Information Governance Assessment of the National Haemophilia Database

Nicholas Jones, Information Governance Manager,
Giovanni Cerisola, Information Governance Manager
Central Manchester University Hospitals NHS Foundation Trust

Contents:

1. Introduction

This report assesses the compliance of the National Haemophilia Database (NHD) with the wider NHS Information Governance Agenda, including the following:

- Data Protection Act 1998
- Caldicott Principles
- Department of Health guidance

This assessment was undertaken on 19 June 2013, when the authors visited the offices of UKHCDO. A previous assessment was carried out in 2009.

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 a very large volume of sensitive personal data which needs to be stored, used and disclosed securely and appropriately.

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 in which the data is processed. The server which holds the data is no longer held by the Trust and is now physically located in a facility at Central Manchester Clinical Commissioning Group (CCG) (previous NHS Manchester).

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.

2. General principles

Explicit patient consent is not sought before data is added to the database, which is operated instead on an opt out model. Explicit consent is not necessary as appropriate conditions as set out in the DPA are met, and individual are given an opportunity to object and ask for their data to be removed. This makes it particularly important that patients are provided with sufficient information about the database and an appropriate Fair Processing Notice that meets the requirements of the DPA.

This information is provided in the leaflet *The National Haemophilia Database: Your Questions Answered*, 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. This is provided to new patients and is also available on the UKHCDO website. An updated version of the leaflet is currently being drafted, and will be made available when finalised.

Recommendation: full details of disclosures and their purposes should be included in the new draft of the leaflet, reflecting recent changes in NHS structures and practice.

3. Data quality

All data stored in the database is deemed to be necessary for the purposes for which it is collected and used. As a general principle the level of data collected should be the minimum necessary. The data is identifiable in nature, and includes patient's 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 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.

In addition it is important that patients who have died are recorded correctly on the database. To facilitate this 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.

Recommendation: the data sharing agreement should be reviewed to ensure it is still valid and up to date following recent structural changes within the NHS.

4. Data rights

Section 7 of the DPA 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. UKHCDO has appropriate processed for handling such requests.

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. Staff are aware of the correct procedure for handling requests.

UKHCDO is aware of the issues regarding requests from children and their competency to give consent, 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

The seventh DPA principle creates a duty to take appropriate measures to ensure the security of personal data, both physical and electronic.This also includes ensuring the reliability of staff through training and other measures.

a) Staff training

All staff with access to the NHD are given 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 and complete annual CMFT Corporate Mandatory Training, both of which contain Information Governance modules which are compliant with the IG Toolkit training requirements. 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.

b) Physical security

The server is now kept within a facility at Manchester CCG (formerly NHS Manchester), and is no longer hosted by the Trust. As such its security falls outside of the remit of this assessment.

Papers files are stored at the UKHCDO offices, and appropriate physical security measures are in place, including locked keypad operated doors, to prevent unauthorised access to areas where information is stored.

Recommendation: Appropriate assurances should be sought from the CCG to confirm the security of these data storage arrangements.

c) Electronic security

Access to the database is password restricted. A username and password is required for all users, and must be requested from the NHD Administrator using the form provided which must be authorised by 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 Socket Layer, and HTTPS secure web page format. Policies exist to prevent the processing of personal data on insecure portable devices. The system is able to create audit logs (audit trail, audit log on successes / failures), and administrators are automatically informed of unauthorised access attempts. More than three incorrect logon attempts automatically locks out the user.

6. IG Toolkit

IT services are provided to UKHCDO by Medical Data Solutions and Services (MDSAS), who have completed the Information Governance Toolkit version 10 (2012/13) achieving compliance with all requirements. UKHCDO has not previously completed the Toolkit but is considering doing so.

Recommendation: To ensure comprehensive assurance of compliance with the relevant IG standards UKHCDO should consider completing the IG Toolkit for the current financial year and subsequent years.

7. Disclosures of information from the database

One of the purposes for the collection of personal data is medical research, and therefore information is disclosed to other organisations for research purposes. 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 always 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. which includes 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 of 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.

8. Conclusion

In the ways stated above the NHD is operated in accordance with appropriate Information Governance

The recommendations made in 2009 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, and willingness to undertake the completion of the IG Toolkit reinforces this. As with all organisations it is important to keep up with rapid changes in technology and ensure that policies and processes and updated as necessary to reflect this.