 'information security' are clearly related, although not synonymous. 'Data protection' generally refers to the principles, policies and processes required to ensure that personal information is handled appropriately. 'Information security', on the other hand, generally refers to the technical measures and standards required to ensure that information is kept secure.

Information security is becoming more and more topical in the UAE, with the federal government, and local governments and government entities, having recently released laws and policies aimed at ensuring that information security measures are implemented within their respective organisations. While data protection and the confidentiality of patient information is often at the forefront of the minds of healthcare providers setting up in the UAE, compliance with applicable information security requirements should not be overlooked.

Healthcare providers in the UAE, and international healthcare providers wishing to move into the UAE market, would be well-advised to familiarize themselves with the relevant data protection and information security landscape.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on data protection and information security matters, including in a healthcare context. For further information about these matters, please contact Nick O'Connell - n.oconnell@tamimi.com