H1 2017 GLOBAL HEALTHCARE DATA BREACHES

Industry with the highest number of data breaches

228 data breaches

31 million stolen records

*Figures taken from Gemalto's Breach Level Index H1 2017

The Information Commissioner's Office (ICO) reported an 11% increase in reported data breaches in healthcare organisations in Q1 2017.

The most recent fine issued by the ICO to a single healthcare organisation was £200,000 to HCA International Ltd for failing to keep fertility patients' personal information secure, in contravention of the Data Protection Act (DPA).

2017 INCIDENTS	
WannaCry ransomware	**NotPetya ransomware**
May 2017	June 2017
Estimated 300,000 victim machines	**Estimated 20,000 victim machines**
The attack is reported to have led to the cancellation of 14,778 patient appointments and 850 operations across the NHS	For pharma giant Merck, the attack disrupted the distribution of vaccines and prescription medication worldwide

TIMELINE FOR COMPLIANCE

A number of changes will come into effect throughout 2018 regarding the responsibilities and obligations facing organisations that process or manage personal and sensitive data. Pre-emptive action can reduce the impact of these changes, helping to protect organisations from the operational disruption, reputational damage and financial penalty associated with a data breach.

April 2018 Release

From April 2018, the Information Governance Toolkit (IG Toolkit) will be replaced with the **Data Security and Protection (DSP) Toolkit** as the assurance framework for all health and social care organisations.

The Department of Health (DoH), in conjunction with NHS England, has released guidance on these upcoming changes in the 2017/18 Data Security and Protection Requirements.

May 2018 GDPR

The **General Data Protection Regulation (GDPR)** extends the data protection rights of individuals, and requires organisations to adopt appropriate technical and organisational measures to protect personal data. The Regulation also places stronger controls on the processing of health data.

Penalties for non-compliance are due to increase under the GDPR, with the maximum fine for non-compliance set at €20 million or 4% of the organisation's annual global turnover – whichever is higher.

May 2018 NIS Directive

The **Directive on Security of Network and Information Systems (NIS Directive)** aims to achieve a high common level of network and information systems security across the EU.

The NIS Directive applies to operators of essential services (OESs) in critical national infrastructure (CNI) and digital service providers (DSPs). The NHS is confirmed as one of the OESs to which the NIS Directive applies.

PLAN NOW TO MINIMISE YOUR CYBER RISK AND TO ENSURE COMPLIANCE BEFORE THE DEADLINE

IT Governance Ltd

Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park, Ely,
Cambs. CB7 4EA. United Kingdom.

t: +44 (0)333 800 7000
e: servicecentre@itgovernance.co.uk
w: www.itgovernance.co.uk

/ITGovernanceLtd /ITGovernanceLtd /ITGovernanceLtd