Data Protection: Implications and challenges

The vulnerability of data protection is clearly evidenced through costly data leakage incidents such as the recent loss of 25 million Child Benefit records by HM Revenue & Customs. Security breaches make headline news and highlight the need for organisations and individuals to ensure that all information is accessed and stored securely. However, this is a digital age of ever growing collections of information which is kept on computers, laptops and USB sticks, making security an increasing risk.

As the capabilities of information technology (IT) grow, individuals are in danger of underestimating the scope of IT security threats. When protecting our data it sad fact many of us are bad at choosing adequate passwords, 1 in 4 of us it is already known choose passwords on factors of ego, nicknames or personal family names, including pets. It is little wonder that a hacker, using a Pentium 100 PC, can guess a 6 character password of upper and lower case letters in just over 27 hours, hitting 200,000 different combinations every second. Anyone that handles data has a responsibility to act in accordance with the Data Protection Act 1998, however, it is not the panacea that safeguards the rights and protection of everyone, particularly patients.

The interpretation of this Act and how it affects individuals particularly in terms of research purposes can be fraught with confusion and uncertainty. The act for example has eight key principles the first of which states that personal data “shall be processed fairly and lawfully” and only for the purpose it was intended for, you can not simply collect data speculatively. The definition of “fairly” may be subject to different interpretations. Notions of what is, or may not be “fair”, only very recently stimulated contentious debate in the news following on from Mr George Osborne’s budget! Exemptions to the Act can also appear contradictory as data can be processed for a different purpose to that which it was collected for and kept indefinitely if “that data are not processed in such a way that substantial damage or substantial distress, is, or is likely to be, caused to any data subject”.

Dr Hilary Paniagua, Editor
Matters of anonymisation and access to patient’s records for research purposes subsequently need more uniformity of practice and policy guidance. Variations in the thinking of Trusts and research ethic committees for example, can lead to delays in research and idiosyncratic requirements. Anonymised data is not regulated by the Act as long as it has not been taken in a reversible way. However, difference of interpretation can arise as some may take the view that any personal data that has been encoded continues to be personal data in terms of the Data Protection Act as long as the key for that decoding remains evident.

Given the Act’s reputation of controversy, while its principles may protect privacy there is often the need for greater awareness of its legal framework. The penalties for non-compliance with the Act make it more important than ever that individuals and particularly researchers, have effective data collection protection policies and practices in place and take its ramifications very seriously.