A Blueprint for Health Records Research in Scotland

APPENDIX 6

FUNCTIONS, ROLES AND RESPONSIBILITIES OF DATA CONTROLLERS

Background

The UK Data Protection Act 1998 (DPA) came into force on 1 March 2000 and is the UK enactment of the European Data Protection Directive 95/46/EC.

At present the UK Government is gathering evidence on Data Protection practice and experience under the DPA in anticipation of negotiations for a new Data Protection Directive in 2011.

In the meantime all UK individuals and organisations must ensure that their use and disclosure of personal data complies with the requirements of the DPA.

Key Concepts

Identifying the Data Controller

The DPA confers the responsibility and liability for compliance with the requirements of the DPA on the Data Controller. Identifying the Data Controller(s) in relation to a set of personal data and its processing operations is therefore key to ensuring that data protection obligations are known and adhered to. It is sometimes challenging to identify the Data Controller where a number of actors and processing operations are involved.

The opinion of the Article 29 Data Protection Working Party[1] published in 2010[2] recognised the challenge in this area. The Working Party made some unambiguous observations:

In identifying a Data Controller, identifying who sets the purposes of the processing is the paramount consideration;
The actors involved must have the legal and factual capacity to fulfil their role i.e. a Data Controller is not a Data Controller unless in facts and law they have the capacity to set the purposes for the processing of the personal data;
A pluralistic situation, with a number of Data Controllers, including with different degrees of responsibility and liability, is both possible and acceptable.

[1] The Article 29 Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy.

[2] Opinion 1/2010 on the concepts of 'controller' and 'processor' , 00264/10/EN, WP 169, adopted 16 February 2010

A Blueprint for Health Records Research in Scotland

Key messages:

It is essential to be clear as to who is acting as a data controller with respect to any given data set which involves the processing of personal data
It is possible that one or more parties can act in the capacity as a data controller and will accordingly be held jointly liable
It is possible to agree between parties who will act as a data controller with respect to a given dataset and/or to agree difference levels of responsibility and liability

Data Controllers and Data Processors

The Data Controller is defined as the person or persons who determines the 'purposes for which and the manner in which personal data are to be processed'.

The Data Processor is defined as any person '…other than an employee of the data controller who processes data on behalf of the data controller'.

Data Controllers and Data Processors are typically organisations, authorities or businesses e.g. the Data Controller of the personal data used across NHS hospitals in the Lothians area is Lothian NHS Board.

An important feature of the Data Controller/ Data Processor relationship is that the Data Controller retains liability under the DPA for all processing of personal data undertaken by the Data Processor on their behalf. There is a legal requirement that a written contract between the Data Controller and Data Processor governs processing undertaken by a Data Processor on behalf of a Data Controller.

Data Controllers may only disclose personal data in accordance with their Register entry in the Information Commissioner's Register of Data Controllers, and the Data Protection Principles set out in Schedule 1 of the DPA. Whilst the Data Controller is legally required to ensure that all disclosures of personal data meet these requirements, they do not retain these obligations after the data are disclosed. These obligations essentially flow to their recipient, who then becomes the Data Controller and liable for their use and disclosure in accordance with DPA.

Key messages:

Data controllers retain legal liability with respect to processing of data and the activities of data processors who work on their behalf until such time as data are disclosed
It is imperative to be clear with respective parties as to the capacity in which they are entering a relationship and also the point at which the responsibilities of data controller(s) will pass (if at all).

A Blueprint for Health Records Research in Scotland

Processing

The DPA defines 'processing' widely so as to encompass virtually anything that might be done with personal data (e.g. obtaining, storage, the act of anonymisation, use, disclosure, destruction) throughout its lifecycle.