When Worlds Collide

What are theOobligations of the NHS at the Interface between Data Protection and Freedom of Information Regimes?

EdinLR Vol 10 pp 150–155

When Worlds Collide: What are the obligations of the NHS at the interface between data protection and freedom of information regimes?

On 11 January 2005, ten days after the Freedom of Information (Scotland) Act 2002 (FOISA) came into force, the Common Services Agency for the Scottish Health Service (CSA) received a request for information on incidences of childhood leukaemia, in the range of 0–14 years, by year and census ward from 1990 to 2003 for the Dumfries and Galloway postal areas. The CSA refused the request on a number of grounds: that the combination of the rare diagnosis, specified age group, small geographical area and low numbers meant that individuals could be identified—the information therefore fell within the definition of "personal data" under the Data Protection Act 1998 (DPA) and should not be disclosed, "personal data" being an exempt category of information under FOISA; that having never carried out the analysis of the data by census ward the CSA did not hold the data requested; and that the CSA had a duty of confidence equivalent to that of the clinicians to whom the information were originally disclosed (and on whose behalf CSA were acting as custodians of the data). The applicant, Mr Collie, did not respond to invitations to discuss accepting alternative data or to address his needs in other ways. After requesting that the CSA review its decision and receiving the same response he then turned to the Scottish Information Commissioner (SIC) for a ruling.[1]

While accepting that the requested data constituted personal data under the DPA, the SIC nevertheless ruled that a perturbed, "barnardised" version of the requested table—that is, one that involved changing small figures by adding 0, +1 or -1 in an attempt to maintain anonymity—could have been provided. On this basis the SIC held that the CSA was in breach of FOISA because it had not provided sufficient advice and assistance to Mr Collie as to what information it was able to supply as required under section 15 of the Act. The CSA has decided to appeal this decision and the case will now go to the Court of Session in Edinburgh.

The *Collie* case is the first decision to explore the interface between data protection and freedom of information with an impact on healthcare.[2] It involves the interpretation of freedom of information provisions that are more or less standards across the whole of the United Kingdom[3] and its ultimate resolution therefore has potentially wide-ranging implications. It raises significant policy issues and has the potential to create a dangerous and onerous precedent for public authorities in the health sector that are charged, simultaneously, with protecting patient data and complying with provisions of freedom of information legislation.

1 Decision of the Scottish Information Commissioner, *Mr Michael Collie and the Common Services Agency for the Scottish Health Service*, 15 Aug 2005, available at *http://www.itspublicknowledge.info/*.

2 For an overview in the healthcare context, see B Meredith, "Data protection and freedom of information" (2005) 330 *British Medical Journal* 490-91.

3 The legislation in England and Wales is the Freedom of Information Act 2000.

The aim of the data protection regime as it relates to healthcare is to protect patient privacy by regulating the processing of "personal data", defined as data which relate to an individual and from which the individual can be identified, either from one set of data or when data sets are linked.[4] *Identifiability* is, therefore, a crucial concept, and the obvious consequence is that if the processing of data cannot lead to the identification of a specific individual the provisions of data protection law do not apply. The most commonly recognised mechanism to avoid identifiability—and therefore the terms of the law—is anonymisation. But what counts as legally acceptable levels of anonymisation remains unclear.[5] While it is accepted that the law does not require *absolute anonymity* to be achieved—that is, that a link can never again be made between data and individual—*relative anonymity* is, as its name suggests, a relative matter entailing varying degrees of risk of identification depending on the circumstances of a given case.[6] It was just such a concern that preoccupied the CSA, which has argued that the application of the particular type of "barnardisation" the SIC seeks to impose is not enough to anonymise the data in this case to an acceptable degree. The fear is one of *connectivity* of data, that is, that there remains a significant degree of risk that the data revealed in the statistical table might, on release, be easily linked to other data in a manner that would point to individuals who have suffered from leukaemia. This reflects the spirit of the data protection regime, which engenders a culture of caution, and where non-disclosure of personal data is the order of the day.

The spirit of the freedom of information regime is diametrically opposed to such a culture. It imposes obligations of transparency, openness and ease of access on public authorities. Here, the information to which there is a right of access is, simply, information held by, or on behalf of, a Scottish public authority.[7] This, of course, does not apply to all information so held, and the relevant exemption in the present context is that concerning "personal data" as defined by reference to the DPA.[8] Requests for access to such data need not be complied with. If they come from the data subject herself they must be handled according to the data protection regime as a "subject access request". Moreover, if a public authority receives such a subject access request from within the freedom of information regime it must, nevertheless, process that request as subject to data protection. Thus, it would seem that the statutes draw a clear line in the sand as between their respective competencies.

The *Collie* case demonstrates all too well, however, how the respective regimes cannot be kept entirely apart. There is, in fact, a potential clash of cultures between, on the one hand, a world where the default position is non-disclosure and another where the expectation is that access should be given. The tension at the interface between these two worlds increases depending on where the expectations are set that public authorities will *facilitate* access to information that they hold. This distils into what is meant by

4 DPA, s 1(1).

5 For a useful discussion see W Lowrance, *Learning from Experience: Privacy and the Secondary Use of Data in Health Research* (2002).

6 See, e.g., the Council of Europe's Recommendation on Regulations for Automated Medical Databanks (No R(81)1) and the Council of Europe Recommendation on the Protection of Medical Data (1997, No R(97)5).

7 FOISA, s 3(2).

8 FOISA, s 38.

the obligation both north and south of the border "… to provide advice and assistance to a person who proposes to make, or has made, a request for information to it".[9]

What sort of advice and assistance must, then, be provided? The UK Information Commissioner's Office issued Guidance in October 2004 suggesting a casuistic (case-by-case) approach and recommending dialogue with the applicant to make the best assessment of his or her needs. In the instant case the applicant failed to respond to offers to discuss the issue, and one might expect this to have been the end of the matter. Importantly, the Guidance states:

> In general there will be no additional burden involved in the provision of advice and assistance as it is essentially a matter of customer service. This will mean that the duty to provide advice and assistance under the Act will much of the time be fulfilled by the delivery of an authority's usual customer service standards.[10]

The interpretation by the Scottish Information Commissioner in *Collie*, however, seems far to exceed these parameters. While it was confirmed that the information requested constituted "personal data" *and* that it would be a breach of the DPA to release the data requested by the applicant, the CSA was none the less found to be in breach of FOISA because it was held that the CSA had failed in its obligations to advise and assist by refusing to disclose perturbed data as an *alternative* to the actual data requested.

This may be a reasonable compromise at first blush: if personal data can be adequately anonymised so as to take them out of the data protection regime then there is no reason why they should not then be made public. But this ruling is based on a number of underlying assumptions which, if allowed to become established precedents, would have deleterious and far-reaching consequences.

First, is it the case that mere perturbation of data of this kind is enough to meet the requirements of relative anonymity and non-identifiability? The SIC was content to assume that the risk of identification would be "substantially removed" by these means. But this raises the question of what is required in law to ensure an *acceptable* level of anonymisation. There is, in fact, no clear legal ruling on the matter, although the UK Information Commissioner has issued guidance to the effect that it is "… incumbent on anyone processing data to take such technical and organisational measures as are necessary to ensure that data cannot be reconstituted to become personal data and to be prepared to justify any decision they make…"[11] This points to the problem of addressing the unknown risk that data may indeed be "reconstituted" once in the hands of a third party because of the possibility of connecting the disclosed (anonymised) data with other data held by, or accessible to, that party. Data protection culture would have us err on the side of caution.

This also reveals another clash of cultures between data protection and freedom of information. Whereas under the former regime it is possible to seek written assurances concerning the uses to which disclosed data may be put and so potentially limit connectivity of various data sets, the freedom of information regime expressly

9 FOISA, s 15(1). The equivalent provision in the Freedom of Information Act 2000 is s 16.

10 Information Commissioner's Office, *Freedom of Information Awareness Guidance No 23* (Oct 2004) 2.

11 Information Commissioner's Office, *Legal Guidance* (2000) 14.

prohibits public authorities seeking *any* information about the reasons behind an access request or the possible uses of disclosed information.[12] In fact there is an established set of procedures for those wishing access to data held by CSA on behalf of NHS Scotland. Researchers and others have always been required to obtain approval from a research ethics committee for access to data for research—this ensures that the purpose is justified and ethical. When access to personal data is required they have further been required to apply for approval to a Privacy Advisory Committee whose purpose is to ensure that legal and professional guidance is being adhered to. This possible route to obtaining the data was pointed out to the applicant but no response was received. Thus this decision by the SIC appears to undermine well-established safeguards put in place to ensure the legal ethical use of health data in research.

The SIC's interpretation of the duty to provide advice and assistance is potentially very wide and costly. The UK Information Commissioner's Office has made it clear that the duty is to assist applicants *in the process of their request for information*, for example, by helping them to formulate that request or by directing them to another body that may hold the relevant information. In our opinion the *Collie* case confuses this procedural duty with a duty to provide information generally; but that cannot be the nature of the duty to advise and assist, since this is the entire objective of the freedom of information legislation itself. The duty to advise and assist must concern something complementary to the general obligation; otherwise it is redundant in terms of the broader objective of the law. Moreover, the *Collie* ruling conflates the duty to disclose what you hold with a duty to disclose what you can; importantly, the specific data that were the subject of this request were not "held" by the CSA. Further analysis was required of various datasets to generate the information in the form requested, entailing further costs and man-hours of research. Thus, while the information *could* be collated, a decision that it *should* be collated raises the question of whether this is an appropriate use of freedom of information procedures, and how far, now, the duty to assist will extend. In particular, such an interpretation of this statutory duty, in the light of concerns about disclosing personal data, runs the risk of rubbing out the clear line in the sand between the realms of freedom of information and data protection.

Broader issues are also at stake in the no man's land between these two realms. For instance, the CSA pointed to the public interest in maintaining public trust and confidence in a public authority that is a custodian of health data. There is a genuine concern that this might suffer as a result of disclosure orders. If a public authority's ability to protect the identity of data subjects is weakened then the public may be less sanguine about allowing that public authority to process their data. This might in turn have important consequences in medical research, for example, concerning the completeness and reliability of data in cancer registries. A decrease in data flow to such registries could not possibly be in the public interest. Yet, while the SIC acknowledged public interest arguments, he pointed to the technicality of the exemption relied upon by CSA. This is an absolute exemption under FOISA which does not require an appeal to the public interest to justify its application. It is to be contrasted with qualified exemptions—for example where disclosure might endanger a person's safety or

12 UK Information Commissioner, *Freedom of Information Awareness Guidance No 23* (Oct 2004) 2.

physical or mental health[13]—which only apply if it is in the public interest for them to do so. We would simply point out that public interests permeate FOI legislation, DPA, and most particularly the common law of confidentiality, where the courts have repeatedly pointed to the need to consider the public interest in maintaining patient privacy and in being seen to do so.[14] The interconnectedness of these fields requires further exploration, and even the SIC himself expressly acknowledged the overlap between data protection and the common law.[15]

A final point concerns liability. FOI legislation protects public authorities against civil actions for failure to disclose information,[16] but it says nothing about exempting them from liability arising *from* disclosure where an action could still be raised under DPA by the subject of personal data released contrary to that Act.[17]

The test case of *Collie* will serve as a very important signpost for the future direction of freedom of information obligations, but as this short commentary demonstrates, the interface between the worlds of freedom of information and data protection remains largely unexplored.

Graeme Laurie
Professor of Medical Jurisprudence
University of Edinburgh

Renate Gertz
Research Fellow
AHRC Research Centre for Studies in
Intellectual Property and Technology Law
University of Edinburgh

EdinLR Vol 10 pp 155–163

Is the Disability Discrimination Act Discriminatory?

A. INTRODUCTION

The experience of litigants has shown that it is extremely difficult for those with a mental illness to fulfil the requisite requirements to be classified as disabled in terms of the Disability Discrimination Act 1995 (DDA 1995). This raises the question as to whether the DDA 1995 is itself discriminatory, in the sense that it is easier for someone with a physical impairment to meet its conditions than someone with a mental impairment. Historically, the lack of attention given to "psychiatric disability" means that disability law, policy and practice has developed more with physical rather than

13 FOISA, s 39.
14 See *X v Y* [1988] 2 All ER 648. and more recently *Campbell v Mirror Group Newspapers plc* [2004] 2 AC 457.
15 Note 1 above, para 102.
16 FOISA, s 55.
17 DPA, s 3.