

Yee Hong Centre for Geriatric Care

Developer: DCD	Division: Corporate	Category: Corporate Administration	Policy Number: CAD-VI-02
Effective Date: July 2004	Subject Name: Privacy - Confidentiality		Approval: CEO
Reviewed/Revised Date: March 2010	Next Review Date: March 2011	Supersedes: CGA-III-15	Pages: 1 of 3

PURPOSE

Breach of privacy or confidentiality is a serious offence and places the organization at risk. This policy specifically addresses the maintenance as confidential of:

- All personal health information (PHI) handled by the Yee Hong Centre for Geriatric Care (YHC) as Health Information Custodian, and staff as agents of the organization.
- Corporate information concerning corporate finance and other proprietary planning activities deemed to be sensitive in nature.

POLICY

1. YHC is committed to protecting the privacy and the confidentiality of all PHI collected in the course of transacting YHC business.
2. All individuals (employee, physician, volunteer, student, vendor, contractor, researcher, consultant, and affiliated service provider) associated with YHC must be committed to maintaining the privacy and confidentiality of our clients and staff and their associated PHI
3. Corporate information deemed to be sensitive or proprietary is not to be divulged without authorization by the appropriate manager.
4. This policy is not intended to impose such excessive restraint as to discourage efficient communication and work processes. Instead it sets contextual guidelines within which individuals should exercise reasonable and sound judgement in handling information concerning others' right to privacy and the proprietary nature of specific organizational information.

PROCEDURES

1. All individuals entering a relationship with YHC must sign a confidentiality agreement. This agreement will be placed in the appropriate file and subject to be reviewed or renewed at regular intervals (with annual performance or contract review).
2. Confidential information about the organization, its clients, donors, and/or employees shall not be divulged to anyone other than persons who are authorized by YHC to receive such information.

3. The release of information on employees' employment record and salary shall only be done by Human Resources following a written consent by the employee.
4. When an individual is in doubt as to whether certain information is confidential, no disclosure should be made without first seeking appropriate management approval and/or consulting the Corporate Privacy Officer, as applicable. This basic practice of caution and discretion in handling confidential information extends to both internal and external disclosures.
5. Confidential information obtained as a result of employment or association with YHC is not to be used by any individual for the purpose of furthering private interests, or as a means of making personal gains.
6. Students may have direct access to charts or records of specific clients only while participating in authorized direct client contact personally or with their instructors.
7. All client identification must be removed to ensure the anonymity of the client when the information is used for seminars, case studies, or other teaching purposes. At no time may a client be made identifiable without his/her consent.
8. Use of PHI for purposes of research must adhere to provisions of the Quality Care Information Protection Act of Ontario, and the provisions approved by the YHC Research Standards and Review Committee.
9. Where staff is authorized to access the YHC Data Network, staff is responsible for ensuring his login password is kept confidential, and that he logs out of the system after each active episode of use.
10. In the course of their function to maintain the information technology system and address hardware and software technical issues Information Services (Technical) Staff might be in a position to access private and confidential data e.g. in human resources or clinical files, and PHI of clients or staff. They are expected to refrain from viewing and divulging to others information they are inadvertently exposed to in such instances.
11. In situations where multiple electronic data repositories are accessible via shared software or software licenses – e.g. Monitor Pro
 - 11.1 Specific management staff members are authorized to view and work with selected data sets – e.g. staff vs. clinical records – for human resources management, quality improvement, and other purposes.
 - 11.2 They are to refrain from viewing data not specifically relevant to their work tasks but which might be accessible within the context of shared information technologies.
12. In the context of a police investigation or another government agent requesting access, confidential PHI concerning clients/residents is only released where a court issued warrant, subpoena, or equivalent legal document authorizing access has been presented.

13. Disclosure or improper use of confidential information, including accessing PHI without authorization and without a need-to-know, can result in disciplinary measures up to and including termination, and civil or criminal penalties.