

THE NEWCASTLE UPON TYNE HOSPITALS NHS TRUST

PROCEDURE MANUAL

FOR

SECURITY AND PROTECTION OF PAPER-HELD

PATIENT INFORMATION

Version	1
Effective Date	2001
Revised	May 2007
Review Date	May 2008
Author	Liz Hogarth
Issue List and Date	

CONTENTS

- 1 Management of security.
- 2 Responsibility for security control of access to Libraries.
- 3 Security incident management.
- 4 Housekeeping.
- 5 Patient information.
- 6 Data Protection Act 1998
- 7 Disclosure of Information.
- 8 Medical Legal/Complaints investigation.

MANAGEMENT SUMMARY

The following is a policy relating to paper-held patients information. Confidentiality of such information is a national requirement of each Trust. The security preservation, retention and destruction of the said paper is based on the HSC 1999/053 Health Circular issued by the NHS Executive.

~~~~~

## **1 MANAGEMENT OF SECURITY**

The Clinical Records Advisory Committee (or appropriate committee) must ensure that the Trust identifies a Security Officer responsible for the safe-keeping and preservation of paper-held patients information.

The Security Officer to have a specific role and responsibilities.

The Clinical Records Advisory Committee should ensure that the internal systems and processes in place meet all requirements to safeguard information held on patients in a paper form.

Regular internal audits must be planned and undertaken to maximise awareness of all personnel involved in the management of patients and the handling of patients medical case folder.

The management of personal health records applies to all departments and professions within the hospital setting. There are legal requirements which must be met and various guidelines and good practice which should be adhered to when dealing with personal health records. Procedure manuals must be in place and known to staff and updated as required with changes to legislation etc.

All new permanent, temporary or agency staff into the Trust must be instructed in and sign a declaration on the correct keeping of patient's confidentiality (non disclosure) which includes paper held information as part of their contract of employment.

## **2 RESPONSIBILITY FOR SECURITY OF MEDICAL RECORDS LIBRARIES**

The Security Officer will be responsible to ensure the security of the medical records libraries and their access control.

Staff will only gain access to libraries by way of their ID staff badge/coded security lock following a request to the Security Officer and relevant clearance authorised.

The Security Officer will ensure that staff adheres to the access control policy by not allowing other individuals into an area via access by their ID pass or disclosure of the security code.

The Security Officer will make it known to all relevant staff that disciplinary procedures will be commenced if it is identified through access audit that staff have breached these rules.

Libraries will not be accessible to unauthorised personnel.

## **3 SECURITY INCIDENT MANAGEMENT**

The Security Officer will monitor the access security system, investigate any breach and take relevant action.

#### **4      HOUSEKEEPING**

The Security Officer will ensure that guidelines are in place and adhered to relating to the correct handling, filing and preservation of paper-held casenotes.

Information and guidelines relating to safe and correct security of data held in paper form in a patient's casenotes will be raised and discussed with relevant staff by the Security Officer.

The importance of correctly recording entries in a patient's case folder will be raised with all relevant staff. Handouts will be distributed to staff as guidelines.

Instructions relating to the correct transportation of casenotes both, internal and external, must be adhered to by all staff, guidelines will be circulated. The Security Officer will monitor this process and take relevant action if breaches are identified.

#### **5      PATIENT INFORMATION**

The Security Officer will endeavour to ensure that paper-held information recorded in a patient's casenotes will be accessed on a need to know basis only.

Unauthorised access will be dealt with under the Trust disciplinary procedure. The Security Officer will periodically circulate information on safe and correct handling of paper-held patient's records to raise awareness.

#### **6      DATA PROTECTION ACT 1998**

The Security Officer will ensure that compliance with the Data Protection Act 1998 is maintained.

Guidelines and relevant forms are available to all applicants relating to paper held medical records and used to process all requests. The Security Officer will ensure all departments are aware of this Act and have been circulated guidelines with instruction that all requests must be forwarded and handled by the Trust Medical Records/Out-patients Manager or Deputies.

#### **7      DISCLOSURE OF INFORMATION**

The Security Officer will raise awareness through relevant departments and give personnel strict instructions relating to disclosure of paper-held information. All staff must play their part in ensuring information is not disclosed to a third party even if that third party is a member of the patient's family without consent being gained from the patient or patients legal representative.

All staff must play their part in ensuring information is not disclosed or confidentiality breached by overheard telephone calls and discussion relating to data originating from a paper- held casenote.

Any paper held information or documents which identifies a patient must be disposed of using the appropriate confidential waste sack and not in a waste paper basket.

PASSING ON INFORMATION TO HELP PREVENT, DETECT OR PROSECUTE IN THE CASE OF SERIOUS CRIME WILL BE THE RESPONSIBILITY OF THE SECURITY OFFICER OR DESIGNATED DEPUTY FOLLOWING APPROPRIATE CLARIFICATION.

## **8      MEDICAL LEGAL/COMPLAINTS INVESTIGATION**

The Security Officer, through the Trust Chairman and members of the risk management group, will endeavour to ensure that paper-held information relating to all elements of a patient's care whilst in the Trust is correctly recorded and available for inspection. All relevant personnel involved in recording details in a patient's casenotes are made aware that to change, delete or amend an entry in a patient's casenotes that becomes part of a litigation or complaints investigation, is a criminal offence and may result in criminal proceedings against the identified person.

If you require assistance with any aspect of the security of paper-held records, please contact the Trust Nominated Data Protection Officer on Ext. 37360.

**Approved:**                      **Mrs E A Hogarth**  
                                            **Trust Medical Records/Out-patients Manager**

**Revised Date:**              **May 2007**