


STANDARD OPERATIONAL POLICY & PROTOCOLS

TOPIC	CONFIDENTIALITY, SECURITY AND MANAGEMENT OF INFORMATION	Identifier 24.02
AUTHORISED BY	CHIEF EXECUTIVE OFFICER	
VERSION NO.		1.8
EFFECTIVE DATE	SEPTEMBER 2002	
REVIEWED	JULY 2009	
LAST REVIEWED	APRIL 2013	
REVIEW DATE	APRIL 2016	
RESPONSIBILITY	IMPROVING PERFORMANCE COMMITTEE	
DISTRIBUTION	ALL AREAS	
SIGNED AUTHORISATION		DATE 14/04/13

1. PURPOSE

East Grampians Health Service (EGHS) is committed to protecting the confidentiality of residents and consumers (including patients, clients, employees, volunteers and contractors) personal information.

2. POLICY OUTCOMES

Systems are in place to ensure a patient's/resident's personal (including health) information, and other confidential information related to the management of the organisation, is safeguarded against loss, unauthorised access and use, modification or disclosure.

All information both health and non-health, created by hospital personnel is to be assessed in accordance with the associated procedures so that a security classification can be applied immediately it is recognised that the information is Sensitive Material.

A comprehensive, effective security management programme that complies with relevant State legislation and Australian Standards will ensure the safety and protection of:

- patients and others
- drugs, other controlled substances and other dangerous goods
- information and
- other property, including money, owned by, or in control of the facility and the property of patients, staff and others within the facility.

For the purpose of this document, 'patient' is defined as an inpatient, resident or client of EGHS.

3. DEFINITIONS

Records, files and documents are any written materials obtained, created or maintained by the hospital stored by either paper or electronic media and includes:

- personnel records and documents
- cashier's records and documents
- patient records
- purchasing and supply tender documentation
- legal agreements and other contracts and
- other administrative documents (i.e. minutes)

Classified Information is a generic term which describes information that has been identified as requiring protection to minimise the risk of it being acquired by personnel not authorised to receive it (i.e. to minimise the risk of it being lost, stolen or compromised) and which has been graded for receipt of an appropriate level of protection.

Sensitive Material is material that the unauthorised disclosure, loss, compromise, misuse or damage of which would cause harm to the hospital, staff member, patient, or agency; cause serious harm to any person, agency or government which provided information to the hospital under an assurance or expectation of confidentiality; or which would breach a statutory requirement to protect that material; or give an unfair advantage to any individual, group or organisation.

4. RESPONSIBILITIES

The Chief Executive Officer shall:

- Ensure that sensitive information maintained by the hospital is appropriately classified and receives the appropriate corresponding level of protection as delegated by the Board President.

The Unit Manager/Department Head shall:

- Co-operate with the classification of information policy.
- Ensure that all staff who handle hospital information are familiar with the requirements of this policy.
- Confirm the classification assigned to sensitive information by employees within their area of responsibility.

The Employee shall:

- Co-operate with EGHS to maintain a secure work environment.
- Comply with the requirements of this policy and associated procedures to assess and classify sensitive hospital information.

5. PROTOCOL

5.1 Classification of Information

Information is to be classified in accordance with the associated procedures using the criterion of the estimated degree of harm the unauthorised disclosure, loss, compromise or misuse would cause. 'Sensitive Material' will be classified as either 'IN-CONFIDENCE' (several types), 'PROTECTED' or 'HIGHLY PROTECTED'.

The level of classification assigned to information within the hospital should be periodically assessed to reaffirm it still warrants the level held and therefore the level of protection provided.

Access shall be restricted according to the security classification of the classified information and the level of approval or security clearance particular staff members have in order to access that material.

Staff shall be given approval to access sensitive material at the levels of:

- "Staff-in-Confidence" (Personnel Records)
- "Medical-in-Confidence" (Medical Records)
- "Commercial-in-Confidence" (Management Information, including business strategies, marketing plans, negotiations, meeting minutes, contracts and tenders, etc)
- "Protected" (any of the above, but at a higher level of sensitivity and/or criticality)
- "Highly Protected" (staff, medical or commercial information of the highest level of sensitivity or criticality).

Classified material acquired or created by the Health Service shall be stored under secure conditions.

All classified and/or sensitive material no longer required by the Health Service and which is not required to be preserved by statutory regulation shall be disposed of by the approved process for the Health Service. (Note that the law may require that psychiatric and some other records be held indefinitely and are not destroyed).

No documentation, records or files maintained by the Health Service (classified, sensitive or otherwise) shall be destroyed without the express permission of the Unit/Department Manager or their delegate. Refer to Records Management - SOPP 24.03.

5.2 Personal / Health Information

Health information will be collected in a lawful and sensitive manner according to the Health Records Act 2001 and Information Privacy Act 2001.

- Personal information is information or an opinion, which can be used to identify a person in any form.
- Sensitive information relates to;
 - Ethnicity/cultural background
 - Religion
 - Political opinions

- Union / Association membership
- Criminal record
- Health information relates to:
 - A person's health or disability related to the past, present, future
 - A person's expressed wishes about future health services
 - Health services provided or to be provided to a person
 - Ongoing record of planned care, outcomes of care and all treatment provided

All personal information whilst providing acute/community/allied/aged care etc. is referred to as Health Information with respect to patients/residents.

5.3 Confidentiality

- Any member/s of staff/volunteers who is/are engaged in conversation by a member/s of the public regarding EGHS, or any decisions made by the Board regarding the Health Service, shall inform such person/s to address their concerns to the Chief Executive in writing. Such staff member/s shall not enter into discussion regarding the Health Service and decisions made by the Board.
- Any staff member who is bothered by members of the public in relation to decisions made by the Board should refer the matter to the Chief Executive.
- Promotion of EGHS in a positive light is the responsibility of all staff, and this should be remembered in all discussions both within and outside the Health Service. Refer to Privacy - SOPP 26.01.

5.4 Privacy

Refer to Privacy - SOPP 26.01

5.5 Staff Personal Information

- Systems are in place to ensure staff information is safeguarded.
- Refer also to Privacy - SOPP 26.01.
- Staff phone numbers must not to be given to any person outside the organisation.
- No information about the hospital or its staff, either directly or indirectly, is divulged to any person, who does not, in the duty of care, need to know.
- No statements shall be made to the media without the explicit authority of the Chief Executive.

5.6 Collection of Information

- Wherever possible information is collected from the individual patient.
- Implied or expressed consent is required when collecting health information. On admission, staff must ensure each patient or representative is aware of the purpose of collection, use and disclosure of information, the protection and use of your health information brochures answering questions and the patient or representative is asked to sign the consent to use and disclosure of information form. This form is then filed in the patient's/resident's admission notes.

- Staff must organise a suitable interpreter for patients from non-English speaking background. Refer to Managing Cultural and Linguistic Diversity - SOPP 60.18.
- Refer to Privacy - SOPP 26.01

The authorised representative may be:

- Enduring Power of Attorney – (Financial)
- Enduring Power of Attorney (Medical)
- Enduring Guardian
- Guardian appointed by the Victorian Civil and Administrative Tribunal (VCAT).
- Person with written authority by the resident to provide access
- Guardian

5.7 Quality of Data

- Refer to Clinical Care Documentation - SOPP 58.15.
- Refer to Patient Client Health Record - SOPP 25.01.
- Refer to Documentation in Health Record - SOPP 25.03.

5.8 Disposal/Destruction of Records

- Refer to Records Management - SOPP 24.03

5.9 Storage of Confidential Information

- Staff are to ensure filing cabinets and storage rooms/facilities containing confidential information, are locked when unattended
- Whiteboards/documents with patient/resident details should be located in areas where privacy is maintained
- Computers with access to confidential information should be 'locked' when unattended

5.10 Privacy, Confidentiality & Security Agreement

- Refer to Privacy Confidentiality Security Agreement - 26.01.08 - to be signed by all new staff to EGHS, contractors, volunteers and students.

5.11 Secondary Storage/Archived Confidential Information

Health/personal/organisational information, of a confidential nature, is stored in secure locations, accessible for medico-legal or Freedom of Information.

All records, no longer stored in main filing areas, must be boxed with destruction date marked clearly on front of archive box and description of contents. (See Attachment 1)

If departments have no allocated secondary storage, records must be kept securely within the department until storage space can be allocated.

No records are to be placed in secondary storage without approval from the Health Information Manager.

6. RELATED DOCUMENTS

Policies:

[CLINICAL CARE DOCUMENTATION - SOPP 58.15](#)

[DOCUMENTATION IN HEALTH RECORD - SOPP 25.03](#)

[MANAGING CULTURAL AND LINGUISTIC DIVERSITY – SOPP 60.18](#)

[PATIENT CLIENT HEALTH RECORD - SOPP 25.01](#)

[PRIVACY - SOPP 26.01](#)

[RECORDS MANAGEMENT - SOPP 24.03](#)

Forms:

[Consent to Use and Disclosure of Information – Day Centre – 26.01.04](#)

[Consent to Use and Disclosure of Information – District Nursing – 26.01.02](#)

[Consent to Use and Disclosure of Information – Inpatient – 26.01.01](#)

[Consent to Use and Disclosure of Information – Resident – 26.01.05](#)

[Privacy Confidentiality Security Agreement - 26.01.08](#)

[Protection and Use of Your Health Information – BRA05](#)

[Protection and Use of Your Health Information – Day Centre – BRA06](#)

[Protection and Use of Your Health Information – Emergency Department – BRA07](#)

[Protection and Use of Your Health Information – Radiology – BRA09](#)

[Protection and Use of Your Health Information – Resident – BRA08](#)

7. REFERENCES

Aged Care Act 1997, Division 62-1, 62-2, 86-1-9, 88-1-3, 89-1, Records Principles 1997, 19.1-19.6.

Brooks, J. 2002, Residents Records, Privacy, Confidentiality and Information, lecture notes, 18/03/02, Melbourne.

DHFS 1998, *Standards and Guidelines for Residential Aged Care: St. 1.8.*

Public Record Office, *Retention and Disposal Authority for Patient Information Records* PROS11/06

Health Record Act 2001

Information Privacy Act 2001

AS2828.1:1985 Medical Record Content

AS2828.1:1985 Hospital Medical Records

AS/NZS 7799.2:2000 Information Security Management

AS 4390.1-4390.6 Records Management

Health Service Act 1988

EQUIP 5 Criterion 2.3.4

A/Care Standard 1.8

National Safety and Quality Health Service Standards – Standard One

Attachment 1

Department:

HEALTH INFORMATION

Description:

**DECEASED RECORDS
2005**

Destruction Date:

**TO BE DESTROYED
2017**