Caldicott Inspection of the National Haemophilia Database

Nicholas Jones, Data Protection & Freedom of Information Manager, Central Manchester University Hospitals NHS Foundation Trust

Contents:

Introduction

This report assesses the compliance of the National Haemophilia Database (NHD) with both the Data Protection Act 1998 (DPA), which sets out a legal framework for processing of personal data, and the Caldicott Principles, which relate to the handling patient identifiable information within the NHS.

The NHD exists to collect data about patients with bleeding disorders within the UK. The database contains detailed information about patients including names, diagnosis, NHS number and details relating to treatments and conditions. As a result it contains personal data as defined in s.1(1) of the DPA, as individual data subjects are identifiable from the information held. Much of the data is sensitive personal data, as it relates to physical health or condition of data subjects (DPA s.2). This means that conditions must be met from both Schedules 2 & 3 of the Act.

The data controller for the database is the UK Haemophilia Centres Doctors' Organisation (UKHCDO), as it is this body which controls the purpose and manner which and the server which contains the data is physically located within Central Manchester University Hospitals NHS Foundation Trust (CMFT).

UKHCDO is notified with the Information Commissioner's Office as a data controller; the stated purposes for the processing of personal data relevant to the NHD include Health Administration and Services, and Research.

There has recently been correspondence between UKHCDO and the Department of Health (DH) regarding whether in light of the fact haemophilia centres are required by DH to collect data, the DH should in fact be seen as data controller. However, while it is possible this will change in the future the

UKHCDO is currently responsible for the database and the information contained in it.

1. The First DPA Principle

DPA First Principle:

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

1.1 Fair processing notice

The first requirement of the First Principle is that data must be processed fairly. In order for processing to be fair data subjects must be made aware of how their data is being used, and specifically must be provided with the following details:

- Identity of the data controller
- Identify of any nominated representative
- Purpose(s) for which the data will be processed
- Any further information necessary for fairness

This is often referred to as a Fair Processing Notice. This information in relation to the NHD is provided in the leaflet *The National Haemophilia Database: Your Questions Answered*, which meets all the necessary requirements. The leaflet sets out how and for what purposes data will be processed, and gives details about precisely what information is held on the database

It is very important therefore that all patients are provided with the leaflet before their data is collected, so that data subjects are provided with the necessary fair processing information. this is done through the national network of haemophilia centres.

1.2 DPA Schedules 2 & 3

In addition to being fair and lawful any processing of personal data must meet one of the justifications set out in Schedule 2 of the Act and, as the NHD contains sensitive personal data, a schedule 3 condition is also necessary.

The conditions which can be met are as follows:

DPA Sch. 2 Condition 6:
The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is

unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

DPA Sch. 3 Condition 8:
8 (1) The processing is necessary for medical purposes and is undertaken by—
(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

These conditions are met and so therefore this element of the First Principle is met.

It should be noted that explicit consent is not sought from data subjects before their data is collected. Explicit is not necessary as other schedule 2 & 3 conditions are met, as demonstrated above. UKHCDO has been in correspondence with the Information Commissioner's Office (ICO), which has advised that this arrangement is acceptable. However, it is still important that the Fair Processing Notice (contained in the leaflet) is supplied to the data subjects as soon as is practicable, especially as this contains details of how patients can object to their data being included.

2. Purposes

DPA Second Principle:

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Caldicott First Principle:

Justify the purpose(s) of using confidential Information

The purposes for which the data is used are contained in the leaflet *Your Questions Answered*, and also specified in the UKHCDO's notification as a data controller. These purposes are lawful.

UKHCDO is aware that data could not be used for other purposes that could not reasonably be expected, without seeking further consent from the data subjects. There are no plans to use the data for purposes other than those already stated.

3. Data Quality

DPA Third Principle:

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

DPA Fourth Principle:

Personal Data shall be accurate and, where necessary, up to date.

Caldicot Principle 3:
Use the minimum data that is required

All data stored in the database is deemed to be necessary for the purposes for which it is collected (see section 2 for further details on the purposes).

The data is identifiable in nature, and includes patients names and NHS numbers which can be used as identifiers. However, the use of named rather than anonymous data is justified as this is necessary to prevent the possibility of multiple records, which would lead to inaccuracy. Identifiable data is therefore not excessive for the purposes for which it is collected, but rather anonymous data would be inadequate for the purposes for which it is used. This therefore does not breach the third Caldicott principle which states that only the minimum necessary data should be used.

The fourth DPA principle requires that data be accurate and kept up to date, and the NHD is committed to ensuring that the data it holds is accurate. The previous Caldicott inspection from 2006 recommended that a programme of work around data quality and accuracy should be carried out, and a large amount of work has been done to ensure accuracy and quality, including the following actions:

- The NHD has an information sharing agreement with 'The Information Centre' (formerly the Office of National Statistics). Patients registered with the NHD are notified to The Information Centre. The Information Centre provides the NHD with notification of any deaths and a copy of the death certificate.
- The NHD also carries out a once or twice yearly patient demographic update through the NHS strategic tracing service (NSTS) to ensure accuracy of data. This is facilitated through the CMFT Data Quality Team.
- A data cleaning exercise, focussing on severe Haemophilia A and B patients not treated since 2006 was carried out in July 2008. This was carried out as part of the UKHCDO Data Quality Accreditation Programme when the National Haemophilia Database began reviewing its definition of a 'Registered Patient'. The definition contains the follows: A patient who is treated at a haemophilia centre on a regular basis or a patient who is reviewed at a haemophilia centre on a regular basis

4. Rights

DPA Sixth Principle:

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The DPA sets out a number of rights which data subjects can exercise, and the sixth principle makes it a breach of the Act for data controllers not to process personal data in accordance with these. The rights that are of greatest relevance to the NHD are:

- **s.7 – right of subject access**
- **s.10 – right to prevent processing likely to cause damage or distress**

Section 7 of the Act provides data subject with a right of access to personal data about themselves, subject to certain exemptions. This means that patients have a right to request the information that is held about them.

UKHDCO produces a form entitled ‘Application for Access to Health Records’ which allows data subjects to request details from the database (although patients do not need to complete this form to make a valid request). Patients are asked for a form of identification in order that identities can be verified to ensure that data is not given out to those who do not have a right to it, and requests are dealt with within the statutory 40 day time limit.

The 2006 Caldicott inspection made a number of recommendations in this area which have now been carried out. As information on the database is held electronically a maximum of £10 is charged.

UKHCDO is aware of the issues regarding requests from children and their competency to give consent (Gillick competency), although due to the nature of the NHD it is highly unlikely that requests from minors will be received.

Requests for data to be anonymised or fully deleted have been received and have been respected and handled in accordance with section 10 of the Act.

The DPA does not apply to deceased patients, but there is still a duty of confidentiality towards information about such individuals, and any requests for such records are handled under the Access to Health Records Act 1990 (AHRA).

5. Security

DPA Seventh Principle:

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.

Caldicott Fourth Principle:

Access to patient identifiable information should be on a strict need-to-know basis

Caldicott Fifth Principle:

Everyone must understand his or her responsibilities

Caldicott Sixth Principle:

Understand and comply with the law

These principles relate to security, and make it necessary to ensure that only authorised staff with a genuine need to access the database are able to do so, and also to take measures to ensure both physical and electronic security. This also includes ensuring the reliability of staff through training and other measures.

5.1 Staff training

The interpretation of the seventh principle in the DPA states a data controller must take reasonable steps to ensure the reliability of any employees who have access to personal data. All staff with access to the NHD are giving training both on use of the system and on their responsibilities to maintain privacy and confidentiality.

All new staff are required to attend the CMFT induction day which includes a session on Information Governance containing an overview of the DPA and

the Caldicott Principles. In addition they are required to annually view training material produced by the ICO in order to refresh and maintain their knowledge.

Standard NHS confidentiality clauses are included in all contracts, ensuring that staff are contractually bound to respect confidentiality.

The data collection team are all members of the UKHCDO Haemophilia Data Managers Forum, which meets twice yearly. Data protection is a regular agenda item and at previous meetings a member of staff from the Information Commissioners Office has attended to speak to at the forum.

Staff are therefore aware of the law and their own responsibilities, and are fully trained to use the system correctly.

5.2 Physical security

The secure server is kept within a server hotel within Manchester Royal Infirmary, within CMFT. Full operating system and data backups are performed to tape on a nightly basis. The power supply is un-interruptible and the server works on R.A.I.D. 5 configuration.

Any physical documents containing identifiable data are stored in locked, secure areas to which only authorised staff have access.

5.3 Electronic security

Access to the database is password restricted. A username and password is required for all users, and must be requested from the Haemophilia Centre Director. Only those with a need to access the data are provided with login credentials. Usernames are sent by email and passwords are sent separately by post to the new user.

All data sent between the server and clients is encrypted using Secure Sockets Layer, and HTTPS secure web page format.

Patient identifiable data is never carried by staff on any form of storage device. The system creates audit logs (audit trail, audit log on successes / failures, audit emails), and administrators are automatically informed of unauthorised access attempts.

6. Other considerations:

6.1 DPA 8th Principle:

This is not engaged as no data is transferred out of the EEA, and there are no plans for this to happen.

6.2 Disclosures of information from the database

One of the purposes for the collection of personal data in medical research, and therefore information is disclosed to other organisations for research

purposes. These purposes are included both in the UKHCDO's registration with the ICO and in the *Your Questions Answered* leaflet, and so are specified purposes in relation to the second principle. Such disclosures are described in more detail in *Your Question Answered* and so data subjects are informed that their information may be used for these purposes. Such data is anonymised, and so patient identifiable information is not disclosed. This processing is therefore compliant with the DPA.

A process is in place for assessing applications for such data. This includes the consideration of ethical factors. Disclosures are therefore authorised or refused according to a detailed policy, which includes consideration of any possible privacy concerns.

Following the previous report UKHDCO is aware of the possibility that in some circumstances release of details relating to small numbers patients may make it possible for individuals to be identified, even if all identifiers are removed. This possibility is considered when deciding whether or not to disclose anonymised information.

7. Conclusion

In the ways stated above the NHD is operated in accordance with both the DPA and Caldicott principles. The recommendations made in 2006 have been acted on in order to ensure that all requirements are met, demonstrating the commitment of the organisation to maintain the highest standards of privacy and security.

Nicholas Jones
Freedom of Information & Data Protection Manager
CMFT