PROTECTING PATIENTS' MEDICAL RECORDS UNDER THE GDPR

IAN DEGUARA

The rapid progress in technology and in the field of electronic data processing has radicalised the conventional handling of personal data, leading to increasing risks and vulnerabilities. It is an unchallenged fact that such risks may have a significant effect on the fundamental rights and freedoms of data subjects. The online environment is exposing personal data to security breaches, hacking and other unlawful forms of processing, regretfully to the detriment of the individuals' privacy rights. The recent Facebook scandal involving the sharing of users' personal data with Cambridge Analytica speaks for itself!

The need for a major reform in the European data protection framework, led the European Commission, in January 2012, to publish a proposal for the General Data Protection Regulation (GDPR). The GDPR is one of the most wide-ranging pieces of legislation adopted by the EU in recent years. It aims to establish accountability, consistency and harmonization across the EU, rebalance rights in the digital world and provide legal certainty for economic operators. Harmonization was a key element in the decision taken by the Commission in the choice of the legal instrument. In fact, a regulation was chosen as the most appropriate instrument to be adopted for the GDPR due to its binding effect and direct applicability in all Member States.

After a long negotiation process at European level, the GDPR came into force on 25 May 2016. It provided for a transitional period of two years for data controllers to familiarise themselves with the new provisions and align the processing operations involving personal data with the new rules. The GDPR will therefore start to apply on 25 May 2018 and will replace the twenty-year-old Directive 95/46/EC.

The GDPR will not bring about a revolution in the way personal data are processed, but it is an evolution of the current legal framework. If one had to compare the principles and legal criteria of the current Directive against those set out under the GDPR, the conclusion is that the same principles and criteria have indeed withstood the test of time and have not changed. Having said this, the GDPR provides for stronger rules on data protection, which effectively mean that data subjects will have more control over their personal data and business operators will benefit from a level playing field.

A medical professional, operating as a self-employed, is the data controller responsible for determining the means and purposes of the patients' health records collected during the exercise of the professional duties.

As previously considered by the current Directive, medical records constitute special categories of personal data, as the processing can create significant risks to the data subject's fundamental rights and freedoms. The GDPR now expressly includes "genetic data" and "biometric data" within this category, particularly when the latter is processed 'through a specific technical means allowing the unique identification or authentication of a natural person'.

Although the rule dictates that the processing of special categories of personal data is prohibited, article 9(2) of the GDPR provides, in a closely replicated fashion to the present Directive, the grounds to process such data in the area of health and healthcare management. Therefore, the processing is legitimised if one of the following criteria applies:

- the data subject has given his explicit consent, unless reliance on consent is prohibited by EU or Member State law;
- processing is necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement;
- processing is necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent;
- processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and/of medicinal products or medical devices.

Article 9(2)(j) sets a new provision for the processing of personal data for the purposes of archiving and research and statistics, subject to appropriate safeguards. Those safeguards shall ensure that technical and organisational measures are in place to guarantee respect for the principle of data minimisation. These measures may include pseudonymisation, which provides that the

IF THE [DATA] PROCESSING CONCERNS PERSONAL DATA FROM PATIENTS OR CLIENTS BY AN INDIVIDUAL PHYSICIAN ... A DATA PROTECTION IMPACT ASSESSMENT SHOULD NOT BE MANDATORY

personal data can no longer be attributed to a specific data subject without the use of additional information and that the additional information is held separately. Additionally, further processing of personal data for scientific research purposes shall not be incompatible with the original processing purposes.

The principles of storage and purpose limitation apply to medical records too. Retention should not be longer than necessary. In the process of determining a justifiable timeframe, the applicable legal and operational requirements should be taken into consideration. Furthermore, when personal data are processed solely for scientific research it may be stored for longer periods. However, in both cases, appropriate technical and organisational safeguards have to be adopted.

Under the current law, health professionals already have the obligation to provide certain information to patients about the processing of personal data, including but not limited to, the purposes of processing, categories of recipients with whom the data may be shared and also, data subjects' rights. However, the GDPR expands the list and sets out that data controllers shall provide information on how long they will store the data, the existence of any automated-decision making and the right to lodge a complaint with the supervisory authority. Although there may be other acceptable approaches to fulfil this obligation, the preferred practice should be for health professionals to develop a privacy policy and make it accessible to their patients.

As from 25 May 2018, data controllers will be obliged to carry out a data protection impact assessment (DPIA) where processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA involves an assessment of the probability and severity of the risks involved in the proposed data processing as well as the measures and safeguards to be introduced to mitigate such risks. Having said this, it is relevant to make reference to recital 91 of the GDPR which specifically provides that "*the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory*".

The GDPR also introduces an obligation on data controllers to report breaches of patients' health records to the data protection authority within 72 hours from becoming aware of the incident. A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. If the breach is likely to result in a high risk to patients, for instance, the compromised

THE MAXIMUM ADMINISTRATIVE FINE CONTEMPLATED BY THE GDPR IS OF 20 MILLION EURO OR 4% OF A COMPANY'S GLOBAL ANNUAL TURNOVER IN CASE OF AN INFRINGEMENT

electronic health records were not encrypted and no measures could be taken to reduce the risk, the health professional would be required to notify all the affected individuals.

With the GDPR, data subjects have new rights, such as the right to data portability. This means that where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to request the transmission of those personal data which are retained by an automated processing system (no paper records).

Existing rights have been strengthened, in particular, the right to erasure and the right of access. Exercising a right of access entitles patients to request copies of their medical records. When acceding to such right, the health care professional must ensure that any information identifying third parties is redacted or blanked out; most importantly, health care professionals must always be guided by their primary responsibility to act in the best interests of their patients.

Whether health data are collected, stored or accessed via wearable devices, mobile applications, cloud computing capabilities or databases, security of health records must be placed at the top of the priority list, since any misuse may have irreversible consequences for the data subject. Both the controller and the processor share the responsibility to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such measures may include encryption, pseudonymisation, and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. Physical security must not be overlooked since it plays an equally important role in the security chain.

It is pertinent to note that the maximum administrative fine contemplated by the GDPR is of 20 million Euro or 4% of a company's global annual turnover in case of an infringement. This might very well be a reason why the GDPR has become the talk of the town over the past months.

A final take-away message is that, if you are not able to protect, do not collect!