Disclaimer: This legal update describes the law in general terms. It is not intended to provide legal advice on specific situations and should not be relied upon as a source of legal advice.

Date produced: 27/10/16

qLegal Legal Update
Data and health – A legal update on e-health

INTRODUCTION:

Gunther Eysenbach, a top researcher on e-health issues, defines e-health as 'an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology.'

According to World Health Organization, 'e-health is the transfer of health resources and health care by electronic means. It encompasses three main areas: 1) the delivery of health information, for health professionals and health consumers, through the Internet and telecommunications; 2) using the power of IT and e-commerce to improve public health services, e.g. through the education and training of health workers; 3) use of e-commerce and e-business practices in health systems management.

From these two definitions it is clear that the main aim of e-health is to improve health care on a domestic and international level by using information and communication technologies.

The update will specifically discuss electronic health records in the context of Data Protection and on the use of the cloud in electronic health records.

AT THE EUROPEAN LEVEL:

At the European level, Directive 95/46/EC sets out the rights of patients in relation to electronic health records and the right of the patients to access, erase and modify their data.

Article 12(a) of the Directive states that patients have the right to access to their data that has been processed as well as to the purpose of the processing of data and the identity of the recipients or categories of recipient of the data. Article 12(b) sets out that patients also have the right to erase and correct data which does not comply with the provisions of the Directive, in particular if it is incomplete or inaccurate. However, the Directive provides only for the basis required for the protection of those rights and it is for the Member states to decide what measures should be put in place.

A study conducted by the EU Health Programme (July 2014) reported that all countries provide for patients to be able to access their electronic health records. Only 13 countries provide for the right to erase/modify data, although in most countries the patients cannot do so themselves, Austria is the only country where patients can. Also, in all but three countries, it is limited to the data put in by the patients themselves. Also, only 14 Member States allow for full access, whereas other Member States implemented Article 13, which limits those rights in some cases.

THE UK POSITION:

In the UK the Directive 95/46/EC was implemented through the Data Protection Act 1998. Under *Section 7* of the Act, patients have the right to access their Electronic Health Records, however records can be withheld in cases where it might cause serious harm to the physical or mental health of the patient (or other persons). British Medical Association Ethics released guidance on access to health records, which may be helpful to practitioners and patients.

A court may order for records that are incorrect, to be modified or erased, this cannot be undertaken by patients.

THE USE OF THE CLOUD IN E-HEALTH RECORDS:

The focus of a well-functioning health system should be a patient's health and well-being. As e-health progresses, health records should, in theory, be accessible to patients whether it be for information or for an emergency..

To achieve this, practical means of storing e-records is required.. Cloud platforms provide this accessibility as they simplify the storage and transfer of electronic medical records. Cloud storage means that patients would need to access one interface for their complete medical history, instead of having to make applications to access their data through different health organisations and departments

However, as would be expected, there are complex legal issues arising from cloud storage, particularly security and data protection issues. Health data is confidential sensitive information between doctors and patients and therefore, risk of disclosure of sensitive data is a risk stake. As with any kind of data security cloud computing, there are also several cloud-specific security risks such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures.

A wide range of cloud-computing services, such as `CareCloud` and `Medscribbler` have been offering Software as a Service arranging, among other things, the submission of patient's data and even solutions for doctor-patient virtual interaction. The European Commission stresses that a cloud provider has full responsibility for the processing of data, as it may also act as a data controller, and must fulfil all legal obligations that are stipulated under applicable national laws, such as confidentiality, through for example, encryption of data.

It is also important to also mention the recent Safe Harbor ruling in the context of electronic health data. The Safe Harbor decision saw the European Court of Justice strike down a 15-year-old data transfer agreement between the European Union and the U.S. FAQ 14 of the Safe Harbor principles used to claim that pharmaceutical and medical device companies were allowed to provide personal data from clinical trials

conducted in the EU, to regulators in the United States for regulatory and supervision purposes. The Safe Harbor ruling now puts Cloud Service Providers in a difficult position because US companies will be required to meet the standards of data protection in the EU and each Member State's data protection laws, something that will prove to be costly and time consuming.

CONCLUSION:

The existence of EU legislation such as "Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data" that sets out a general goal all EU countries must achieve in e-health sphere; domestic laws that outline the ways of achievement of such goals; opinions of the EU Commission and WHO that reflect the general position of these bodies, but are of not binding nature, the concept of e-health has a sufficient legal standing for its development. However, legal, financial, administrative and technical barriers slow down this process. As an example, in the `Overview of the national laws on electronic health records in the EU Member States, National Report for Poland` is stated that it will take at least 4 years for Poland to cope with the majority of these issues and to adopt electronic health records.

Cloud platforms and mobile health too can provide uniformity for patients' medical history, making it convenient for patients to access their complete medical history. However, due to the reluctance of governments and companies to apply cloud platforms directly to public health electronic records and the recent European Court of Justice ruling in relation to Safe Harbor Framework the process of implementing cloud services can be slow.

The desire to facilitate visibility, coherence and effectiveness in medical treatment from patients and health providers will no doubt accelerate the development for e-health and current European Union law and domestic legislation provide a sufficient basis for its development. However, it should be taken into account that despite the EU desire to promote e-health and enhance cooperation between states, due to financial, political, safety issues coupled with the principle of state sovereignty and independence, it is not easy to achieve.

This legal update was drafted by students from the Centre for Commercial Law Studies, Queen Mary University of London: ANASTASIOS KAREKLAS, ALEXANDRA VLADIMIROVA *and* YURIY MELNYK ©