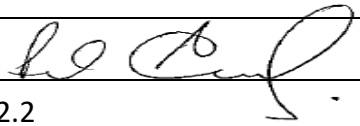
STANDARD OPERATIONAL POLICY AND PROCEDURES

TOPIC	Confidentiality, Security and Management of Information – SOPP 24.02		
RESPONSIBILITY	Improving Performance Committee		
AUTHORISATION	Chief Executive		
SIGNED		**DATE**	22/11/2021
VERSION	2.2	**LAST REVIEWED**	November 2021
EFFECTIVE	September 2002	**NEXT REVIEW**	November 2024

1. PURPOSE

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

To ensure that EGHS provides safe high quality health care and experiences to our consumers by actively following the Victorian Clinical Governance Framework and through its Community Participation Framework to actively engage and partner with consumers.

2. POLICY OUTCOMES

Systems are in place to ensure consumers 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 if it is recognised that the information is sensitive material.

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

- Consumers and others.
- Drugs, other controlled substances and other dangerous goods.
- Information.
- Other property, including money, owned by, or in control of the facility and the property of consumers, staff and others within the facility.

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;
- Consumer's records;
- Purchasing and supply tender documentation;

- Legal agreements and other contracts; and
- Other administrative documents (e.g. 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 (e.g. 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, consumer, 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

All staff are responsible and accountable to know, understand and support each other to meet the requirements of the Victorian Clinical Governance Framework. All staff will be aware of the Community Participation Framework and actively engage and partner with consumers, demonstrate ownership and accountability of quality and safe care, and participate in regular evaluation and monitoring of performance to inform improvement.

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:

- Cooperate 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:

- Cooperate 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.

Classified material acquired or created by the health service shall be stored under secure conditions. Access shall be restricted to ensure material is only available to the appropriate staff members.

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 Privacy and Data Protection Act 2014.

- 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.
    - Sexual preferences or practices.
    - 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.
- Any staff member who is approached 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.
- All persons, including EGHS staff, contractors, volunteers and students who come into contact with, or have access to, confidential information have a responsibility to maintain the privacy, confidentiality and security of that information. Refer Privacy Confidentiality Security Agreement - 26.01.08.

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. Refer to Media-Public Relations – SOPP 7.05.

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.
- Medical Treatment Decision Maker.
- Guardian appointed by the Victorian Civil and Administrative Tribunal (VCAT).
- Person with written authority by the resident to provide access.
- Guardian.
- A parent of an individual, if the individual is a child.

An authorised representative does not include:

- A person acting as an authorised representative of the individual if that acting is inconsistent with an order made by a count or tribunal.

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 Access to and 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 must be 'locked' when unattended and generic passwords should not be used.
- Staff must not share their password under any circumstance, allow other staff to use a computer that they are logged into and they are responsible for all transactions performed under their login.
- Staff are to be provided access to IT systems in accordance with the requirements of their role as approved by their Manager and/or the Manager of Health Information Services. When a staff member changes roles, access to IT systems/confidential information must be reviewed and changes made as required.
- Access to and use of confidential information will be audited on a regular basis and changes will be made as deemed appropriate by Department Heads/Manager of Health Information Services.
- Refer to Privacy Confidentiality Security Agreement - 26.01.08.

5.10 Privacy, Confidentiality and 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

Refer to Records Management - SOPP 24.03.

6. RELATED DOCUMENTS

Clinical Care Documentation - SOPP 58.15

Documentation in Health Record - SOPP 25.03

Managing Cultural and Linguistic Diversity - SOPP 60.18

Media-Public Relations – SOPP 7.05

Patient/Client Health Record - SOPP 25.01

Privacy - SOPP 26.01

Records Management - SOPP 24.03

Consent to Use and Disclosure of Information - Patricia Hinchey Centre - MR093.3

Consent to use and Disclosure of Information - MR092.15

Privacy, Confidentiality and Security Agreement - 26.01.08

Protection and Use of Your Health Information – BRA05

Community Participation Framework

7. REFERENCES

Health Record Act 2001

Data Protection and Privacy Act 2014

AS/NZS 7799.2:2000 Information Security Management

AS ISO 15489.1:2017 (ISO 15489-1:2016)

Health Service Act 1988

Australian Commission on Safety and Quality in Health Care. National Safety and Quality Health Service Standards guide for hospitals. Sydney: ACSQHC; 2017.

Delivering high-quality healthcare, Victorian clinical governance framework. Melbourne: SCV; 2017.

Australian Government Aged Care Quality and Safety Commission. Aged Care Quality Standards. July 2018.