CONFIDENTIALITY GUIDELINES
FOR
CANADIAN OCCUPATIONAL HEALTH NURSES

March 17, 2004
Committee Members

COHNA-ACIIST gratefully acknowledges the following members of the Alberta Occupational Health Nurses Association (AOHNA) for their contribution to the original AOHNA document.

Ruth Anstruther
Pat Bayliss
Delores Brisbois
Sharon L. Chadwick
Susan Ens
Toni Fluker
Margie Garner

2002 Review committee
Barb Sonnenberg
Connie Pietrzyk-Cook
Grace Bowditch

The AOHNA guidelines were reviewed and revised to meet the needs of the national association by the following members of the COHNA-ACIIST Executive and Board of Directors:

Sharon L. Chadwick - Alberta
Brenda Marsh – Nova Scotia
Eleanor Gilding – British Columbia
Alexis Lloyd - Manitoba
Manon Legresley – New Brunswick
Jane Lemke - Ontario
Jane Deters - Saskatchewan
Lise Brasszard - Quebec
Natalie Dinn – Newfoundland and Labrador

Published by the Canadian Occupational Health Nurses Association/Association Canadienne des Infirmieres et Infirmiers en Sante du Travail (COHNA/ACIIST)
www.cohna-aciist.ca

Care has been taken to confirm the accuracy of information presented in this guideline. The authors and COHNA/ACIIST however, cannot accept any responsibility for errors or omissions or for the consequences from application of the information provided in this guideline and make no warranty, expressed or implied with respect to its contents.

© Copyright 2004, Canadian Occupational Health Nurses Association/Association Canadienne des Infirmieres et Infirmiers en Sante du Travail (COHNA/ACIIST)
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Definitions</td>
<td>4</td>
</tr>
<tr>
<td>Components of a Confidentiality Policy</td>
<td>5</td>
</tr>
<tr>
<td>The Policy Statement</td>
<td>5</td>
</tr>
<tr>
<td>Employee Health Record Considerations</td>
<td>6</td>
</tr>
<tr>
<td>Guidelines for Charting</td>
<td>6</td>
</tr>
<tr>
<td>Access and Ownership of Employee Health Records/Information</td>
<td>7</td>
</tr>
<tr>
<td>Access</td>
<td>7</td>
</tr>
<tr>
<td>General Guidelines for Access to Health Information</td>
<td>8</td>
</tr>
<tr>
<td>Disclosure of Information Without Authorization by the Employee</td>
<td>10</td>
</tr>
<tr>
<td>Storage, Retention, and Disposal of Employee Health Records</td>
<td>11</td>
</tr>
<tr>
<td>Storage</td>
<td>11</td>
</tr>
<tr>
<td>Retention</td>
<td>14</td>
</tr>
<tr>
<td>Disposal</td>
<td>15</td>
</tr>
<tr>
<td>References</td>
<td>17</td>
</tr>
<tr>
<td>Website Resources</td>
<td>18</td>
</tr>
<tr>
<td>Appendix A: Sample Pledge of Confidentiality</td>
<td>19</td>
</tr>
<tr>
<td>Appendix B: Sample Release of Employee Health Information Form</td>
<td>21</td>
</tr>
</tbody>
</table>
CONFIDENTIALITY GUIDELINES FOR OCCUPATIONAL HEALTH NURSES

INTRODUCTION

Occupational health nurses (OHNs) have a professional responsibility to maintain confidentiality of health information. This is supported by provincial and federal privacy and health information legislation, and nursing or health professions legislation across Canada. Employers and legal processes are increasingly challenging confidentiality. This can place OHNs in a position of conflict with their employer, the union, and employees. Reviewed and updated in 2002 to reflect current legislation, the Alberta Occupational Health Nurses Association (AOHNA) established a task force to develop guidelines for confidentiality for nurses in the occupational health setting. These guidelines were reviewed and adapted for use nationally by the Canadian Occupational Health Nurses Association/ Association Canadienne des Infirmieres et Infirmiers en Sante du Travail (COHNA/ACIIST) in 2004. These guidelines are not binding, but are intended to give general answers to possible questions on the appropriate handling of employee health information.

As specific legislation related to confidentiality varies federally and provincially, it is recommended that OHNs review all relevant provincial and national documents that may be applicable to their professional nursing practice.

DEFINITIONS

Confidential information: This includes all personal information regarding an employee received by the OHN in the course of duties that is not public knowledge and becomes part of the health record (e.g. preplacement health assessments, physician's certificates, rehabilitation progress, laboratory tests, personal family history, employee assistance program feedback, counselling, etc). The principles of confidentiality regarding the employee's health record apply equally to verbal and written information. Information that is not recorded is subject to the confidentiality provisions and can only be used or disclosed for the purpose for which it was provided i.e. verbal.

Confidentiality: The right of individuals to have all information about themselves released only to those to whom they have consented either expressly or impliedly (Picard, 1986). The conditions under which the obligation may be breached are usually determined by laws that vary from one jurisdiction to another (Nova Scotia Occupational Health Nurses Association, 1992).

Personal Information Protection and Electronic Documents Act (PIPEDA): applies to employee information in federal works, undertakings, and businesses.

Privacy Act: applies to employee information in federal government institutions.
COMPONENTS OF A CONFIDENTIALITY POLICY

COHNA/ACIIST strongly recommends that occupational health nurses assist in the development of a policy and associated procedures on confidentiality of employee health information at their worksites. To ensure confidential handling of health information COHNA/ACIIST recommends that written policies and procedures encompass right of access, release, transmittal and storage of all health information.

Senior management approval is critical in the development process. The essential components for such a policy are:

- policy statement
- employee health record considerations
- access and ownership of employee health records/information
- storage, retention, and disposal of employee health records/information
- disciplinary action for violation of the policy
- appendices which include forms for access to and release of employee health information, a pledge of confidentiality, and any legislation pertaining to the setting

THE POLICY STATEMENT

A policy statement should include:

1. title of the policy and type (e.g., Confidentiality - corporate or departmental policy); approval date and authority approving policy
2. employer identification (Name of the Company)
3. purpose (i.e., a general statement of philosophy and the reason for the policy)
4. scope/application of the policy
5. list of contents of the policy
6. references
EMPLOYEE HEALTH RECORD CONSIDERATIONS

1. Access to the health record is limited to medical and nursing professional staff and designated staff of the occupational health service who have a bona fide need to such access. Staff who have access to the employee health records are required to understand and sign a Pledge of Confidentiality (Appendix A).

2. All health information pertaining to the employee should be contained in individual Occupational Health files. These files must be stored in a manner that incorporates physical safeguards to prevent reasonably anticipated unauthorized access.

3. The employee health record must contain the minimum amount of information necessary to prove that adequate observation and/or intervention took place.

4. The OHN's written information in the employee health record will be used to evaluate the quality of nursing care that was provided. Clear, accurate, and timely charting will provide better legal protection.

5. The employee health record is a legal document and must not be altered or destroyed.

Guidelines for Charting

1. Record, preferably in black ink, in chronological order, at the time of the event, or at the earliest opportunity.

2. Each entry should be preceded by the date and time and signed using the legal signature and title of the person making the notation.

3. Do not erase a mistake. Mark through the error to indicate a mistake was made, initial, and recopy the notation correcting the error. Do not paste in notes or use correction fluid.

4. Never insert notes between lines or leave an empty space where someone else could insert a note. If there is an empty space, put a line through it so no one else can write in it.

5. Use only accepted, standardized abbreviations referenced in the corporate procedure manual. These should be developed with medical and company-specific standard abbreviations.

6. Each OHN must do her/his own charting.

7. Avoid general terms, and quote the employee's own words where possible.

8. Ensure that each page of the employee health record is properly identified with the employee's name.
9. The OHN should document on a need-to-know basis and include all information relevant to the service provided.

10. The amount of charting detail is dictated by nursing and medical practice standards which address:
- the complexity of the health problem;
- the degree to which the employee's job puts him/her at risk in the workplace; and
- the degree of risk involved in the treatment or care provided (clarify/justify the reason for care).

11. Record every contact made with an employee such as injuries, illnesses, immunization, laboratory test, blood pressure readings, counselling services, employee assistance counselling, and medications administered.

ACCESS AND OWNERSHIP OF EMPLOYEE HEALTH RECORDS/INFORMATION

Right of Access

1. Access is the release of health information to the individual that is the subject of that health information. This is also known as “right of access” (Health Information Act, 2001).

2. “Access is the right and opportunity to examine, be informed, to copy and to transmit information” (Occupational Health Nurses Association of Nova Scotia, 1992, p.3).

Ownership

Property ownership does not give right of access. The content of the employee health record enjoys joint ownership between the health professional who developed the information and the employee. The OHN or physician controls access and disclosure of health information, and they are custodians of all employee health records.

Property ownership in Canadian law indicates that actual physical employee health records including paper, computer discs, and computer hardware are the property of the employer (Occupational Health Nurses Association of Nova Scotia, 1992). In Alberta, the physical property of the record belongs to the agency that compiled the data (Alberta Association of Registered Nurses, 1986).

Access to the employee health record in the occupational health setting is limited to medical and nursing professional staff and to designated staff of the occupational health service who have a bona fide need to such access. Staff who have access to the employee health records should be required to understand and sign a Pledge of Confidentiality document. (Refer to Appendix A).
Physical access to the employee health record is restricted by the use of a locked filing system in a secured area of the occupational health service.

**General Guidelines for Access to Health Information**

1. An individual (employee) has a right to access any part or all of their health record (Krever, 1980).

2. Access by and release to any other individual can only be made with the employee's informed, written consent.

3. Disclosure of specific health information should be authorized by **written** consent of the employee and should include:
   - signature of the employee requesting the release of information as well as the signature of the witness;
   - date of the request;
   - name and description of the recipient of the information;
   - name and description of the person or institution intended to release the information;
   - a description of the specific health information to be disclosed (Appendix C);
   - purpose for which the information is requested and how it is to be used;
   - an expiration date or time limit for the validity of the authorization;
   - a statement indicating that the client may rescind or amend the authorization in writing at any time prior to the expiration date, except where action has taken place in reliance on the authorization. (See Appendix B.)

4. It is recommended that the OHN remain with the record during access by the employee for reasons of interpretation and to assist with clarification and understanding.

5. The employee may also have a witness in the viewing of the record; however, a signed statement by the employee that they have requested this witness should be entered into the record.

6. During access, the employee may submit notations of objections to the contents of the record by way of a letter to the file (Krever, 1980).
7. The general right of access to medical records is not absolute. The Alberta Hospitals Act (Province of Alberta, 1995a) is structured to allow patients access to their medical information, but gives the institution and physician the right to refuse. The Health Information Act (Province of Alberta, 2001) is structured to allow denial of access which may occur if the responsible health professional believes it is not in the patient’s/employee’s best interest to inspect the medical records, or if access may endanger the health and safety of a third party. In cases of denial, the onus is on the responsible health professional to justify the reason for denial of access. **Check the legislation that applies to your jurisdiction.**

8. The court system must provide appropriate written authorization for access to health records. A signed court order or written consent from the employee is required.

9. Alberta provincial legislation allows for release of confidential employee medical information to the Workers' Compensation Board (WCB). This information must be requested in writing and be deemed to be necessary and relevant to the claim. Specific diagnosis of an ailment can only be released to WCB if the treatment relates to the worker's occupation (Krever, 1980). **Check your local WCB legislation regarding release of employee medical information.**

10. When information is forwarded to the WCB, a copy of the medical information should be offered to the employee (Krever, 1980).

11. Where a claim is transferred from Workers' Compensation to a claim under disability benefits, the claimant must be advised and his or her consent be obtained before this health information is transferred (Krever, 1980).

12. Where a nurse is operating in a non-traditional role, it must be clear whether there is a nurse-client relationship. Some OHNs are involved in claims management, which requires claims adjudication for the purposes of allocating benefits and medical payments by determining eligibility. OHNs in this role (which requires sharing information with insurance carriers) must be clear with clients that no nurse-client relationship exists (Anderson, 1995; Ontario Occupational Health Nurses Association, 1994). Disability management is a proactive process to minimize the impact of injury, disability, or disease on a worker's capacity to successfully perform his/her job (Shrey & Lacerte, 1995). OHNs need to ensure that their role in disability management (which differs from claims management) meets professional nursing practice standards and that confidentiality is maintained.
Disclosure of Information Without Authorization by the Employee

Disclosure of information without authorization by the employee may occur under the following circumstances:

1. when there is an exchange of information between the Medical Services Department of the Workers' Compensation Board and the Alberta Government Workplace Policy and Standards branch that relates to the epidemiology of industrial diseases and of particular disabilities suffered by claimants (Alberta WCB Act, 1995d)

2. when an injury occurs, the Alberta Occupational Health and Safety Code, Part First Aid, requires an exchange of information about the injury between the employer and the Workers' Compensation Board to establish responsibility of the claim (WCB Act, 2002);

3. where there are statutory requirements to disclose information that falls under the Public Health Act and/or the Alberta Occupational Health & Safety Act for the designation of notifiable diseases. The Alberta Occupational Health and Safety Code defines specific diseases for which notification must take place in accordance with Section 22 of the Alberta Occupational Health and Safety Act, RSA 2002 Chapter 0 to 2);

4. when child abuse is suspected;

5. in accordance with a court order during the course of legal proceedings;

6. when public interest or safety overrides the duty of confidentiality because of a clear danger to the employee, to fellow employees, or the public (Province of Alberta, 1983).

NOTE: Each individual case may be open to interpretation, and the OHN may be required to seek legal advice before making a decision.
STORAGE, RETENTION, AND DISPOSAL OF EMPLOYEE HEALTH RECORDS

Storage

**Hard copy:**

1. Health records and information must be kept in a secured area and not left unattended in areas accessible to unauthorized individuals.

2. Employee health records must be maintained separately from general personnel files.

3. Keys should be held only by the custodian of the records (i.e., the OHN, occupational health physician, and other authorized health staff).

**Electronic:**

Increasingly, employee health information is being stored and transmitted electronically. To protect the interests of the employees and employer, employers should have written policies in place that clearly state their expectations and requirements related to the use of e-mail (Tapp, 2001). The following guidelines are designed to assist OHNs who use this media.

1. **Access:**
   - Not recommended as a method of transmission for health information (Tapp, 2001).
   - Only persons who would normally have access to employee health information should have such access when information is available on computer.
   - A second area of concern is the introduction of e-mail messages as evidence in a court of law (Tapp, 2001).
   - E-mail messages are another type of document and if they are relevant can be subject to disclosure in legal proceedings (Tapp, 2001).

2. **System Security:**

   A copy of the security policy should be available to all users and may include:
   - Terminals must be located in a manner so that the screen cannot be readily viewed by an unauthorized person.
   - An active terminal must not be left unattended.
   - The computer system should be programmed to log off after a period of non-use (e.g., 30 minutes)
   - Programs should be logged off at the end of the day.
   - All disks and hard drives containing records must be backed up on a daily basis.
   - All disks must be cleaned before disposal.
○ All disks must be cleaned for viruses before being used.
○ Disks should be stored in a locked cabinet under the care of the OHN.

○ A pledge of confidentiality must be signed by each person given authorized use of the system as an acknowledgement of the rules and regulations that are associated with the issuance of an identification and password. This includes systems maintenance individuals.

○ Each user should be issued a password that will authenticate the user. All users should realize the importance of not sharing passwords.

○ Each user should be issued an identification which will designates which information she/he may access.

○ Three sign-on attempts using invalid passwords should cause the identification to be disabled until restored by the system support person.

General Security:

○ Terminals must be located in a manner that an unauthorized person cannot readily view the screen.

○ An active terminal must not be left unattended. The computer system should be programmed to log off after a period of non-use (eg. 30 minutes).

○ Programs should be logged off at the end of the day.

○ All disks and hard drives containing records must be backed up on a daily basis.

○ All disks should be cleaned before disposal.

○ All disks must be checked for viruses before being used.

○ Disks should be stored in a locked cabinet under the care of the OHN.

○ Audits:

○ A system that allows information input errors to be corrected and additions to be made must be in place to ensure data integrity.

○ The system must identify such changes, the date, and the person making the change.

○ An occupational health professional should be designated as the only person granting access to automated information. They should be responsible for periodic auditing to ensure compliance.
5. Electronic Mail Systems:

○ Such a system can be used to transmit employee health information (e.g., a report of fitness to a supervisor). The person receiving the information should have a personal vs. shared identification, and the sender should ensure a copy of the transmission is kept. An informed consent for release of information is required regardless of the media used to transmit the information.

6. Facsimile Transmissions (Fax):

To reduce the risk of faxing personal information:

○ All guidelines regarding consent to release information apply to materials being faxed.

○ Develop a policy on the copying, retention and destruction of facsimile documents.

○ Fax only personal information that must be transmitted immediately. Send other urgent information by hand. Fax may be used when the original document or mail-delivered copies are not required.

○ Always confirm that the receiver has taken appropriate precautions to prevent anyone else from seeing the faxed documents. Fax only from and to machines located in secure or restricted access areas.

○ Faxes should be sent either by the OHN or by a designated person who understands proper procedures for the handling of confidential material.

○ Arrangements should be made to have an identified individual present to receive the information at a specified time (Grant, 1996).

○ Before sending a fax, check that the receiver's number is correct, then verify in the machine's display window that you have keyed it in correctly.

○ If you must send personal information, always complete the fax cover sheet, clearly identifying both sender and intended receiver. The cover sheet should include a warning that the information is intended for the named recipient only, as well as a request to contact you if the transmission was misdirected.

○ Call the recipient to verify that he or she received the complete transmission.

○ Consider making one individual responsible for the fax machine. Otherwise, limit the chances that passers-by can see personal documents by sending the documents yourself. Arrange a time to receive faxes containing personal information so you can be at the machine as they arrive.

○ Fax only the personal information that you would feel comfortable discussing over the
telephone.

- If your fax machine is equipped, use the feature requiring the receiver to enter a password before the machine will print the fax. This ensures that only the intended receiver can retrieve the document. Similarly, ask the sender to make sure that you must supply a password to retrieve the document.

- If you are sending personal information by a fax modem (a fax device contained in a computer), confirm that other users of the computer system cannot get access to the fax without a password. Likewise, if you are expecting information by fax modem, ensure that other users of your system cannot access the information without a password.

If someone asks you to fax his or her own personal information?

- Explain how faxing personal information can result in it being accidentally disclosed or deliberately intercepted by other people.

- Explain the risks and the precautions you have taken to reduce the risks. Ensure the person consented before you fax personal information.

**Retention**

1. Federal and provincial statues and regulations may specify length of storage.

2. Retention policies should be established when a health service is offered to employees.

3. In some companies, worker health records are kept for either twenty years from the date of last entry or for a total of forty years, whichever is longer.

4. Legal requirements for some types of health records are outlined in some provincial occupational health and safety legislation. OHN’s should be familiar with the requirements in the area where they are practicing. For example the Alberta Occupational Health and Safety Act, Regulation and Code require:

   - audiometric test results (audiograms) be kept until a worker terminates employment with the employer.

   - first aid records be kept three years or if in a record book three years after the date of the last entry.

5. The Treasury Board of Canada sets Federal guidelines. These are presently under review.
Disposal

1. Authorized Destruction:

   This should include method of destruction, who gives authorization, and what needs to be done after a specified retention time.

   - It is recommended that authorized destruction of all information in the health record be by effective shredding, burning, or erasure as in electronic storage.

2. Company Downsizing or Closure:

   - When a corporate structure is closing a subsidiary occupational health service, the employee health records may be forwarded to another health care professional (e.g., at the head office or another subsidiary occupational health service).

   - If the Occupational Health Service is closing, but the company still employs senior management, the records may be left secured at the site and should be the responsibility of the senior management official of the company. The OHN or physician should provide a letter of direction and agreement to the senior manager outlining the manager's responsibility to maintain the employee health records in a confidential manner, i.e., no employee health information shall be accessed or released by the manager without the written consent of the employee. This letter of agreement should be signed by both the occupational health nurse or physician and the senior manager. (Talisman Energy Inc., 1993). Employees should be advised of this agreement, and a copy of this agreement should be forwarded to the health and safety committees.

   - If the company is closing completely, the employees concerned should be given the opportunity of having a copy of the record and/or having the record forwarded to a personal physician or physician of choice. The records should otherwise be destroyed by effective shredding, burning, or erasure of the automated records (Alberta Association of Registered Nurses, 1986).

   - If any of the above is not viable, the OHN or physician should express concerns in writing to the employer and the employees.
3. Transferring Employee Health Records to a New Health Care Professional:

○ When health care professionals change within an agency or health service, written consent of the employee is not generally required.

○ When the service or agency providing the occupational health service is changed, written consent should be obtained from the employee for the transfer of records to the new health care service or agency (Talisman Energy Inc., 1993).
REFERENCES


WEBSITE RESOURCES

Canadian Nurses Protective Society for CNA members: http://www.cnps.ca/index_e.html

CNPS' assistance is available free of charge to those nurses who are, or were at the time of an occurrence, permit holders or members in good standing of one of the following nursing associations / colleges: AARN NANNB RNANT/NU SRNA CRNNS YRNA CRNM ANPEI RNAO ARNNL

Canadian Nurses Association (CNA) Privacy of Personal Health Information: Position Statement: http://www.cna-nurses.ca/_frames/search/searchframe.htm


Privacy Commissioner of Canada: http://privcom.gc.ca/information/guide_e.asp

Privacy Commissioner of Canada: Privacy Legislation in Canada Fact Sheet: http://privcom.gc.ca/fs-fi/02_05_d_15_e.asp

Privacy Commissioner of Canada: Privacy in the Workplace Fact Sheet: http://www.cnps.ca/index_e.html

Privacy Commissioner of Canada: Application of PIPEDA to Employee Records Fact Sheet: http://privcom.gc.ca/fs-fi/02_05_d_18_e.asp

Privacy Commissioner of Canada: Faxing of Personal Information Fact Sheet: http://privcom.gc.ca/fs-fi/02_05_d_04_e.asp
APPENDIX A

Sample Pledge of Confidentiality
SAMPLE

Pledge of Commitment to Confidentiality

In recognition of the ethical requirement for confidentiality in the delivery of medical- or health-related services, and to maintain the trust and co-operation of employees, I hereby affirm that I will:

1. treat as confidential whatever personal or health information is learned about an individual.

2. treat as confidential all information contained within an employee's occupational health record.

3. not disclose such health information except:
   * as authorized by the informed consent of the employee;
   * as required by law; or
   * where there is a serious and imminent risk that the health or safety of the employee or others would be jeopardized.

4. abide by the policy and guidelines regarding confidentiality.

This agreement is to be signed when an employee first joins the department.

Signature: ________________________  Date: ________________________
APPENDIX B

Sample Release of Employee Health Information Form
ABC COMPANY
OCCUPATIONAL HEALTH SERVICES

Authorization For Release of Confidential Medical Information

TO: (Name of authorized occupational health person and address)

You are hereby authorized to release information from the confidential medical/health records of:

NAME:__________________________________________________________

EMPLOYEE ID NUMBER:__________________________________________

DATE OF BIRTH:________________________________________________

INFORMATION TO BE RELEASED:

_________________________________________________________________

_________________________________________________________________

PURPOSE:________________________________________________________

_________________________________________________________________

RELEASE TO:

NAME:__________________________________________________________

ADDRESS:________________________________________________________

DATE:_________________________ EXPIRY DATE:______________________

SIGNED BY:_____________________ RELATIONSHIP:____________________

EMPLOYEE OR LEGALLY AUTHORIZED REPRESENTATIVE

ADDRESS:________________________________________________________

SIGNATURE OF WITNESS:_______________ RELATIONSHIP:_______________

ADDRESS:________________________________________________________

Authorization must be signed by the employee or by the legally authorized representative in the case of certified mental incompetence or death. This consent may be rescinded at any time prior to expiration date at request of the employee, except where action has been taken in reliance on the authorization.