PRIVACY, CONFIDENTIALITY AND SECURITY AGREEMENT

As part of my position/contract I am required to understand and agree to the following:

1. I WILL ONLY access information I need to perform my duties.
2. I WILL NOT disclose, copy, release, sell, alter or destroy any confidential information unless it is part of my contract. If I am required to do any of these tasks, I will follow the correct procedure (such as putting confidential papers in appropriate security bins or using EGHS faxing guidelines).
3. I WILL NOT misuse or be careless with confidential information.
4. I WILL NOT disclose my personal computer passwords and will only use shared passwords in authorised situations.
5. I ACCEPT responsibility for all activities undertaken using my password.
6. I KNOW that my access to confidential information may be audited.
7. I WILL NOT remove confidential information (eg. medical records, photocopied patient forms or electronic data) from EGHS unless it is an authorised work practice.
8. I WILL report any activities to my manager / contract supervisor that I suspect may compromise the confidentiality of information. I understand these reports, made in good faith, will be held in confidence to the extent permitted by law.
9. I WILL wear my identification badge at all times whilst on EGHS premises.
10. I WILL protect the privacy of EGHS patients and employees.
11. I AM RESPONSIBLE for my use or misuse of confidential information.
12. I UNDERSTAND my obligations under this Agreement will continue after termination of my contract.

I am aware that failure to comply with this agreement may result in the termination of my contract at EGHS and/or civil or criminal legal penalties.

By signing this, I agree that I have read, understand and will comply with this agreement:

Signature: _____ Date: _____

Print Name: _____ Department: _____

ORIGINAL – to be signed and held in employee record within Human Resources/Administration

PHOTOCOPY – to be held by employee/volunteer/contractor etc

26.01.08 – V1.3 – Mar 13

PRIVACY CONFIDENTIALITY AND SECURITY AGREEMENT

EGHS is committed to complying with relevant privacy, confidentiality and security legislation to protect our clients; our staff; and our organisation. As part of this, individuals are required to understand their obligations and responsibilities, including what it means to sign this agreement.

For all persons, including East Grampians Health Service staff, contractors, suppliers, volunteers and students

East Grampians Health Service

improving the health of our community

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.

Confidential information may include information relating to:

- PATIENTS / CLIENTS / RESIDENTS AND / OR THEIR FAMILY MEMBERS

  Such as medical records, conversations and financial information

- EMPLOYEES, CONTRACTORS, VOLUNTEERS, STUDENTS

  Such as salaries, employment records, disciplinary actions

- BUSINESS INFORMATION

  Such as financial records, reports, memos, minutes, contracts, computer programs, technology

- THIRD PARTIES

  Such as vendor contracts, computer programs, technology

- OPERATIONAL IMPROVEMENT, QUALITY ASSURANCE, PEER REVIEW

  Such as reports, presentations, survey results

To assist EGHS in complying with legislation a range of policies and procedures have been developed and implemented. Staff and contractors are encouraged to make themselves aware of the content of the policies.

Further information

If you have any questions or concerns relating to privacy, confidentiality or security of information whilst at EGHS contact:

Manager, Health Information Services
Health Information Services
East Grampians Health Service
5252 9300

Examples of Breaches

NOTE: *These are examples only. They do not include all possible breaches of privacy, confidentiality or security covered by this agreement. Staff should read and understand relevant EGHS policies and procedures.*

What You Should Not Do!

Accessing information that you do not need to know to do your job:

- Reading of a client's medical record or an employee file without authorisation.
- Searching of Patient Master Index for familiar names.
- Accessing information on family, friends, co-workers or yourself.
- Reading pathology/radiology results of family, friends, co-workers or yourself.

Divulging personal information without individual's consent:

- Discussing or "gossiping" about client details in situations unrelated to direct patient care.
- Conducting a conversation relating to client or staff information in a public place.
- Telling a relative or friend about a client or patient you have seen.
- Discussing confidential information in a public area such as a waiting room, elevator or cafeteria.
- Divulging information via electronic means – e.g. social media, text

Sharing, copying or changing information without proper authorisation:

- Making unauthorised changes to a client's medical record.
- Making unauthorised changes to an employee file.
- Copying and forwarding client or staff information to a third party without having verbal or written consent.

Sharing your password:

- Telling a co-worker your password so that they can access your work.
- Telling an unauthorised person the access codes for employee files or client accounts.
- Using unauthorised shared passwords.

Using another person's password:

- Using a co-worker's password to log in to the Hospital's computer system.
- Use of a password to access employee files or client accounts without authorisation.
- Using a co-worker's application for which you do not have rights after he/she is logged in.

Disclosing client information without following EGHS guidelines:

- Faxing without including a fax cover sheet.
- Disclosing unauthorised client details over the phone.
- Emailing sensitive papers and information

Leaving a secure information system (ie: System that is password protected) unattended while logged on:

- Being away from your desk (eg. tea or lunch breaks) while you are logged into a secure system.
- Allowing a co-worker to use a secure system for which he/she does not have access after you have logged in.