Data Protection in the EU

Patrick Duxbury, Partner, Wragge & Co LLP
State Capital Meeting, San Francisco, 6-7 October 2013

Wragge&Co

Current Law

- Data Protection Directive 95/46/EC
- Implemented into UK law by the Data Protection Act 1998
- Applies to anyone who "processes" (basically does anything) "personal data"
- Personal data = information from which living individuals can be identified e.g. names and contact details
- Only applies if you are a "data controller" = the person/entity who determines the purpose for which and manner in which personal data is processed
- Two fundamental requirements:
  - have to have a notification within Information Commissioner's Office (in the UK) or equivalent
  - comply with the 8 Data Protection Principles

Eight Data Protection Principles

1. Data must be processed fairly and lawfully. If 'sensitive personal data' (which is specifically defined in the DPA and includes e.g. medical data, data about race or religion etc) being processed, this is likely to require consent.
2. Data must be obtained for one or more specified and lawful purposes and may not be further processed in any manner incompatible with those purposes
3. Data shall be adequate, relevant and not excessive in relation to the purposes for which the data is processed
4. Data shall be accurate and kept up to date
5. Data shall not be kept for longer than is necessary
6. Data shall be processed in accordance with the rights of the data subjects under the Act (ie such as right to access and correct their personal data)
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of data as well as against accidental loss destruction or damage to such data
8. Data shall not be transferred outside the European Economic Area unless the recipient provides an adequate level of protection in line with the EU Data Protection Directive.

Consequences of breaching DPA in the UK

- Breach of notification obligation can be a criminal offence
- Criminal offence to knowingly or recklessly disclose personal data without the consent of the data controller
- ICO can issue enforcement notices
- ICO has right to audit public bodies
- Directors can be personally liable
- Fines of up to £500,000
- Similar provisions exist in the rest of the EU

Some of the big issues

- Breach of security a big issue
- Lots of NHS trusts in the UK have been fined e.g.
  - 12 July 2013 NHS Surrey fined £200,000 after sensitive personal data found on hard drives sold on an auction site
  - 15 February 2013 Nursing and Midwifery Council fined £150,000 after losing three DVDs relating to a nurse's misconduct hearing
- Similar story throughout Europe
- Obligations don't apply (currently) to data processors e.g. IT outsourcing companies – hence contracts have to include clear contractual responsibilities to comply
- Transfers of personal data outside the EEA a big issue
  - Either require consent of data subject or
  - EC approved arrangement for transfer outside the EEA has to be put in place
  - Model form contracts for this purpose
  - Transfer to a non-EEA based server or access by e.g. US headquarters to EEA based data = a transfer

Some particular points in the health sector:

- Organisations have to work out if they are data "controllers" or "processors" e.g. if you are a company providing a connected health service collecting data from patients you might just be a "repository" and not a controller
- Processing of "sensitive" personal data (includes health info) has additional obligations attached to it including generally a requirement to get explicit consent
- Access to patient data for research purposes therefore an issue
- Clinical trials have to be carried out in accordance with Data Protection Directive
- Individuals must give specific consent to the use of their data
- Best practice says use fully anonymised data in which case consent not required – but not practical plus is true anonymisation possible these days?
- Currently use of psuedonymised data (where possible to link back to the patient ID in a separate data base held by data controller) generally ok in the UK (but need to consider each case)
- But not clear if it works in all other EU countries. Problem is that the Directive has been implemented in different ways in different countries
- Ownership and use of data from products like the Nike Fuel Band

New Proposed Data Protection Regulation

- Likely to come into force in 2014/2015
- Direct effect (problem with current Directive is that it has been implemented in different ways in different countries)
- Penalty for non-compliance – up to 2% of global annual turnover
- will apply to processors as well as controllers
- Will apply to data controllers based outside EEA offering good/services in the EEA
- May clear up some of the issues over use of data for scientific research. Calls for psuedonymised data to be specifically exempted
- Watch this space

QUESTIONS & ANSWERS

Wragge&Co