



Ethics, Consent & Confidentiality

The Child and Adolescent Psychiatry Surveillance System (CAPSS) and Patient Confidentiality

Summary

- CAPSS and the research teams involved in studies are unreservedly committed to preserving medical confidentiality in all aspects of their work.
- CAPSS requires study applicants to demonstrate their compliance with each of the eight principles outlined in the Data Protection Act 1998.
- CAPSS requires study applicants to demonstrate their compliance with the principles outlined in the Caldicott Report (1997).
- CAPSS requires study applicants to detail the security measures in place to protect patient confidentiality.
- CAPSS requires study applicants to apply to the Ethics and Confidentiality Committee of the National Information Governance Board for Section 251 approval (formerly PIAG for Section 60 approval).

1. Confidentiality in Law

In the UK there are a number of pieces of legislation that address confidentiality of personal information including Common Law, Data Protection Act 1998 and Human Rights Act 1998.

Common Law

In Common Law anyone who receives information must respect its confidentiality i.e. not disclose it without consent or other strong justification. Common Law enshrines the principle that to disclose confidential information about a living person without consent is, generally speaking, to wrong an individual. In law any information doctors have about their patients must be regarded as confidential. Common Law does however recognise that it can be in the public interest for doctors to disclose confidential personal information and that the nature and scale of the disclosure has to be balanced against the benefits to society. While Common Law establishes some core principles it does not specify when confidential information may or may not be disclosed to others in research or most other activities.

Data Protection Act 1998¹

If a living person (data subject) can be identified from any information in your possession this information is considered personal data. Personal data stored in computers and/or paper files (ward notes, X-rays, lab reports etc) is safeguarded by the Data Protection Act 1998. This places obligations on those who record or use personal data and gives certain rights to persons about whom information is held. The eight principles of the Data Protection Act are summarised as follows.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met; and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. 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.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. 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.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

Human Rights Act ²

The Human Rights Act 1998 allows UK citizens to assert their rights under the European convention on human rights in UK courts and tribunals and states that *"so far as possible to do so, legislation must be read and given effect in a way which is compatible with convention rights"*. The European Convention on human rights, so called "the Convention", was ratified by the UK in 1951 and enshrines a right to respect for individual private lives and

¹ Available at <http://www.opsi.gov.uk/acts/acts1998/19980029.htm>

² Available at <http://www.opsi.gov.uk/acts/acts1998/19980042.htm>

prescribes the circumstances in which it is legitimate for a public authority to interfere with the enjoyment of this right.

Caldicott Report

The Caldicott Report (1997) was a review commissioned by the Chief Medical Officer to make recommendations to improve the way the National Health Service handles and protects patient information.

The Caldicott Committee was set up to review the confidentiality and flows of data throughout the NHS for purposes other than direct care, medical research or where there is a statutory requirement for information. Its recommendations are now being put into practice throughout the NHS and in the Health Protection Agency.

The Caldicott report identified six principles, similar in many respects to the principles outlined in the *Data Protection Act*.

1. Justify the purpose(s) for using patient data.
2. Don't use patient-identifiable information unless it is absolutely necessary.
3. Use the minimum necessary patient-identifiable information.
4. Access to patient-identifiable information should be on a strict need to know basis.
5. Everyone should be aware of their responsibilities to maintain confidentiality.
6. Understand and comply with the law, in particular the Data Protection Act.

1.5 251TheNational Information Governance Board (NIGB)

The Health and Social Care Act 2008 established the NIGB as a statutory body. From January 2009, NIGB functions include administration of applications under section 251 of the NHS Act 2006. Section 251 allows the common law duty of confidentiality to be set aside in specific circumstances. This function was formerly carried out by the Patient Information Advisory Group (PIAG).

- Section 251 of the NHS Act 2006 came about because it was recognised that there were essential activities of the NHS, and important medical research, that required use of identifiable patient information, but that had no secure basis in law because patient consent for the use of personal and confidential information had not been obtained. It can only be used to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice. It is intended largely as a transitional measure while consent or anonymisation procedures are developed, and its use is reviewed annually.

- The Ethics and Confidentiality Committee, formerly the Patient Information Advisory Group (PIAG), was established to provide advice to the Secretary of State for Health involving the use of patient information. The terms of reference for the Ethics and Confidentiality Committee (ECC) can be found here <http://www.nigb.nhs.uk/ecc/about>: in essence the ECC has been established to consider ethical issues related to the processing of patient data and to consider applications under Section 251 of the NHS Act 2006. Its membership is drawn from patient groups, healthcare professionals and regulatory bodies.
- CAPSS will continue to work with the ECC to ensure that the studies conducted under its remit fulfil the obligations set down in Section 251 of the Health & Social Care Act.

2. CAPSS Methodology and Confidentiality

2.1 CAPSS Reporting Mechanism

Explicit patient consent is not sought. The CAPSS mechanism is shown Figure 1. Applicants wishing to undertake a surveillance study put forward a detailed protocol. Successful applicants are selected following a detailed, two-phase scientific review by the CAPSS Executive Committee, which has a broad multidisciplinary representation.³ Priority is given to conditions or issues of public health importance, conditions of low incidence and where near-complete reporting is required.

All studies have to be approved by an **Multicentre Research Ethics Committee (MREC)** and funding confirmed before it can be included on the CAPSS surveillance 'YELLOW' card.

Particular attention is taken to ensure that the patient information to be gathered by the investigator is the minimum necessary to allow for optimal case ascertainment matching and removal of duplicate case reports, contacting notifying clinicians and achieving the research objectives.

2.2. Maintaining confidentiality in CAPSS investigations

- Anonymised notifications are provided to the CAPSS office by members of the Royal College of Psychiatrists' (RCPsych) Research & Training Unit using CAPSS methodology i.e. the 'Yellow Card'. CAPSS informs the lead investigator or their nominated staff of the notifying member's details so the investigators can request further details.
- No patient identifiable information passes to CAPSS itself from the reporting psychiatrist.

³ Membership of the Committee includes consultant paediatric psychiatrists, paediatricians, and epidemiologists, as well as representatives of the Royal College of Psychiatry.

- Study investigators request the psychiatrist who has notified a case to CAPPS to complete a short 2-3 page questionnaire.
- The CAPSS Executive reviews in detail the questionnaire of each study. The Executive keeps to an absolute minimum the number of patient identifiable information fields. Some patient identifiable information is necessary to allow for case verification (including correspondence with the clinician who notifies the case) or matching and removing duplicate notifications, whilst other patient identifiers are an essential part of the clinical research data, for example dates of birth, sex and first part of postcodes.
- Questionnaires are structured so that the front page, which contains information only essential for case verification and de-duplication, can be separated from the remaining pages that contain clinical research data.
- Patients' identifiable data must be held in a secure location (e.g. a locked cabinet in a locked room) and on protected computer databases, e.g. using password or other security measures. This includes data that are archived once the study has been completed.
- Secure archiving of patient identifiable data should occur once the study is completed and destruction of data should take place after a specified time period (currently the MRC recommends data archiving for 20 years to allow re-appraisal of research data and to safeguard against fraud: www.mrc.ac.uk/pdf-pimr.pdf).

2.3. Ethical Approval

A CAPSS facilitated study must be approved by a MREC before it can commence.

2.4 ECC (PIAG) Application Form

- All CAPSS studies will have to complete an ECC application to obtain Section 251 support.
- Submissions can be made directly using the on-line IRAS forms.
- Approved applications are placed on the Section 251 Register.
- Approved applications are reviewed/renewed annually.