

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1.

Comments: The [Nuffield Council on Bioethics](#) is an independent UK-based advisory body, funded by the Nuffield Foundation, the Wellcome Trust and the Medical Research Council. Two of its recent reports raise issues in relation to use and sharing of personal information in the public and private sector, and this response is based upon the conclusions of these reports.

Firstly, in September 2007, the Council published a report entitled [The forensic use of bioinformation: ethical issues](#). In this report the Council considered issues around the collection, storage and use of bioinformation in the criminal justice system, particularly DNA samples and profiles and fingerprints. This response highlights its findings on the use and sharing of personal information for forensic use, specifically data held on the National DNA Database and the national fingerprint database, IDENT1.

The Nuffield report noted that effective governance of the National DNA Database (NDNAD) and the national fingerprint database, IDENT1, should help to ensure not only that their utility is maximised, but also that their potential harmful effects such as threatening privacy, undermining social cohesion and aggravating discriminatory practices are minimised. However, there is currently

no statutory basis for the operation of the NDNAD or IDENT1 or for their governance. Rather, the development of the law has been piecemeal, leaving uncertainty in places. Notwithstanding this, the NDNAD and IDENT1 are subject to the laws governing data protection.

The exemptions in the Data Protection Act regarding data that are processed for the prevention or detection of crime and the administration of justice result in (1) the situation that data subjects can be denied access to their data on the NDNAD and IDENT1, and (2) the situation that data are not required to be processed fairly and lawfully under the Data Protection Act, permitting the police to share data with other specified agencies.

Secondly, in November 2007, the Nuffield Council published [*Public health: ethical issues*](#), which considers the ethical and social issues arising when designing measures to improve public health. It illustrates the discussion by reference to case studies, including that of surveillance and monitoring of infectious disease, which raises issues around the collection and use of personal data.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2.

Comments: In relation to the forensic use of bioinformation, due to the criminal offences involved and the usefulness of biometrics from convicted offenders in investigating crime, the Council judged it proportionate only for data concerning the bioinformation of people convicted of recordable offences to be retained (and thus also be capable of being shared with appropriate agencies for relevant purposes). As an exception, the Scottish practice of allowing retention of samples and profiles, for three years, from those charged with serious violent or sexual offences, even if there is no conviction, should also be followed. Thereafter the samples and profiles should be destroyed unless a Chief Constable applies to a court for a two-year extension, showing reasonable grounds for the extension.

When used in combination, new biotechnologies have the potential to build 'multi-modal' identification systems. These might enable the police to link together several separate biometric and other databases. Alongside the benefits to holding data about convicted offenders, it becomes even more imperative that innocent people's data are not held (and thus shared) in this way, given the risks set out in answer to Question 3 below.

In relation to public health and infectious disease, two main types of data collection and usage can be identified. Firstly, broad infectious disease surveillance involves the systematic collection, analysis and interpretation of data about incidence and prevalence of infectious diseases, and factors that may contribute to them. This forms an integral part of the protection of population health, and without collecting and using this data it may not be

possible to assess and predict trends and risks in infectious diseases. These surveillance data will often be anonymised, although in some circumstances it may be necessary to collect such data in a non-anonymised way. Secondly, there is monitoring to detect cases of particular diseases that may require specific public health intervention, for example through the 'notifiable disease' programme. The aim of such measures is generally to prevent harm to others from the spread of disease. In this case, the data collected necessarily includes personal information, for example to identify the individual, and this information may be shared with relevant professionals for the purposes of implementing disease control measures. With both types of surveillance, there are benefits of sharing information for both individuals and for society as a whole.

Question 3.

Comments: The protection of the public from criminal activities is a primary obligation of the state. However, this obligation must be exercised with due respect for a number of fundamental ethical values, primarily liberty, autonomy, privacy, informed consent and equality. The legally enforceable relevant human rights include the right to a fair trial, the right to respect for private and family life, and the right to equal treatment. Any interference with these last two rights must be proportionate.

In terms of retaining innocent people's data on forensic databases (and thus opening the possibility of data sharing), the Nuffield Council judges this to be disproportionate. In the public debate about forensic databases the argument is sometimes put forward that those who are innocent have nothing to fear from being on the NDNAD. We consider that this argument is fallacious, even if we assume that the justice system is perfect and that no one who is innocent of a crime is ever convicted (an idealisation that has historically never been achieved). First, if innocent, simply being the subject of a criminal investigation by the police can cause harm, distress and stigma. For example, if a person is one of a number of persons investigated in connection with a rape because his DNA profile matches a partial profile of the perpetrator, he may well be harmed by the taint of suspicion, both personally and socially, even if he is never arrested or charged. Second, there are reasons to believe that erroneous implications concerning 'criminality' may be drawn from the mere fact that a person's profile is on the NDNAD, even if inclusion signifies only that they have once been arrested. Indeed, the explicit justification for the extent of the NDNAD is precisely that it is intended to represent the actual or likely criminal community. There is thus little doubt that it is not irrational for a person to object to the retention of their biological sample and DNA profile on the Database if they have never committed a criminal act in their whole life nor will ever do so.

In relation to public health and infectious disease, two main concerns with taking and sharing data may be raised: consent and privacy. In the report *Public health: ethical issues*, we suggest that

“it is acceptable to collect and use anonymised data for assessing and predicting trends in infectious disease without consent, as long as any invasion of privacy is reduced as far as possible ... In some

circumstances it may be necessary to collect surveillance data in a non-anonymised way, but provided adequate systems are in place to ensure confidentiality of the collected data, it may be justifiable to collect such data without consent” (para 4.39-4.40).

Furthermore we suggest that:

“the avoidance of significant harm to others who are at risk from a serious communicable disease may outweigh the consideration of personal privacy or confidentiality, and on this basis it can be ethically justified to collect non-anonymised data about individuals for the purposes of implementing control measures. However, any overriding of privacy or confidentiality must be to the minimum extent possible to achieve the desired aim” (para 4.43).

While these conclusions are drawn specifically in relation to infectious diseases, we would anticipate that these principles would apply also in other areas of health research of importance.

Question 4.

Comments:

Question 5.

Comments: *Situations in which excessive data are held*

In relation to the forensic use of bioinformation, the Nuffield Council recommends that the law relating to retention in England, Wales and Northern Ireland should be brought into line with that in Scotland. Fingerprints, DNA profiles and subject biological samples should be retained indefinitely only for those convicted of a recordable offence. At present, the retention of profiles and samples can be justified as proportionate only for those who have been convicted. In all other cases, samples should be destroyed and the resulting profiles deleted from the NDNAD.

The Scottish practice of allowing retention of samples and profiles, for three years, from those charged with serious violent or sexual offences, even if there is no conviction, should also be followed. Thereafter the samples and profiles should be destroyed unless a Chief Constable applies to a court for a two-year extension, showing reasonable grounds for the extension.

Volunteers (who may be victims, witnesses or volunteers in mass intelligence screens) may consent at the time of sampling to their profiles being permanently loaded onto the NDNAD. This decision is currently irrevocable. Such an approach is contrary to standard practice in medical research, and differs from practice in Scotland and many other European countries, where consent can be withdrawn. It is our view that consent given by a volunteer to retain their biological samples and resulting profile on the NDNAD must be revocable at any time and without any requirement to give a reason. In view of the importance of this principle, we recommend that as a matter of policy, volunteers should not be asked to consent to the permanent storage of elimination biological samples and retention of DNA profiles derived from these samples beyond the conclusion of the relevant case.

When considering requests for the removal of profiles from the NDNAD and the destruction of biological samples taken from minors (including from adults who were minors when their DNA was taken), we recommend that there should be a presumption in favour of the removal of all records, fingerprints and DNA profiles, and the destruction of samples. In deciding whether or not the presumption has been rebutted, account should be taken of factors such as:

- the seriousness of the offence;
- previous arrests;
- the outcome of the arrest;
- the likelihood of this individual re-offending;
- the danger to the public; and
- any other special circumstances.

Question 6.

Comments: In relation to the forensic use of bioinformation, the subject samples (swabs of biological material taken by the police from arrestees, victims and consenting volunteers) sent by the police to the private companies that analyse and store biological samples are accompanied by the individual's 'datacard', which contains the name of the person from whom the sample was taken, and their gender. The private providers of DNA analysis have all commented that they do not need the datacards sent to their laboratories as the samples are identifiable by means of a 'barcode'. Yet their possession of them creates the possibility that the security and confidentiality of samples could be compromised. We recommend that datacards should not be provided to private companies. Non-coded identifying details (such as a name) should be removed from the sample as early as possible during the DNA analysis and storage process.

Question 7.

Comments:

Question 8.

Comments: Please also see response to Question 6.
The Nuffield Council recommends that it should be an absolute requirement that any NDNAD samples or data provided for research should be irreversibly anonymised (that is, neither the researchers nor the Custodian or any NDNAD staff should be able to relate any result to any named individual). A condition of the release of any biological sample to researchers should be that the researchers would not profile the DNA of any sample. It would be necessary to ensure that, even if the researchers were to do so, they would never be allowed to interrogate the NDNAD to identify the individual with that profile. If such safeguards could not be put in place for a research project, the project should not be permitted. The safeguards are required to protect the fundamental ethical values of liberty, autonomy, privacy, informed consent and equality mentioned in the response to Question 3.

Section 3: The legal framework

Question 9.

Comments:

Question 10.

Comments:

Question 11.

Comments:

Question 12.

Comments:

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

Question 17.

Comments:

Question 18.

Comments: In relation to the forensic use of bioinformation, the police fingerprint database IDENT1, like the NDNAD, must retain public confidence in its security, especially its protection from non-authorised access and in control of its uses. This confidence depends on ongoing scrutiny and systematic audit of its uses so that the public can be sure that data held in it are not misused or misrepresented. There should be regular public reports on the use, scrutiny and auditing of this database.

With reference to research using stored biological samples and data held on the NDNAD, we make a general recommendation that all research proposals and stored samples should be formally, independently and transparently evaluated. Information provided by the NDNAD Strategy Board detailing requests that it has received for research access to the NDNAD and stored samples is superficial and it is not clear that sufficiently strict criteria are currently applied. At present, there is a significant lack of transparency concerning research using the NDNAD and stored samples, with the cursory details provided in the NDNAD Annual Report being inadequate. Given this lack of information, it is not possible for the public to be reassured that research projects will only be approved if their potential benefits are sufficient to outweigh the harm to the other interests involved. We recommend the

regular publication of further details concerning, as a minimum:

- information on requests and approvals, including the criteria used to determine approval or refusal;
- whether there was informed consent for the use of biological samples;
- which individuals have been given approval to undertake research projects using the NDNAD and stored samples;
- exactly what the purpose of this research was;
- whether the research has been subject to adequate levels of scientific and ethical review; and
- the outcomes of research.

Question 19.

Comments:

Section 5: Technology

Question 20.

Comments:

Question 21.

Comments:

Question 22.

Comments: Please also see response to Questions 2 and 8.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments: Although forensic biometric databases are not currently linked to each other in any sophisticated fashion, it is a stated aim for databases to be 'inter-operable' in the near future. The ethical implications of such databases could then be 'multiplied' by linking with other databases. The concerns, particularly about privacy, where access to one database may permit access to information across several databases, may be further compounded if linkage is envisaged

between databases across different countries. We recommend, on the basis of standard European data protection principles, a minimum set of safeguarding requirements to consider before allowing access to bioinformation databases to international law enforcement agencies, which would be:

- to ensure there is a sufficient level of data protection in all authorities/agencies that would receive information;
- to subject each request to adequate scrutiny as to merit and reasonableness and on a transparent basis;
- to agree the criteria for sharing data, for example only for the investigation of serious crimes or in special circumstances; and
- to share only as much information as is necessary to meet the request and only to those authorities or agencies which 'need to know'.

We recommend, on the basis of standard European data protection principles, a minimum set of safeguarding requirements to consider before allowing access to bioinformation databases to international law enforcement agencies, which would be:

- to ensure there is a sufficient level of data protection in all authorities/agencies that would receive information;
- to subject each request to adequate scrutiny as to merit and reasonableness and on a transparent basis;
- to agree the criteria for sharing data, for example only for the investigation of serious crimes or in special circumstances; and
- to share only as much information as is necessary to meet the request and only to those authorities or agencies which 'need to know'.

Question 28.

Comments:

Full name	Hugh Whittall
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	Director - response submitted on behalf of the Nuffield Council on Bioethics
Date	13 th February 2008
Company name/organisation (if applicable):	Nuffield Council on Bioethics
Address	28 Bedford Square London
Postcode	WC1B 3JS
Address to which the acknowledgement should be sent , if different from above	
We work on the assumption that we will publish the responses we receive. Please state explicitly if you want all or parts of your submission to be treated as confidential, explaining why. Please note, that this does not in itself guarantee confidentiality (see 'Publication of summary of responses' section below).	
We intend to hold more in-depth interviews with certain respondents. Please indicate if you would be happy for us to contact you.	Yes, I would be happy to be contacted ✓ No, please do not contact me <input type="checkbox"/>

Publication of summary of responses

Following the end of the consultation we will publish a paper summarising the responses. The response paper will also be available on-line.

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004). Although information held by the Review Team is not covered by the Freedom of Information Act we intend to operate a voluntary access scheme in keeping with the FOIA, and please be aware that the majority of the Review's information will be handed over to the Ministry of Justice for long-term preservation at the close of the Review, and the Ministry is covered by the FOIA.

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Ministry.

The Ministry and the Review will process your personal data in accordance with the DPA.