

## GDPR: Risk and accountability



**[John Deverell CBE](#)**

\*\*\*\*\*@\*\*\*deverellassociates.com

Deverell Associates – The  
Prepared Mind, UK

[LinkedIn](#)

---

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

The European Union's (EU) General Data Protection Regulation (GDPR) took 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. 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 crisis and risk management expert John Deverell on how healthcare can prepare for the GDPR and how the regulation will impact on the sector.

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.

Published on : Wed, 20 Jun 2018