

National Audit of Dementia (care in general hospitals)

Protocol on data collected by the audit

Definitions:

Within this document, the **funding body**, Healthcare Quality Improvement Partnership, will be referred to as HQIP.

The **managing body**, Royal College of Psychiatrists, will be referred to as RCPsych.

The National Audit of Dementia is funded by HQIP, and contracted by HQIP to design, conduct and report on the findings of the audit.

Partners to the audit

The audit is managed by the Royal College of Psychiatrists' Centre for Quality Improvement, working in close partnership with professional and service user representatives.

The collaborators in this project are the professional bodies for five of the main disciplines involved in providing dementia services, and one of the main voluntary sector providers of supports and services:

- **the Royal College of Psychiatrists;**
- **the British Geriatrics Society;**
- **the Royal College of Nursing;**
- **the Royal College of Physicians;**
- **the Royal College of General Practitioners;**
- **the Alzheimer's Society.**

Additionally, **Professor Martin Orrell**, Professor of Ageing and Mental Health at University College London (UCL) and North East London Mental Health Trust (NELMHT), and **Professor John Young**, Head of the Academic Unit of Elderly Care & Rehabilitation at Leeds University and Consultant Geriatrician in Bradford (LU-ECRU), are expert advisors to the programme.

Data sharing and partnership

Access to the data will be restricted to the core project team at the Royal College of Psychiatrists' Centre for Quality Improvement, key Steering Group representatives, and employees of RCPsych or partner organisations engaged in data analysis. Where data analysis is carried out outside of the core project team, the project will require that information governance principles as set out below are followed and a statement to this effect is available, and that the information is not used for any other purpose or disclosed in any way.

Any Steering Group representative, or person who is not directly employed by RCPsych will be required to sign an undertaking to respect confidentiality requirements before viewing or handling any data collected by the project.

Contents

1. Data collection
2. Data processing
3. Data reporting
4. Data storage and Freedom of Information

1. Data collection

The audit will take a modular approach and will require information of the following types:

Core audit – hospital level data

The organisational checklist will consider the context within the general hospital that supports the care of people with dementia. This includes:

- governance, including development of care pathway for dementia and activities of the board and directorates
- policies and procedures relating to delivery of care including assessment, mental health needs including cognitive testing, discharge policy, training
- specific resources supporting the care of people with dementia, including the presence/absence of key posts
- information and communication procedures

The casenote audit will ask hospitals to identify the casenotes of 40 patients with an existing diagnosis of dementia. Patient identifiable information will not be requested by the audit. Questions in the casenote audit will elicit evidence that standards relating to clinical care have been met for individual patients with dementia admitted to the hospital. This will include:

- comprehensive physical and mental health assessment including cognitive testing
- input from liaison psychiatry
- personal information to aid communication
- input from carer
- planned discharge

Enhanced audit – ward level data

The environmental checklist will gather information about aspects of the ward physical environment known to impact on people with dementia:

- orientation aids e.g. appropriate signage
- identifiable toilet and bathroom facilities
- options for personal care e.g. bathing
- availability of aids for mobility, nutrition
- layout supporting individual needs such as pacing or wandering, quiet areas, personal items and messages visible and within reach

The ward organisational checklist will look at input, policies and support on the ward:

- ward staffing
- information and communication

The observational module will examine the quality of the hour-to-hour provision of care to people with dementia. The domains that will be considered are:

- person centred care
- support and communication

The carer questionnaire (combined with the patient questionnaire) will elicit the views of carers, friends and family members about:

- the extent to which the ward has supported them in their role as a carer
- communication of the needs and preferences of the person they care for

The patient questionnaire (which can be completed with carer support) will ask about patients' experience of care during their time on the ward with a focus on:

- overall perceived quality of care
- recognition of the person as an individual

The staff questionnaire will provide feedback from staff about:

- awareness of dementia and how it might affect a person in their care
- support in caring for a person with dementia
- learning and development provided

1a. Submitting data

Data will be submitted via a secure section of the College website (https). The RCPsych has a bank level end-to-end SSL/Transport Layer Security with 128 bit encryption. Online audit tools used to collect the information required by the audit will be password protected. Passwords and usernames for participating hospitals will be held by the local audit lead.

Usernames and passwords will meet the standards specified in the NHS Code of Confidentiality:

- At least seven characters
- At least one numeral or special character
- At least two alphabetic characters
- At least one upper and one lower case character
- Not similar to login or user id
- Not shared with others except where individuals are specifically so authorised

2. Data processing

All information collected by the audit will be held securely and confidentially in the following locations

- a restricted area of the RCPsych server;
- a password protected and encrypted laptop issued by the RCPsych and protected with PGP software;
- an encrypted RCPsych issued memory stick (AES 256 BIT military level security).

Data will not be held in any of the following locations:

- Computer hard drives
- Personal network drives
- Any mobile device not issued by RCPsych
- Any non restricted area of the RCPsych servers

Web servers

RCPsych web servers are subject to physical access restriction, including 100% supervision, by RCPsych staff, of any contractors required to work in such areas. Monitoring software is in place to ensure that no unauthorised access to servers occurs.

3. Data reporting

Participating hospitals will receive local reports with their own results benchmarked against collated national data, where applicable. Results of individual participating hospitals will be shared only with that hospital, via the nominated audit lead.

The national report will include collated results from all modules together with evidence of local action planning and recommendations for future action.

Collated data sets may also be used for publication in academic journals or on our website.

No data or information which would lead to the identification of an individual or organisation will be included in any publications or reports without prior agreement in writing from the individual or organisation concerned during the period that audit data is managed by RCPsych (see below 4b).

4. Data storage and FOI

The data will be held on a restricted area of the server and will not be stored on laptops or desktops. PCs are password protected.

Access to all RC Psych web servers is restricted.

All College laptops are protected by advanced encryption software, the details of which are held by the IT office.

Industry standard commercial anti-virus protection is used to protect the College servers.

All memory sticks use 256 AES encryption. Encrypted memory sticks should be used whenever there is a need to access any part of the project data outside of College offices.

Back up tapes are encrypted to the highest level, transported in padlocked strong boxes, signed for on arrival and kept offsite in fireproof safes.

The College is subject to the provisions of the Freedom of Information Act where it collaborates with, or works on behalf of another organisation, which is so subject.

All information, data, audit tools and deliverables reverts to the full ownership of the funding authority, HQIP, at the end of the contracted period.

Data will be stored on behalf of HQIP by the Royal College of Psychiatrists for a minimum period of five years.

4a. Data transfer

Data should only be shared and transferred if appropriate and lawful to do so, by one of the following methods (see statement on Partners to the Audit, above).

- Saving in a restricted area of the project folder
- Emailing files in an encrypted format
- Using an encrypted memory stick or laptop
- Uploading on a secure website in an area that is accessible only using username and password.

4b. Retention and disposal of data

National Audit of Dementia data reverts to the full ownership of the funding authority, HQIP, at the end of the contracted period.

Data will be stored on behalf of HQIP by the Royal College of Psychiatrists for a minimum period of five years, in line with stated Department of Health requirements.

During this period data may be transferred to a further contractor for the purposes of re-audit, at the request of HQIP.

Any data so transferred will be collated data, for the purpose of benchmarking, and will not identify individuals or organisations.

This document was approved for use in February 2010. It will be reviewed on a yearly basis or as necessary, and any amendments published on the main web page of the project, contained within the Royal College of Psychiatrists' website (www.rcpsych.ac.uk).

Quick link:

www.nationalauditofdementia.org.uk