HealthManagement
Promoting Management and Leadership

Are you ready? What will the GDPR mean for healthcare leaders?

Stewart Duffy
******@***rlb-law.com

Partner, - Healthcare Team,
RadcliffesLeBrasseur,
London, UK

The European Union's (EU) General Data Protection Regulation (GDPR) will take effect on May 25, 2018, replacing the 1995 Data Protection Directive. Directly binding and applicable in all EU states, the GDPR aims to protect the data and privacy of the European population by giving control back to citizens and to make the regulatory environment simpler for international business. Non-compliance comes at a high price; fines for failure to comply could be as high as €20 million or 4 percent of global turnover. Starting with legal implications, HealthManagement.org spoke to experts on how healthcare can prepare for the GDPR and how the regulation will impact on the sector.

GDPR and legalities

Organisations with mature information governance systems will find it relatively easy to adapt to the changes that the GDPR introduces. However, many smaller organisations will find the transition more challenging, especially where they have previously invested little time or resources in data protection issues. The
enhanced transparency requirements in the GDPR, which include the obligation to specify the lawful grounds relied upon for processing in privacy notices, will require organisations to apply their minds to these issues at the outset rather than relying on post hoc justifications when problems or challenges arise.

Organisations which are used to relying on consent for treatment interventions may struggle to come to grips with the challenges posed by consent as a lawful grounds for processing, particularly the doubt expressed by the Article 29 Working Party about the possibility of consent being freely given, and thus valid, in the context of healthcare provider/patient relationships. Organisations will need to consider the full range of lawful grounds that are available and choose the most appropriate for the processing at issue bearing in mind the heightened requirements which the GDPR applied to consent.

Compliance is a process and it is not too late for organisations to take action. It is important to prioritise. Many organisations processing health data will be required to appoint a Data Protection Officer (DPO) and organisations which have not considered this issue yet will need to address it without further delay. For many organisations the challenge will be to determine whether they are undertaking processing on a 'large scale'. In many cases the correct answer will not be obvious as the examples given in relevant guidance cover only the extreme ends of the spectrum. Organisations which determine that they are not required to appoint a DPO should keep a clear record of their reasoning in case this is called into question.

Organisations also need to map the processing of personal data which they perform and consider the various processing activities in order to determine the lawful basis on which they are relying for that processing. They will need to bear in mind that the lawful grounds relied upon will influence the scope of the data subjects' rights. That mapping exercise will also enable organisations to review their processing activities against the full range of fair processing principles in Article 5 GDPR, and to identify potential changes which better serve those principles. An informed understanding of the organisation's processing activities underpins the preparation of appropriate privacy notices and the application of appropriate organisational and technical security measures.
Organisations will also need to review their internal policies and procedures to ensure that these reflect the revised arrangements, including those for subject access requests. Breach response plans will need to be updated to reflect the requirement mandatory reporting of breaches where the reporting threshold is met.

The data mapping exercise will also assist organisations in identifying third parties that undertake processing on their behalf. Organisations will need to review their contractual arrangements with processors to ensure that they reflect the requirements in Article 28 GDPR.

Healthcare organisations will need to be mindful that much of the personal data which they process will be special category personal data which attracts enhanced protections. Processing of such data is prohibited unless the processing is necessary for one of purposes identified in the list of exemptions in Article 9(2), which includes the health and social care exemption. Where such an exemption applies the processing will also need to meet one of the lawful grounds in Article 6. Whilst those requirements are necessary for lawful processing, organisations must be mindful that they are not sufficient. Compliance with the fair processing principles in Article 5 is required for all processing. Whilst most organisations operating in the health sector undertake
processing with good intentions that must not blind them to the possibility that well-intentioned processing may still breach the Article 5

principles.

Organisations will need to be able to demonstrate their compliance with these principles through appropriate policies and procedures, developed to reflect the particular context in which they operate, and supported by appropriate staff awareness and training. Organisations must continue to address external threats, such as malware and hacking, whilst not forgetting the potential for internal threats, such as rogue employees accessing health data inappropriately.

Published on : Fri, 25 May 2018