HealthManagement
Promoting Management and Leadership

GDPR and healthcare cybersecurity: are you prepared?

Rich Corbridge
Editorial Board Member
HealthManagement
******@***richardcorbridge.com

Ex-Chief Digital and Information
Officer - Leeds Teaching Hospitals
NHS Trust, 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.

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 muchmaligned 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 corporatelevel 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.

Published on : Mon, 4 Jun 2018