National Clinical Audit of Specialist Rehabilitation following major Injury (NCASRI)

Information Governance Policy

Prepared by the NCASRI Team:

Professor Lynne Turner-Stokes
Dr Karen Hoffman
Dr Roxana Vanderstay
Mr Keith Sephton
Ms Heather Williams
Mr Alan Bill
Ms Margaret Kaminska

Version 2.

Last update: <01.04.2016>

Signed off by The NCASRI Programme Board: <21.09.2016>

Summary

The National Clinical Audit (NCA) of Specialist Rehabilitation Services aims to provide a national comparative assessment of the organisation, quality, outcomes and efficiency of specialist rehabilitation services provided for adults with complex needs following major injury. It will drive improved and equitable access to specialist rehabilitation services for these patients.

A key priority for the NCA is to create data linkage between the Trauma Audit and Research Network TARN and UK Rehabilitation Outcomes Collaborative UKROC datasets in order to track patients discharged from MTCs to identify those that subsequently received specialist rehabilitation. Both TARN and UKROC datasets have their own Information Governance Policies and data access processes.

UKROC and TARN are currently pseudonymised by each provider before being submitted to the central teams. The newly created audit dataset will be handled in accordance with the audit Information Governance Policy. UKROC application to the Health Research Authority for Section 251 to be able to collect identifiable data in the form of the NHS number is currently under development. TARN will also need to update its permissions under Section 251 for the purpose of data linkage. The controller of the linked TARN and UKROC data is HQIP. The data processor is the National Clinical Audit team. The audit dataset will be pseudonymised for on-going data storage and analysis.

Feedback will be provided to trauma units and specialist rehabilitation services using the pseudonymised IDs currently used by UKROC and TARN respectively. The feedback aims to seek clarification if missing /suspect data found during analysis of linked data and to improve data quality. Any patient identifiable data will be removed from linked audit dataset. Only TARN and UKROC IDs will remain in the audit data.
Any data transferred in portable form will be encrypted according to DH standards. The audit data will be retained for the entire duration of the audit.

1. Introduction

The National Clinical Audit (NCA) of Specialist Rehabilitation Services aims to provide a national comparative assessment of the organisation, quality, outcomes and efficiency of specialist rehabilitation services provided for adults with complex needs following major injury. It will drive improved and equitable access to specialist rehabilitation services for these patients. This policy is important because it will help the people who work for the Audit understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Information Governance Management.
- Clinical Information assurance for Safe Patient Care.
- Confidentiality and Data Protection assurance.
- Corporate Information assurance.
- Information Security assurance.
- Secondary use assurance.

2. Scope

This policy applies to all information, information systems, networks, applications, location, and all parties involved in the National Clinical Audit.

3. Policy principles

We recognise the need for an appropriate balance between openness and confidentiality in the management and use of information. We support the principles of corporate governance and recognise its public accountability, but equally place importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. There are 4 key interlinked strands to the Information Governance Policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

3.1 Openness

- Non-confidential information about the NCA and its services should be available to the public through a variety of media
- We will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- The NCA will have clear procedures and arrangements for handling queries from patients and the public

3.2 Legal Compliance

• The NCA will comply with the Data Protection Act 1998, Freedom of Information Act, Human Rights Act and the common law of confidentiality

• The NCA regards all identifiable information relating to patients and staff as confidential except where exemptions can be applied. NCA staff will be made aware of all other relevant legislation and guidance relating to information security and confidentiality.

• We will undertake regular assessments of NCA compliance with legal requirements

• Patient and/or staff information will be shared with other agencies in accordance with agreed protocols and relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

3.3 Information Security

• We will establish and maintain guidelines for the effective and secure management of NCA information assets and resources

• We will undertake regular assessments of its information and IT security arrangements

• We will promote effective confidentiality and security practice to its staff through procedures and training

• We will establish and maintain incident reporting procedures which will include the monitoring and investigation where appropriate, of reported instances of actual or potential breaches of confidentiality and security

3.4 Information Quality Assurance

• The NCA will establish and maintain procedures for information quality assurance and the effective management of records

• Wherever possible, information quality should be assured at the point of collection

• Data standards will be set through clear and consistent definition of data items, in accordance with national standards

4. Information Governance Policy Framework

Information takes many forms and includes data stored on computers, transmitted across networks, printed copy, handwritten, sent by fax, stored on tapes, diskettes, CDs, DVDs, USB memory sticks and other

mobile media, or spoken in conversation and over the telephone. Data represents an extremely valuable asset and to ensure its integrity the NCA must safeguard accuracy and completeness by protecting against unauthorised use/disclosure, modification or intelligent interruption.
The increasing reliance of the NHS on information technology for the processing of data and delivery of healthcare makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion to protect from events, accidental or deliberate, that may jeopardise healthcare activities.

1. Information Security Awareness Training

• Information security awareness training shall be included in the staff induction process.

• An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated annually.

2. Contracts of Employment

• Information security expectations of staff shall be included within appropriate job definitions.

• All contract agreement with a Third party supplier of goods, services or consultancy shall contain a confidentiality clause and an undertaking that any information obtained during the course of performing the contract is confidential and shall only be used for the sole purpose of the execution of the contract and will provide all necessary precaution to ensure that all such information is kept secure. We will ensure that their proposals are ethical, in line with your organisation's clinical audit programme and only give appropriate access to the clinical system if the project has been formally agreed.

3. Security Control of Assets

• Each information asset, (hardware, software, IT application or data) shall have a named information asset owner who shall be responsible for the information security of that asset.

4. Access Controls to IT secure Areas

• Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information system and data storage facilities. We will use the HQIP guidelines and Data Access Request - Process. Records of access will be maintained.

Guidance for Storing paper data and information

Records must be contained within a robust folder which clearly identifies the organisation. Always store in either locked cupboards or rooms and ensure access is appropriate.

Guidance for Storing electronic data and information

Password protect files/folders and only give access to those who need access.

5. User Access Controls and monitoring

• Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

• Clinical staff may need access to all data. Clinical audit team could require access to all data. Administrative staff should only need access to anonymised data. Give passwords/access to those members of staff who need it for the clinical audit.

6. Computer Access Control

• Access to computer facilities shall be restricted to authorised users who have a business need to use the facilities.

• Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

• Seek assurance that those who need access to the clinical audit data are aware of their information governance responsibilities

• Give passwords/access to those members of staff who need it for the clinical audit.

7. Security of IT system

• In order to minimise loss of, or damage to all assets, equipment shall be physically protected from threats and environmental hazards.

• The Trust will define certain locations as IT secure areas and the equipment will be installed and sited in accordance with the manufacturer's specification.

• IT equipment should be kept out of view of the general public if possible: where this is not possible computer screens should not normally be visible from public circulation areas.

• Areas housing computer equipment should keep the doors and windows closed or locked when unattended.

• Operate a clear desk policy. Lock paper information away when you're not using it.

• Secure your workstation when absent from your desk by activating a password protected screen saver or using Ctrl-Alt-Del-Lock workstation if your network supports this.

8. IT System Management

• Responsibilities will be appropriately assigned for the management of IT systems. These will include the management, monitoring and auditing of access to IT systems and the timely management of new starters and leavers and those changing job role.

9. Computer and Network Procedures

• Management of computer and networks shall be controlled through standard documented procedures that have been authorised by the IT Department.

10. Protection from Malicious Software

• The Trust shall use software countermeasures and management procedures to protect itself against the threat of malicious software. The Trust will maintain an IT Virus control Procedure.

11. User media

• Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Data manager before they may be used on the Trust's systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action. Only the Trust approved encrypted memory/USB sticks may be used where use of these are deemed necessary.

12. Access to the Internet and Email and data transfer

• The NCA will ensure adequate provision of user training to support access to Internet and Email. The Trust will maintain appropriate policies covering all areas regarding access to the internet and use of email. We will consider the following methods of transferring data and which may be the most appropriate and secure:

• email (this must be encrypted as per organisation's procedures unless using nhs.net to nhs.net)
• fax to a 'safe haven' fax
• sending via Royal Mail (marked private and confidential and using recorded delivery)
• transported by courier or NHS transport
• collected by a member of the team

13. Accreditation of Information Systems

• The Trust shall ensure that all new information systems, applications and networks include a security plan and are approved by the Data manager before they commence operation.

14. Intellectual Property Rights

• The Trust shall ensure that all information products are properly licensed and approved by the IT Department. Users shall not install software on the Trust's property without permission from the IT Department.

15. Information Risk Assessment and Management

• All key/critical computer systems will be subject to periodic risk assessments carried out by systems managers/administrators.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals.

16. Data Quality and Validation

• The Trust will ensure there is up to date, complete and accurate data within information system that support operational and clinical decision-making. Where possible validation of data entry and data analysis at input stage will be incorporated and maintained.

17. Information Security Incident Management

• All information security events and suspected weaknesses must be reported and investigated to establish their cause and impacts with a view to avoiding similar events.

18. Disposal of IT Equipment and/or confidential/sensitive data

• IT equipment disposal must only be authorised by the IT Department.

• The IT department must ensure that, where possible, data storage devices are purged of sensitive data before disposal and organise any proposed secure destruction arrangements where it is not.

• Unusable computer media should be destroyed (e.g. floppy disks, magnetic tapes, CD-ROMS). Where this is performed by an approved third party organisation, a certificate of disposal must be obtained.

• Log the retention period for the audit data, so that it can be destroyed when no longer required.

• All data must be disposed off securely and in accordance with the relevant legislation and Trust policies.

5. Responsibility

The NCA Steering Group has the role to define the NCA's policy in respect of Information Governance and risk and meeting legal, statutory and NHS requirements. It is responsible for ensuring that sufficient resources are provided to support the requirement of the policy.

All NCA staff including contract, temporary and voluntary are required to maintain the security, confidentiality, integrity and availability of all NCA information including that which relates to patients and staff. Information governance responsibilities will be detailed in all job descriptions and staff contracts of employment. Non-compliance with the policy can result in disciplinary action.

IT data Manager provides expert technical advice to the NCA on matters relating to IT Security and ensures compliance and conformance, and provides support and assistance for information security incidents.
The NCA data managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on going compliance; ensuring that all staff job descriptions contain the relevant responsibility for information security, confidentiality and records management and that staff undertake information governance mandatory training and ongoing training needs are routinely assessed. Managers shall be individually responsible for the security of their physical environment where information is processed and stored.

Both TARN and UKROC have in place full system level security policies to avoid loss of data, covering information and network security. Data security policies are available for inspection.
The UKROC database is held on dedicated NHS network servers at Northwick Park Hospital, which are firewall protected and stored in a secure facility with controlled access, onsite security staff and CCTV monitoring. Entry to secure areas is restricted to those whose job requires it. Data are only transferred by the secure NHS N3 network. All portable computing devices connected to the Trust network are configured to automatically encrypt any data stored on the hard disk of the computer.

The TARN database operates on a web-based electronic data collection system (eDCR) that is held on dedicated database servers at the University of Manchester. The servers are firewall protected and stored in a secure facility with controlled access, 24 x 7 x 365 onsite security staff and CCTV monitoring. Due to the encryption algorithm employed, TARN employees cannot view, analyse or transfer patient identifiable information. TARN also has Information Governance Toolkit Approval (ASS/112819) that demonstrates they have satisfactory governance in place to ensure security and protection of data.
Outside of UKROC and TARN, all data will be pseudonymised. KCL has similar data security policies in place to protect its computer network and data handling will comply at all times with the principles set out in the Data Protection Act.

6. Monitoring

The focus is on sustaining robust Information Governance by ensuring that the roles identified within this policy are supported by key documented responsibilities and these are reviewed annually, ensuring that appropriate policy and procedures are in place and are regularly reviewed to ensure that legal and statutory requirements are being met. We will carry out regular review of reported information security incidents

7. Review

The policy will be reviewed in one year time or earlier if appropriate to take into account any changes to legislation that may occur, and /or guidance from the Health and Social care Information Centre

8. Key reference documents

HQIP governance guide. National Clinical Audit and Patient Outcomes Programme Project Information Pack.

Open data. National Clinical Audit and Patient Outcomes Programme Project Information Pack.

NHS Connecting for Health Information Governance

http://www.connectingforhealth.nhs.uk/systemsandservices/infogov

The NHS Confidentiality Code of Practice

http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550

Information Security Management: NHS Code of Practice

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142

Records management: NHS code of practice

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

The Caldicott Guardian Manual

http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563

National Information Governance Board for Health and Social Care (NIGB) http://www.nigb.nhs.uk/

Information Commissioner's Office (ICO) http://www.ico.gov.uk/

Portable Computer Security Policy. The North West London Hospitals.

Network Security Policy. The North West London Hospitals.

INFORMATION SECURITY POLICY. The London North West Healthcare NHS Trust.

Data Protection Policy. The London North West Healthcare NHS Trust.

Data Protection (Personal Information Management) Policy. King's college London.

System level Security Policy_September 2014. Trauma Audit and Research Network.

Freedom of Information Policy, The National Clinical Audit of Specialist Rehabilitation Services

Communication Policy, The National Clinical Audit of Specialist Rehabilitation Services.

Laws affecting the use of clinical audit information

Data Protection Act 1998 — An Act to make provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. All data subjects have a right of access to their health records, therefore all records should be traceable whilst in your care.

Freedom of Information Act 2000 — An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them.

Access to Health Records 1990 —An Act to establish a right of access to health records by the individuals to whom they relate and other persons; to provide for the correction of inaccurate health records and for the avoidance of certain contractual obligations; and for connected purposes.

Human Rights Act 1998 — An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights. The Human Rights Act requires that any invasion of an individual's private life is first subject to a test of necessity and proportionality.

Computer Misuse Act 1990 — An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

Criminal Justice and Immigration Act 2008

Section 251 of the NHS Act 2006 — Section 251 of the NHS Act 2006 re-enacted Section 60 of the Health and Social Care Act 2001.

Common Law Duty of Confidentiality