Information Governance Assessment of the National Haemophilia Database

Date: 24th August 2017

Contents:

Introduction

This report assesses the compliance of the National Haemophilia Database (NHD) within the Data Protection Act 1998 (DPA); Freedom of Information Act 2000; Caldicott Principles and other NHS Information Governance legislation and good practice as appropriate.

The NHD exists to collect data about patients with bleeding disorders within the UK. The NHD contains information about patients including their name; diagnosis; NHS Number and details relating to treatments and conditions. As a result of capturing this data, the NHD contains a substantial volume of both personal and sensitive data, which has to be stored; processed and disclosed in a secure and appropriate manner in line with legislation and good practice.

The data controller for the database is the UK Haemophilia Centres Doctors' Organisation (UKHCDO), and it is this body that controls the purpose and manner in which the data is processed. The physical N3 servers are hosted at a facility operated by the Greater Manchester Shared Services (part of the North West Commissioning Support Unit of the NHS).

UKHCDO is registered 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 is a Data Analysis Group within the organisation which includes patient representatives, which is responsible for reviewing all requests for data held by UKHCDO.

2. General Principles

Explicit patient consent is not sought before data is added to the database. An opt out model is in place enabling patients to choose whether to have their data added to the database or not. Explicit consent is not necessary as appropriate conditions within the DPA are met, and individuals are given the opportunity to object and request that their data 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. All leaflets are revised on a regular basis.

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 provides details about precisely what information is held on the database. This is provided to new patients and is also available on the UKHCDO website.

Recommendation: *The leaflet should be reviewed prior to May 2018, to ensure the leaflet contains any changes required to meet compliance under the European Union General Data Protection Regulations (EU GDPR)*

3. Data Quality

All data stored within the database is deemed to be necessary for the purposes for which it is collected and processed. As a general principle, the level of data collected should be the minimum required. The data is identifiable in nature, and contains patients names and NHS numbers which can be used as identifiers. The use of named rather than anonymised data is justified as this is necessary to prevent the possibility of duplicate and/or multiple records, which would lead to inaccuracy. Identifiable data is therefore not considered excessive for the purposes for which it is collected, but rather anonymous data would be inadequate for the purposes for which it is used.

The NHD also carries out a once or twice yearly patient demographic update through the NHS Strategic Tracing Service (NSTS) to ensure data accuracy. This is facilitated through the Manchester University NHS Foundation Trust (MFT) Data Quality Team. In addition, where UKHCDO is notified that a patient is deceased, this is recorded on the database to ensure accuracy. To facilitate this, the NHD had a process in place whereby information from NHS Digital (formerly the NHS Information Centre) was shared relating to deceased patients to enable the database to be updated. An application to the Health Research Authority (HRA) through the Confidentiality Advisory Group has been submitted for section 251 approval to restart the previous data sharing agreement with NHS Digital.

Recommendation: *Should the section 251 approval from the HRA not be granted, the UKHCDO may need to identify an alternative process for ensuring data accuracy in relation to deceased patients.*

4. Data Rights

The DPA provides data subjects with a right of access to personal data held about themselves, subject to certain exemptions. This means that patients have a right to request information that is held about them. UKHCDO has an appropriate process in place for handling such requests and this is clearly outlined on the website.

A form entitled *Application for Access to Health Records* allows data subjects to request details from the database. Patients are asked for a form of identifications in order that identities can be verified to ensure data is not given out to those who do not have a right to it, and requests are dealt with within the current statutory 40 day time limit. Staff are aware of the correct procedure for handling subject access requests.

UKHCDO is aware of the issues regarding requests from children, and a childs competency to give consent. Due to the nature of the NHS, it is highly unlikely that requests from minors will be received – to date there have been no such requests received. The UKHCDO is aware of potential changes which will need to be taken account of following implementation of the new regulations under the EU GDPR. The Chair of the Data Management Working Party and the Director of the NHD have been briefed on the implications of the new regulations under EU GDPR.

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

The DPA does not apply to deceased patients, but there remains a duty of confidentiality towards information about such individuals. Requests received for records pertaining to deceased patients are handled in accordance with the Access to Health Records Act 1990.

Freedom of Information (FOI) requests are dealt with under the FOI Act 2000 and are in the main received from parliament or the Department of Health. Staff are aware of the correct procedure for handling FOI requests.

Other requests that may be received include Research and Development information in relation to staff appraisals. Staff are aware of the correct procedure for handling such requests.

5. Security
The DPA includes the duty to take appropriate measures to ensure the security of personal data, both in physical and electronic form. This also includes ensuring the reliability of staff through training, awareness and other measures.

5a. Staff Training
All staff with access to the NHD are required to undertake training, both on the use of the system and on their responsibilities to maintain privacy and confidentiality. All new staff are required to attend the MFT Trust Induction day, and complete their annual Corporate Mandatory Training, both of which contain Information Governance sessions/modules, which are compliant with the Information Governance Toolkit (IGTK) training requirements. In addition, staff 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 employment contracts, ensuring that staff are contractually bound by confidentiality legislation and good practice. The data collection team are all members of the UKHCDO Haemophilia Data Managers Forum, which meets twice yearly. Past meetings were confirmed as having taken place on 26th May 2017, and 26th September 2017. Data Protection is a regular agenda item and at previous meetings a member of staff from the Information Commissioners Office (ICO) has attended to speak at the forum. Staff are therefore aware of the law and their own responsibilities, and are fully trained to use the system correctly.

5b. Physical Security
The physical N3 servers are hosted at a facility operated by the Greater Manchester Shared Services (part of the North West Commissioning Support Unit of the NHS).

Paper files are stored at the UKHCDO offices under appropriate physical security measures, including locked keypad operated doors to prevent unauthorised access to areas where information is stored. Old paper records are archived to an off-site storage facility. An audit of records is undertaken every 6 Months.

5c. Electronic Security
Access to the database is password restricted. A username and password is required for all users to gain access, which is only provided by the NHD Administrator using the form provided which must be authorised by the Haemophilia Centre Director.

Only those persons with a need to access the data are provided with logon credentials. Logon credentials in respect of the username are communicated via email, but the password is sent separately via royal mail to the new user.

All data sent between the server and clients is encrypted using Secure Socket Layer (SSL) and HTTPS secure web page format. The following NHD policies are in place to prevent the storage and processing of personal data on insecure portable devices:

- Information Security Policy
- Code of Conduct for Staff
- Remote Access Policy
- Risk Management Policy

The above policies were briefed to staff in August 2017, through Data Security Level 1 Awareness Training.

The NHD has the ability to provide audit logs (audit trail; audit log on successes/failures) and administrators are automatically informed of potential unauthorised attempts. More than three incorrect logon attempts will result in the user becoming automatically locked out of the NHD.

6. Compliance

Compliance is monitored through completion of the Information Governance Toolkit (IGTK) on an ongoing annual basis. IT services are provided to UKHCDO by Medical Data Solutions and Services (MDSAS), who have completed the IGTK which was submitted on 31/03/17. A score of 100% was reported. UKHCDO completed the IGTK assessment for the first time during 2016-17 as a trusted partner, and obtained a satisfactory score of 69%. It should be noted that this is an excellent achievement for a first assessment which provides assurance that the UKHCDO has the required level of Information Governance standards in place.

7. Disclosures of Information from the Database

One of the purposes for the collection of personal data is for medical research. Information is therefore disclosed to other organisations for research purposes. Such disclosures are described in more details in the leaflet: *The National Haemophilia Database: Your Questions Answered* which is available to data subjects to inform them of such disclosures. Data disclosed for research purposes is always anonymised therefore no patient identifiable data is disclosed, and processes are in place for assessing application for such data which includes consideration of ethical factors. Disclosures are therefore either authorised or refused according to a detailed policy which also includes consideration of any possible privacy concerns. UKHCDO also checks that if data requested results in small numbers involved, this does not result in identification being possible, even if identifiers are removed. This consideration is used when deciding whether or not to disclose anonymised information also. This processing is compliant with the DPA.

8. Conclusion

In the ways stated above, the NHD is operated in accordance with the Data Protection Act; Freedom of Information Act; and Caldicott principles. The recommendations made in 2013 have been acted upon to continue the provision of assurance that requirements are being met, which demonstrates the commitment of the organisation to maintain the highest standards of privacy and security. It remains important to keep up with the changes in technology and legislation and ensure that policies and operational procedures are update as necessary to comply with these changes.

Next Review: August 2019