Policy Name	Clinical Information Access Policy		
Policy Number		**Version Number**	2
Effective Date	Jan 1, 2005	**Retirement Date**	
Last Review Date		**Next Review Date**	
Authorising Post	CIO, CEO	**Policy Folder**	
Sub-folder:			

Purpose

To ensure clinical information is accessed only by the appropriate and authorized users.

Policy

1. All persons who have access to Cerner (including employees, private practitioners, consultants (of any type) shall sign the Patient confidentiality agreement prior to being given a username. This agreement shall be kept in Human Resources in the individual's file. If the person is not an employee it will be kept in HR in a separate file for non-employees in alphabetical order by last name. (Exception: Cerner personnel who are providing technical assistance from overseas are covered under the contractual agreement.)
2. Usernames will be created only after IT is notified in writing by HR (for employees,) by HPB / CMO (for private clinicians,) and by management for consultants. PPE, local and contracted end users shall be given an open ended effective date. All other user names shall have a specified end date of the end of their contract or if that is not known, 6 months.
3. No one should enter a record on behalf of another person unless his or her job description would also give him or her privilege to view that information. (i.e. personnel who are not on the compound should not ask users to look up information on a patient unless that user is also caring for that patient.)
4. The staff in one department should only access the records of the patients on that unit and should only have patient lists for the units on which they work.
5. Each user is only to view what they need to see to do their job. Health care providers are restricted to entering records of patients they are caring for. Management and resource personnel are restricted to accessing record for specific investigations only. (e.g. incident investigation, staff evaluations, not to gain medical knowledge about staff members.)
6. Audits of chart access should be done on a monthly basis.
7. Failure to comply with the confidentiality agreement and clinical information access policy will result in disciplinary action.

Procedures

1. Audits of chart access to be done on a monthly basis.
    a. An IT Analyst is to run a 'Chart Accessed by Provider' report for randomly selected users per department on a monthly basis. (Found in Explorer Menu – Main Menu – Core Security Audits – Chart Accessed by Provider) These audits will be forwarded to the appropriate supervisor for verification of appropriate access to records. No one is exempt from this audit.
    b. Section supervisors and managers are to randomly audit patient's charts to check on the person or persons viewing patient's information in their department. Persons accessing records inappropriately shall be reported to the appropriate manager/ HR.

c. The STI nurse will monitor the persons who are entering the HIV patient's charts and report any inconsistencies to the appropriate manager.

d. Audits received by a supervisor/manager of that department will be reviewed for appropriate access by the end user. The end user will receive a report of that audit and may view the report (but not keep it) regardless of the results of the audit. All audits to be treated as confidential information and filed or shredded appropriately.

8. Disciplinary process for inappropriate access to patient records.

   a. First offence of inappropriate access – written notice to the end user by manager with copy on file and manager to request audit of access by that user from IT for the next 3 months.

   b. Second offence of inappropriate access - written report to head of department and HR. Manager to request audit of access by that user from IT for the next 3 months.

   c. Third offence – Username to be inactivated. HR to take disciplinary action. (i.e. Reassignment to non clinical post, suspension or dismissal.)

   d. If any of the first three offences involve multiple charts accessed inappropriately, immediate referral to HR for disciplinary action.

Cross-references

Forms

Confidentiality agreement (attached)

Signatures

Authorising Post Title	Name (Print)	Signature	Date

CONFIDENTIALLY AGREEMENT

As an employee of the Health Service Authority I consider that patient and employee information from any source and in any form (i.e paper, electronic) is confidential and as such will do everything possible to protect the privacy and confidentially of this information.

I may see or hear confidential information on:

- PATIENTS AND /OR FAMILY MEMBERS
  Such as patient records, conversations and financial information
- EMPLOYEES, VOLUNTEERS, STUDENTS ETC
  Such as salaries, employment records, disciplinary actions
- BUSINESS INFORMATION
  Such as financial records, reports, memos, contracts, HSA computer programs, technology
- THIRD PARTIES
  Such as vendor contracts, computer programs, technology
- OPERATIONS IMPROVEMENT, QUALITY ASSURANCE,,PEER REVIEW
  Such as reports, presentations, survey results

I further understand that access to this information is allowed ONLY if I need to know it to do my job.

I HEREBY AGREE TO THE FOLLOWING:

1. I WILL ONLY access information that I need to do my job.
2. I WILL NOT show, tell, copy, give, fax, email, sell, review, change, trash or distribute in any other manner any confidential information unless it is part of my job. If it is part of my job to do any of these tasks, I will follow the correct department procedure (such as shredding confidential papers before throwing them away).
3. I WILL NOT misuse or be careless with confidential information.
4. I WILL KEEP my computer password secret and I will not share it with anyone.
5. I WILL NOT use anyone else's password to access any Health Service Authority system.
6. I AM RESPONSIBLE for any access using my password.
7. I WILL NOT share any confidential information even if I am no longer a Health Service Authority employee.
8. I KNOW that my access to confidential information may be audited.
9. I WILL tell my supervisor if I think someone knows or is using my password.
10. I KNOW that confidential information I learn on the job does not belong to me.
11. I KNOW that the Health Service Authority may take away my access at any time.
12. I WILL protect the privacy of our patients and employees.
13. I WILL NOT make any unauthorized copies of Health Service Authority's software.
14. I AM RESPONSIBLE for my use or misuse of confidential information.

Failure to comply with this agreement may result in the termination of my employment at the Health Service and/or civil or criminal legal penalties. By signing this document, I agree that I have read, understand and will comply with this agreement.

Signature:_____ Date: _____

Print Full Name: _____ Unit/Section: _____

Examples of Breaches of Confidentially
To be given to the Signer.
(What you should not do)

These are examples only. They do not include all possible breaches of confidentially covered by this policy and the agreement.

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

- Unauthorized reading of patient account information.
- Unauthorized reading of a patient's chart.
- Accessing information on your self, children, family, friends or co-workers.

Sharing your sign on code and password:

- Telling a co- worker your password so that he or she can log into your work.
- Telling an unauthorized person the access code for employee files or patient accounts

Leaving a *secured application unattended while signed on:

- Being away from your desk while you are logged into an application**.**
- Allowing a co-worker to use your *secured application for which he/she does not have access after you have logged in.

**** secured application =*** *any computer program that allows access to confidential information. A secured application usually requires a user name and password to login*

Sharing, copying or changing information without proper authorization:

- Making unauthorized remarks on a patient's chart.
- Making unauthorized changes to an employee file.
- Discussing confidential information in a public area such as a waiting room or elevator.

Using another person's sign-on code and password:

- Using a co-workers password to log into the Computer system.
- Unauthorized use of a log-in code to access employee files or patient accounts.
- Using a co-workers application for which you do not have rights after he/she is logged in.