HealthManagement.org
Promoting Management and Leadership

Are you ready? What will the GDPR mean for cybersecurity?

James Mucklow
******@***paconsulting.com

Digital healthcare expert - PA Consulting Group London, UK

LinkedIn Twitter

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 cybersecurity, HealthManagement.org spoke to experts on how healthcare can prepare for the GDPR and how the regulation will impact on the sector.

GDPR and Cybersecurity

Healthcare organisations are used to handling sensitive data, but the new EU GDPR introduce 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, IS027001 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.

Published on : Fri, 18 May 2018