# Legal Aspects of Pseudonymisation

Dr Mark J Taylor

*Pseudonymisation Workshop, University Of Nottingham*

*22nd September 2011*

# Disclaimer

- Please do not cite or distribute without express permission of the author: m.j.taylor@sheffield.ac.uk

- The content of this presentation is believed to be correct on 22 Sept 2011. You should be aware however that changes in the law or other guidance may affect its accuracy.

- It is intended as a general introduction to the matters under discussion. It does not constitute legal advice.

# In search of a definition..

- Pseudonymised patient data is either **'personal data'** or **'confidential information'** or it is not.

- "**personal data**" means data which relate to a living individual who can be identified—

  (a) from those data, or

  (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

  and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual [DPA 98, S.1(1)]

- "**sensitive personal data**" consists of information as to physical or mental health or condition. [DPA 98, S.2]

# In search of a definition...

- ‘patient information is “**confidential patient information**” where — (a) the identity of the individual in question is ascertainable—

(i) from that information, or

(ii) from that information and other information which is in the possession of, **or is likely to come into the possession** of, **the person processing that information**, and

(b) that information was **obtained or generated by a person** who, in the circumstances, **owed an obligation of confidence** to that individual. [NHS Act 2006, S.251(11)]

# In search of a definition....

- Therefore, data is specifically (and especially) regulated if an individual is **identifiable from those data**, or, from those data **and other information** which is in the possession of, or is **likely to come into the possession** of,

- the data controller

- the person processing the data

- or anybody else with access.

"to determine whether a person is identifiable, **account should be taken of the means likely reasonably to be used either by the controller or by any other person** to identify the said person"

[Recital 26, 95/46/EC]

# "to anyone with access using means reasonably likely to be used"

- "If it were **impossible for the recipient** of the barnardised data to identify those individuals, the information **would not constitute personal data in his hands**." (Lord Hope, CSA v SICO, para 26(B))

- **The fact that the data controller can identify a data subject from the data does not preclude the possibility that data, in the hands of others, may be removed from the requirements of the DPA 98.**

# "to anyone with access using means reasonably likely to be used"

- "**Rendering data anonymous** in such a way that the individual to whom the information from which they are derived refers is no longer identifiable would **enable the information to be released without having to apply the principles of protection**." (Lord Hope, CSA v SICO, para 25(H).)

- "shared understanding that anonymised **data which does not lead to the identification of a living individual does not constitute personal data**." (Mr Justice Cranston, *DoH* v *Information Commissioner* [2011] EWHC 1430 (Admin), para 51.)

# "to anyone with access using means reasonably likely to be used"

- "Therefore, the fact that there is **a very slight hypothetical possibility** that someone might be able to reconstruct the data in such a way that the data subject is identified **is not sufficient** to make the individual identifiable for the purposes of the Directive.

- "The starting point might be to look at **what means are available** to identify an individual **and the extent to which such means are readily available**.

- "When considering identifiability it should be assumed that you are **not looking just at the means reasonably likely to be used by the ordinary man in the street**, but also the means that are likely to be used by a determined person with a particular reason to want to identify individuals. Examples would include investigative journalists, estranged partners, stalkers, or industrial spies."

(Technical Guidance Note on Determining What is Personal Data, ICO, p.7)

# "to anyone with access using means reasonably likely to be used"

- "the issue before the Tribunal was **one of assessment: the likelihood that a living individual could be identified from the statistics**. That was in my judgment **only partly a question of statistical expertise**, as regards matters such as the sensitivity of the data. **Partly, also, it was a matter of assessing a range of every day factors, such as the likelihood that particular groups, such as campaigners, and the press, will seek out information of identity and the types of other information, already in the public domain, which could inform the search**. These are factors which the Tribunal was in as good a position to evaluate as the statistical experts, a point which one of the Department of Health's experts conceded." (Mr Justice Cranston, *DoH* v *Information Commissioner* [2011] EWHC 1430 (Admin), para 82)

- **"A person who puts in place appropriate technical, organisational and legal measures to prevent individuals being identifiable from the data held may prevent such data falling within the scope of the Directive."** (Technical Guidance Note on Determining What is Personal Data, ICO, p.7)

# Relevance of identifiability to a Human Rights Argument?

- **Personal vs Private Dichotomy?**

- **Can the disclosure of anonymised personal information constitute a breach of Article 8 (right to a private and family life)?**

- "Some judicial statements before the Human Rights Act in the case of *R v Department of Health ex parte Source Informatics* suggested that the disclosure of personal information would not constitute an infringement of personal privacy where this was anonymised. However, it can be argued that anonymisation may not necessarily constitute sufficient protection for privacy interests." (JV McHale, J Jones, *Privacy, confidentiality and abortion statistics: a question of public interest?* J Med Ethics [pub online 27 June 2011])

- "In my view, the Tribunal was not flawed in concluding that the risk of individual identification is so remote that the right under Article 8.1 was not engaged." Mr Justice Cranston, *DoH* v *Information Commissioner* [2011] EWHC 1430 (Admin), para.82

# 7th DPP: Information Security

- **"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."**
- You must have appropriate security to prevent personal data being accidentally or deliberately compromised.
- "In particular, you will need to:
  - design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
  - be clear about who in your organisation is responsible for ensuring information security;
  - make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
  - be ready to respond to any breach of security swiftly and effectively." (ico.gov.uk)

# Summary

- Either P.D. or not P.D : no special category of pseudonymised data `as such'
- Key questions:
  - 'Who has access'? (Reasonably anticipatable rather than necessarily intended!)
  - 'What methods of (jigsaw / mosaic) identification are reasonably likely to be used'?
- Identification is probably crucial even to a human rights argument.
- Pseudonymisation may constitute an appropriate technical measure to protect against unlawful or unauthorised processing even if it does not remove data from scope of DPA 98.