Code of practice 2 - handling of patient data

Processing patient data on computers attached to the College network.

1. It is recognised that some research, particularly clinical, requires the processing and/or storage of personal and sensitive information relating to living individuals e.g. patients. All such activity is governed by the Data Protection Act 1998 and members of College must comply with the Act and process/store all personal information in accordance with the eight Data Protection Principles shown at the end of this note.

2. It is a condition of Use of Information Technology (IT) Facilities at Imperial College that members of College may only process and/or store information relevant to their College work on computers, portables, desk-top or servers, attached, permanently or temporarily, to the College network. Examples of processing and/or storage include e-mail messages (whether stored locally, or on a College server), word processed documents, medical images, databases and Web pages. Processing of data for patient management purposes is not permitted on the College network or equipment connected to it.

3. With respect to the security of personal data (Principle 7 below) it must be noted that the College network is widely and legitimately accessible across the campus and from the internet via its connection to JANET. In terms of the processing and storage of personal data, the network must be regarded as being insecure, having no access restrictions. Consequently, any identifiable patient data stored on any computer connected to the academic network must be encrypted and/or secured behind an appropriate firewall. It is not sufficient to rely on normal system passwords. It is also not acceptable for unencrypted personal data to pass across the College network.

4. Information relating to the clinical management of patients under the care of an NHS Trust typically belongs to that Trust (and not to the individual clinician), irrespective of the usage to which the data is being put, i.e. clinical diagnosis or research purposes. However, in the latter case, the data may well be transferred to a third party, such as the sponsor of a study. Information obtained on patients and healthy volunteers specifically for the purpose of a research study, i.e. beyond normal clinical care, will belong either to the study sponsor or the investigator.

5. In all cases, it is a requirement of the Data Protection Act that the explicit consent of the Data Subject be obtained, by the Data Owner, before any such sensitive data are stored or processed. The Data Owner may be a Trust, a sponsor or the investigator. When seeking consent, Data subjects should be informed of the purposes for which it will be used, in accordance with the first principle, and the likely recipients to whom their information could be disclosed (e.g. the College if the data has been collected by the Trust). Where such data are to be processed on a computer connected to the College network, or passed across that network, a separate registration of the data must be made with the College Data Protection Officer through your Departmental/Divisional Data Protection Coordinator.

6. To summarise, data on living individuals e.g. clinical data, collected for whatever purpose, must not be stored or transmitted on the College network unless both registered and adequately protected to prevent disclosure of that data to unauthorised persons. This requires either that adequate security measures are in place or that the data are adequately anonymised. It should be noted that where the data has been codified there exist separate records, electronic or paper, which enable the individual to be ultimately identified, then that data is not fully anonymised and falls under the Act. Thus it must be registered, properly processed in accordance with the Act and adequately protected.