CAPSS Investigators Code of Conduct on Patient Confidentiality

1. Introduction

In what follows the term CAPSS refers to the system itself, its Executive Committee and studies conducted through CAPSS.

1.1 Much of the work undertaken through CAPSS involves the collection, analysis, reporting and storage of information on patients, including activities involved in communicable disease surveillance. In order to discharge these functions effectively it is often necessary for CAPSS to collect and process person-identifying health-related data.

1.2 Under their contracts of employment all employees have a duty to observe general rules regarding confidentiality of information concerning patients. To enable employees to meet this contractual requirement, consistent with also enabling CAPSS to discharge its functions as outlined in 1.1 above, employees should handle patient data in accordance with the principles contained in the Data Protection Act 1998, and also the "Caldicott Principles" which are outlined below.

2. Caldicott Principles

Employees of CAPSS and those employed to facilitate surveillance should ensure that patient-related information is handled in accordance with "Caldicott Principles" (outlined in the recommendations of the Caldicott Committee's Report on the Review of Patient-Identifiable Information, published in December 1997).

Principle 1 – Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from CAPSS should be clearly defined and scrutinised to ensure that there is no alternative to the use of such data; continuing use will be reviewed regularly by the CAPSS Executive, and the relevant "Caldicott Guardian" to ensure that the use remains justified.

Principle 2 – Don't use patient-identifiable information unless it is absolutely necessary. Patient-identifiable information items should not be used unless there is no alternative and its use is necessary for the medical management of the individual or for the protection of Public Health. Administrative convenience is not a reason for using such material.

Principle 3 – Use the minimum necessary patient-identifiable information where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

Principle 4 – Access to patient-identifiable information should be on a strict need to know basis. Only those individuals who need access to the patient-identifiable information should have access to it, and they should only have access to the items they need to see.

Principle 5 – Everyone should be aware of their responsibilities. All facilitators of CAPSS who handle patient-identifiable information (both clinical and non-clinical staff) should ensure that they are aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Understand and comply with the law.
Every use of patient identifiable information must be lawful. The principal investigator, as advised by CAPSS Executive and its Caldicott Guardian, is responsible for ensuring that the project as a whole complies with legal requirements.

3. Practical Measures

Management and staff at all levels are responsible for taking all reasonable steps when carrying out their normal day to day duties to ensure adherence to the Caldicott Principles on patient confidentiality, including:

- Arrangements for storage and disposal of patient information (manual and computerised) must protect confidentiality.

- Appropriate security measures to protect computer-based and manual information must be devised and installed.

- Care should be taken to ensure that unintended breaches of confidentiality do not occur e.g. by not leaving files, fax machines or computer terminals unattended, double checking to avoid transmitting information to the wrong person, not allowing sensitive conversations to be overheard and guarding against people seeking information by deception.

- Where a non-NHS agency or individual is contracted to carry out NHS or CAPSS facilitated functions the contract must draw attention to the obligations on patient confidentiality and require information to be treated and stored to specified standards and used only for the purposes consistent with the terms of the contract.

- Where anonymised information would be suitable for a particular purpose, patient-identifiable information should be omitted wherever possible.

- Patients who feel that confidentiality may have been breached should be advised to pursue any complaint through their NHS Trust Complaints Procedure.

4. Breaches of Confidentiality

Any alleged breach of confidentiality will be regarded as a potentially serious disciplinary offence, which will be investigated and dealt with formally under the guidelines of the NHS Trust or institute Disciplinary Policy and Procedure. Where the allegation is substantiated and found to constitute gross misconduct (e.g. where the breach is found to be deliberate) this will result in summary dismissal.

Disciplinary action short of summary dismissal may be appropriate in other circumstances. In any case where the breach of confidence is committed by a health professional, he/she may also be subject to action by the relevant regulatory/professional body e.g. GMC, UKCC, CPSM (HPC – Health Professions Council – with effect from 1 October 2000). Employees also have the right and duty to raise any concerns they may have about possible breaches of confidentiality by colleagues or clients. Employees who raise such concerns in good faith will not be penalised.

5. Training and Further Information and Advice

The principal investigator is responsible for ensuring that all employees are provided with appropriate information and guidance on patient confidentiality and specific arrangements for handling patient-related data e.g. during induction and on-the-job training programs. Employees have a duty to attend induction and other relevant training programs that are arranged for them.

Duty of confidentiality with regard to patient data

1 CAPSS and those who facilitate its use have a common law duty of confidentiality to patients and a duty to support professional ethical standards of confidentiality.

2 Every facilitator of CAPSS has a personal common law duty of confidentiality to patients and to CAPSS.

3 In addition, health professionals (including medical, scientific, nursing and technical staff) have, by virtue of professional regulation, an ethical duty of confidentiality.

4 Any alleged breach of patient confidentiality should be considered seriously. It needs to be reported to CAPSS Executive immediately. Any substantiated breach may lead to the termination of the surveillance project. ln addition, where the breach of confidence is committed by a health professional, he/she may be subject to action by the relevant regulatory/professional body.

5 Employees also have a right and duty to raise any concerns they may have about possible breaches of confidentiality by colleagues or clients. Employees who raise such concerns in good faith will not be penalised.