ENRF Briefing Note

on the new EU General Data Protection Regulation

The EU General Data Protection Regulation (EU) 2016/679 (GDPR) has been adopted in 2016 and will become applicable in the Member States from 25 May 2018. The GDPR replaces the Data Protection Directive 95/46/EC, and it comes as an evolution of 20 years of EU regulation on data protection. It has been designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to respond to the new privacy issues and possible data breaches related to an increasingly data-driven world.

The biggest change of the new legislation concerns the extended jurisdiction of the GDPR, as it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller (health professional) or processor (cloud-service provider) not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. The new provisions included in the GDPR will have important consequences on the nursing profession and health research.

The GDPR imposes a higher standard of protection for the processing of health data that aims at protecting the fundamental rights and privacy of patients (data subjects), but this target can also result in a higher burden on the healthcare professionals (data controllers) who will have to comply with it. In particular, some of the new data subject rights have a significant impact on the health sector:

- Right to access is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Therefore, when processing health data, the healthcare professional needs to inform the patient about the specific purpose for which information about his/her health is collected or used, and the patient must be allowed to exercise his/her rights to access or change/update this information free of charge. For instance, a patient is entitled to a free copy of his/her medical records containing information such as diagnosis and test results. In addition, a patient has the right to obtain from his/her health service provider the correction of any inaccurate information about his/her health, and, in certain cases, he/she also has the right to object to the processing or use of his/her health data and even the right to have some data about his/her health situation removed from the file.

- Breach notification, that will become mandatory in all Member States, implies that data controllers have the obligation to secure health data that are under their control and to notify the authorities of any data breaches. This means that every independent healthcare professional or health service provider must take the appropriate security measures to make sure his/her patients' health data are kept secure. This can be done by securing personal computers with private logins and passwords and by installing firewall updates and antivirus software. If the device onto which patients' records are saved is stolen or is unrightfully accessed online, the GDPR obliges the healthcare professional to notify the data breach to the competent Data Protection Authorities within 72 hours from when becoming aware of it. Regarding the procedure of keeping health records of patients on servers connected to the internet or in the "cloud", healthcare professionals should be aware of data breaches that are likely to occur. However, in such cases, it is not only the health professional but also the cloud-service provider who will have direct legal obligations and responsibilities under the GDPR, including the security and breach-notification obligations.

- Right to be forgotten, it is a right that entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. This right is linked to the strengthened conditions for consent that require that the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. In addition, Article 7.1 establishes that controllers shall be able to demonstrate that the data subject has consented to processing of his personal data. These requirements will be particularly important for health research because, as prescribed by Article 5(1)(b), personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Therefore, specific health data collected for a given research purpose cannot be used for others, unless further consent is given. Namely, the GDPR prescribes that if personal data are processed for scientific research, appropriate safeguards should be enacted to guarantee that technical and organisational measures are in place to ensure respect for the principle of data minimisation (use as less as possible identified data). If the research purpose does not imply the identification of the data subject, such measures are not necessary, as the GDPR does not apply to anonymised data but only to personal data. However, the process of anonymising does not represent a lasting solution, due to the constant technology progress.

Conclusion

Given the amount of new provisions proposed compared to the previous directive, two years transition have been planned to give time to align the requirements to other legislative instruments, and to have dialogue with national authorities in order to foster a common understanding on key concept of GDPR.

To this purpose, some stakeholders are already working to prepare codes of conduct to serve as compliance tools for data controllers and processors, following the principles established by the GDPR Articles. In this sense, it is important to exploring cross-sectoral codes as health data is a multiple user environment.

In addition, the European Commission – that will approve the Code - has indicated the importance of "representativeness" of codes: ideally all people represented should be involved in the process.

However, as several fields will be strongly affected by the GDPR provisions, many stakeholders feel that some clarification is still needed to achieve a full compliance. The most sensitive issue concerns the consent rules and the consequences on research: the limit of consent for specified purposes will pose threats to a smooth development of research.

Therefore, there is a need to interpret the GDPR in a flexible way and adopt an open interpretation in the re-use of data, together with more guidance on the safeguards that are to be applied and the accountability mechanisms.

ENRF Briefing Note – 6 November 2017

European Nursing Research Foundation (ENRF)
Registration Number: 0533.978.961
Clos du Parnasse 11B, 1050 Brussels, Belgium
Tel: +32 2 511 34 84 - Fax: +32 2 512 35 50
Email: enrf@enrf.eu