HealthManagement.org
The Journal
LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES
VOLUME 18 • ISSUE 3 • 2018 • € 22
ISSN = 1377-7629

Emerging Markets

General Data Protection Regulation and healthcare

What could the new data protection law mean for health sector leaders?

The European Union's (EU) General Data Protection Regulation (GDPR) will take effect on 25 May 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. GDPR was implemented in April 2016 and will be enforced in all EU member states by the end of May 2018. 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. *HealthManagement* spoke to experts in the fields of law, cybersecurity, the patient space and crisis management on how healthcare can prepare for the GDPR and how the regulation will impact on the sector.

Cybersecurity

James Mucklow
Healthcare Expert, PA Consulting Group, London, UK

Healthcare organisations are used to handling sensitive data, but the new EU GDPR introduces fines of up to four percent of revenue or £17m, whichever is the greater, for not meeting the regulations will bring a number of challenges.

Healthcare organisations are responsible for the appropriate management of all personal data storage and processing in both their own organisation and that of their suppliers, who are now jointly liable for any personal data breach. The GDPR leaves the level of appropriate controls up to the organisation to put in place, based upon the level of sensitive personal data held. However, should you encounter a breach, you will need to show that you properly considered the risks and mitigated them through the appropriate controls. For example, does your supply chain meet standards such as the Information Governance Toolkit, ISO27001 and Cyber Essentials Plus?

You must be clear on the legal legitimate basis for holding the data; is it based on legislation or consent? Ideally you should try to focus on holding data on the legal legitimate basis before resorting to the need for consent. If consent is required, you need to make sure

that subjects opt in to you holding and processing their personal data and that you provide them with the ability to opt out at any point. This assumes that you do not have a legal or statutory obligation to retain their personal data.

You can no longer offload the responsibility. A particular area of concern is when data is shared beyond the organisation and/or used beyond direct care. The GDPR says you are jointly liable for any personal data breach. As well as fines from the regulators, you could be subject to civil claims for damages. In addition, the regulators also have the option to suspend your ability to process personal data.

Cybersecurity

Elliot Rose

Digital Trust and Cybersecurity Expert and Member of Management Group, PA Consulting Group, London, UK

The more widely data is shared appropriately, the more valuable it is in the support of patient care. The challenge is, do you have a clear rationale for sharing data or accessing shared data?

The EU GDPR should be seen as an opportunity to review how you handle data and ensure that you have clarity on the processing, storage and sharing of it. The key to doing this is having a systematic approach. You need clear identification of data assets and the governance you have to date. You should have the operational rationale for holding data now and in the future and how it can be enhanced with the right personal data captured. For example, does sharing data promote safer care? Finally, you need a clear view of the basis on which data is processed to enable this.

Ensure you have a plan to be compliant by the end of May. Know what the regulators will be expecting and conduct scenarios to ensure that your plan is realistic and robust. Remediate your risks. Create your inventory analysis, conduct data protection impact assessments and address those areas where you need to take action. Make sure you cover process, people and technology changes that may be required, as well as staff awareness training. Do not forget to conduct the due diligence and changes that will be required across your third parties. Put in place the operating model you will need after May 25. Make sure you have an operating model—and associated tools—which will help you shape all of the things you will need to put in place in order to remain compliant with the GDPR in the most efficient manner.

Cybersecurity

Richard Corbridge

Chief Digital Information Officer, Leeds Teaching Hospital NHS Trust, Leeds, UK

The impact of the General Data Protection Regulation in the public health sector has many different and diverse consequences. The National Health Service (NHS) in the UK is prepared for GDPR perhaps better than many due to the focus brought by elements like the Information Governance tool kit and with the work that NHS Digital and NHS England have done to promote good governance around data over the last decade.

GDPR in many ways gives the health system a more solid basis on which to build governance around data; it certainly provides the organisation-based and much-maligned Information Governance teams with a new platform to promote the need for a renewed focus on data governance. The GDPR also pushes the governance of NHS organisations to discuss the data risks they have at the most senior level and build corporate-level plans with real engagement in actions that need to be undertaken.

The classification of what makes up health data and identification have been added to by GDPR. Again this is useful for health systems as it enables standardised approaches to be created and enables the transferral of information to be controlled in a way that guarantees standardised approaches to data handling.

Privacy Impact Assessments (PIAs) have become common parlance across the health sector over the last three years. GDPR and the system's reaction to these also now place the delivery of PIAs in the public domain increasing transparency and ownership clarity of information risk.

Limiting the security risk and therefore complying with elements of GDPR have now been clarified from a board responsibility in each health organisation throughout the public health system. The 'teeth' of the Data Protection Act have given this a renewed push and the positioning of the Data Protection Officer (DPO) in each organisation has given boards a focal point to rally around.

Legalities

Stewart Duffy
Partner, Healthcare Team, RadcliffesLeBrasseur, London, UK

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 applies 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 for 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.

Patients

Peter Kapitein

Patient advocate, Inspire2Live, The Netherlands

The General Data Protection Regulation (GDPR) does exactly what it says: it protects data. The consequence of this is that the data is much harder to use for the benefit of society and our case for patients.

There is a big difference between citizens and patients. Where citizens might want to protect their data more intensely, patients want it to be used for the benefit of society and if possible for their own. Patients want the data being used by researchers for better treatments and the improvement of quality of life. Most patients don't even want to give permission for it. It's more a matter of "Simply use my data and hurry up".

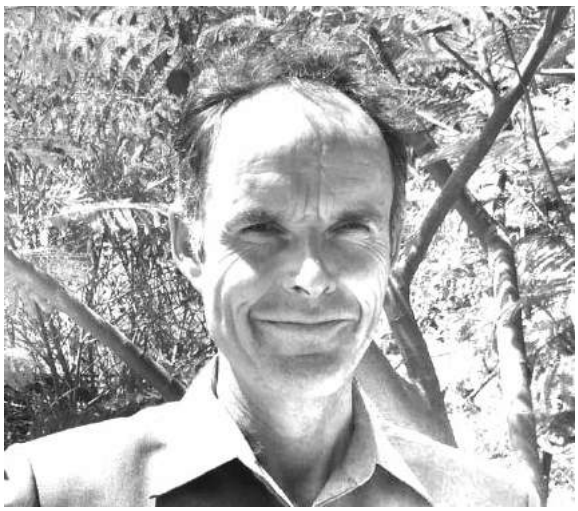
What is seriously lacking in the implementation of GDPR is the comparison of the costs-benefits-risks of the existing situation (without GDPR) where data can be used more easily and the cost-benefit-risk ratio in the new situation (with GDPR). We patients take the risk and pay the bill—with our lives. Therefore, it is simply wrong that politicians and lawyers determine what can and should be done with 'my data'. It is my self-determination that should answer the question about what can be done with my data.

For this reason of self-determination, I refer to an excellent Estonia EU initiative called 'Digital Health Society' and their working group 'Citizen-controlled data governance and data donors' that says: "The patient owns and maintains the data and the data is available for research with an opt out way of working".

Risk and accountability

John Deverell

CEO, Deverell Associates, UK



GDPR will apply to companies processing personal data in the EU, companies offering goods or services to EU residents and companies that monitor the behaviour of EU residents. It is not dependent on the location of the business in question. As a result, people should feel more confident that their personal data is secure. GDPR stipulates that the data 'controller' (senior management of the firm) and the data 'processor' (the department or employee working with the data) have equal accountability. It specifies an "accountability principle". This means that senior managers are required to demonstrate compliance with GDPR and to state their responsibilities for doing so. GDPR outlines seven obligatory requirements for the purpose of safeguarding the security interests of EU citizens; consent, breach notification, right to access, right to be forgotten, data portability, privacy by design and data protection officers. The GDPR continues the trend of the last few years in making senior managers specifically accountable. Gone are the days when managers could legitimately defend themselves by simply and plausibly claiming that they were ignorant of their employees' wrongdoings. Senior managers are now specifically accountable for putting in place the procedures, resources and training to reduce the likelihood of a widening range of adverse events – and for demonstrating that they have done so. While this requires more effort and probably more expenditure on their part, it will – assuming that managers fulfil their responsibilities – increase public and shareholder confidence in business and in the intention to handle risk more effectively. ■