

OCCUPATIONAL AND ENVIRONMENTAL SAFETY & HEALTH OPERATIONAL PROCEDURE

Subject: Employee Health Records

Effective Date: September 2010

Supersedes: March 2007

Review Date: 3 years or legislation or job changes

Original Signed by: Diane Gantzel, Director, WRHA Occupational and Environmental Safety & Health

1.0 Guiding Principles

- 1.1. The documentation system should provide a user-friendly platform that enables authorized health team members to access, enter and use employee health information. The system should enable team members to demonstrate their professional practice standards. (CRNM – Standard I: Professional Responsibility and Accountability).
- 1.2. Quality documentation is crucial to demonstrating that nursing care was reasonable and prudent and met the *Standards of Practice for Registered Nurses*. The documentation system must reflect the expectation that registered nurses competently apply their knowledge to assess, plan, intervene, and evaluate employee health outcomes. It must allow the recording of the pertinent information used to make clinical decisions. (CRNM – Standard II: Competent Application of Knowledge)
- 1.3. Quality documentation demonstrates the application of current knowledge, clinical skills and judgment and also acknowledges limitations. Documentation of the planning, development, implementation and evaluation of care articulates what care was given and why it was given. The documentation system must accommodate the recording of situations that are referred or reported to other members of the health care team (e.g. information provided when a physician is notified regarding a patient's condition). The documentation system should support adequate documentation of situations of risk (e.g. document all incidents in the event that care provided is challenged in a formal or informal process). (CRNM – Standard III: Competence in Nursing Practice).
- 1.4. Quality and timely documentation facilitates safe care and demonstrates the accountability of health care providers. It should enhance continuity of care and employee confidence in care providers. Appropriate documentation share knowledge and enables care providers to work together with the employee to provide optimal care. (CRNM – Standard IV: Communication and Collaboration).
- 1.5. Documentation of shared objectives, employee choices, and other ethical standards demonstrate meeting the Canadian Nurses Association *Code of Ethics for Registered Nurses*. The documentation system should communicate the expectation that the employee's choices

and decisions are recorded. If an employee makes a choice that may jeopardize his or her health, it is crucial to document pertinent information that led to this decision, including what information was given to the employee and whether the employee was adequately informed about risks, and what measures were taken to ensure that the employee had the necessary knowledge. The documentation system should be designed to ensure a secure location for the health record. Employee information should only be disclosed when the employee had the necessary knowledge. The documentation system should be designed to ensure a secure location for the health record. Employee information should only be disclosed when the employee has given consent or when required by a court or as otherwise permitted by legislation.
(CRNM – Standard V: Ethical Practice).

2.0 Definitions

2.1. Confidentiality: A condition under which information is not disclosed by a person or organization to others. Preserving confidentiality is one means by which an organization protects the privacy of individuals.

2.2. Personal Information:

2.2.1. *Personal Health Information:* All information, recorded or exchanged verbally, about an employee that relates to:

- The employee's health, or health care history, including generic information about the employee or the employee's family.
- The provision of healthcare to the employee, or
- Payment for health care provided to the employee, and includes
- The PHIN and any other identifying number, symbol or particular assigned to an employee, and
- Any identifying information about the employee that is collected in the course of, and is incidental to, the provision of health care or payment for health care.

2.2.2. *Other Personal Information:* Other information may include:

- The employee's personal information, including financial position, home condition, domestic difficulties, work performance or any other private matters relating to the employee which have been disclosed to staff or persons associated with Occupational and Environmental Safety and Health (OESH) or WRHA, and at the discretion of the OHN has been incorporated into the Occupational health file.

2.3. Occupational Health Record: A confidential, cumulative account of health information for each employee. Individual health records include employee-specific documentation of occupational injuries and illnesses, occupational and medical health histories, results of pre-placement and periodic health examinations, laboratory results, health surveillance results, immunizations, disability information and documentation of episodic care.

2.4. Privacy: The right to be left alone. In practical terms, it is the ability of individuals to control access to their personal information in the custody or under the control of others through accountability, consent, security, right or access, and regulation.

- 2.5. Secured Place:** A physical environment for the temporary or permanent storage of, or for the use, processing or transmittal of personal health information that has the following characteristics:
- Not readily accessible by unauthorized users
 - Supervised or monitored by authorized users
 - Keyed to allow entrance to authorized users only
 - Locked when authorized users are not in attendance
 - Protected by controls to minimize loss, destruction or deterioration caused by fire, water, or humidity damage; and
 - Proper containers and adequate labeling are used to reduce accidental loss or destruction.
- 2.6. Security:** The processes, tools and measures used to:
- Identify threats and risks to the confidentiality or integrity of information, and
 - Implement administrative, physical and technological means to combat those threats and risks.
- 2.7. Trustee:** A health professional, health care facility, public body, or health services agency that collects or maintains personal health information.
-

3.0 Responsibilities

- 3.1. Occupational Health Nurses (OHN's) have a professional responsibility to act competently and ethically, and be accountable for their own nursing practice. It is the responsibility of all registered nurses in Manitoba to understand the standards of practice and apply them to their own nursing practice, regardless of roles or practice settings (*CRNM Standards of Practice for Registered Nurses, 2004*).
- 3.2. WRHA OESH personnel are responsible to ensure that recorded personal health information will be properly secured and maintained in the appropriately secured record, and shall be kept in a Secure Place at all times manner to protect its confidentiality and integrity. (see WRHA Policy No. 10.40.120)
- 3.3. Security safeguards shall include both physical and human resource safeguards to prevent unauthorized personal health information collection, use, disclosure and access. (see WRHA Policy No. 10.40.120)
- 3.4. The OHN should consult with a PHIA Privacy Officer if uncertain how to respond to situations involving employee personal health information.
-

4.0 Operational Procedure

4.1. Collection of Personal Health Information:

- 4.1.1. The Occupational Health Nurse should limit the amount and type of information collected to the least amount of health information necessary to meet the needs of their Occupational Health function. (see WRHA Policy No. 10.40.070)
- 4.1.2. Personal Health Information should be collected directly from the employee.

- 4.1.3. Occupational Health Nurses need to notify the employee about the Occupational Health purposes of collecting information before the information is collected or as soon as possible afterwards.

4.2. Documentation of Employee Health Information:

- 4.2.1. All health information pertaining to the employee should be contained in properly labeled, individual records, and/or in an electronic system and kept in a Secured Place in the occupational health setting.
- 4.2.2. Recorded information should be objective, accurate, timely and easily retrievable by authorized personnel.
- 4.2.3. The Occupational Health record must contain sufficient information necessary to demonstrate that adequate observation, assessment and/or intervention took place.
- 4.2.4. The written information in the employee health record may be used to evaluate the quality of nursing care that was provided. Clear, accurate, and timely charting will provide better legal protection.
- 4.2.5. The employee health record is a legal document and must not be altered or destroyed.
- 4.2.6. Each nurse must do his or her own charting.

4.3. Recordkeeping – General

- 4.3.1. Record, preferably in black ink, in chronological order, at the time of the event, or at the earliest opportunity. Diagrams should be used in recording for clarification and to assist in describing injury location and size.
- 4.3.2. Each entry should be preceded by the date and time and signed using the legal signature and title of the person making the notation.
- 4.3.3. Mistakes should not be erased. 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.
- 4.3.4. 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.
- 4.3.5. Avoid general terms, and quote the employee's own words where possible.
- 4.3.6. Ensure that each page of the employee health record is properly identified with the employee's name.
- 4.3.7. 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 of care provided (clarify/justify the reason for care).
- 4.3.8. Record every contact made with an employee such as injuries, illnesses, immunization, laboratory test, blood pressure readings, counseling services, employee assistance counseling, and medications administered.
- 4.3.9. All information pertaining to employee contact, whether in person or by telephone or e-mail, must be maintained in the employee health file.
- 4.3.10. All e-mail notes that are added to an employee's chart must be dated with the date received or sent and noted on the occupational health record.

4.4. Storage and Disposal of Records

- 4.4.1. An employee's personal health information that has been submitted to an employer shall be contained in the Occupational Health record. An employee's medical note containing personal health information should never be maintained by a manager or supervisor but must be forwarded to OESH.
- 4.4.2. Employee health information stored in electronic form on a fixed computer server or terminal shall be properly secured from unauthorized access. Employee health information stored on electronic media shall be kept in a secured place at all times and shall be used only by authorized personnel having access to a protected system. Any hardware or software contained employee health information must be secured or removed before equipment is discarded or reassigned to a non-OESH site. (see WRHA Policy No. 10.40.120)
- 4.4.3. Individuals who sign on to a computer containing personal health information must not leave the computer on in areas accessible by unauthorized persons when they leave their workstation. User password protocols must be in place and utilized. Where possible, automatic shut offs after a prescribed period of disuse should be programmed for all workstations (see WRHA Policy No. 10.40.120).
- 4.4.4. All employee health information that is mailed through regular postal service, interdepartmental mail or sent via courier must be marked Confidential and have reasonable safeguards put in place to ensure security and integrity of the information.
- 4.4.5. Employee health information shall not be transmitted via electronic mail without appropriate safeguards such as encryption or transmittal within a secure firewall where practicable (see WRHA Policy No. 10.40.120).
- 4.4.6. Persons leaving voice messages containing personal health information should be discreet. Personal health information should never be left on an employee's voicemail unless the individual whom the information is about has authorized it. Any personal health information relayed by voice message should be kept to the minimum required for the purpose of communication and should be recorded on the employee health record. Persons receiving voice messages containing personal health information should listen to the message in private, document the message in the employee health record and delete the message as soon as possible. Appropriate passwords and security measures should be in place for access to voice mail.
- 4.4.7. Fax machines shall be located in a Secured Place where they can be used and monitored only by authorized persons. A cover sheet, using the approved WRHA logo, should be attached to all documents stating that the transmittal is confidential and that any unintended receiving party is prohibited from reading or disclosing the information to anyone else (see WRHA Policy No. 10.40.130).
- 4.4.8. Reasonable precautions to protect employee health information from fire, theft, vandalism, deterioration, accidental destruction or loss and any other hazards shall be taken.
- 4.4.9. All confidential material shall be disposed of by incineration, shredding or other approved method of disposal. (see WRHA Policy No. 10.40.090)
- 4.4.10. All confidential material requiring disposal shall be stored, transported, shredded or incinerated in a secure manner.

4.5. Disclosure of Health Information

- 4.5.1. Employee health information will be disclosed on a “need –to-know” basis.
- 4.5.2. If consent is obtained from an employee to disclose personal health information only disclose the least amount of information necessary in the circumstances to meet the purpose of the consent.
- 4.5.3. Disclosure of specific health information should be authorized by written consent of the employee and should include:
- The signature of the employee requesting the release of information
 - 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
 - The purpose for which the information is requested and how it is to be used or disclosed
 - An expiration date or time limit for the validity of the authorization
 - A statement indicating that the employee 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.
 - The OESH Release of Medical Information Confidential form should be completed to obtain immunization record information (see Appendix 1).
 - The WRHA Consent to Disclose Personal Health Information should be completed for disclosure of other personal health information. (form #W-00332 04/10) (see Appendix 2 – see also: http://home.wrha.mb.ca/privacy/phia_forms.php).
- 4.5.4. A record should be kept and shall be placed in the employee health record, which shall identify the personal health information disclosed. The disclosure record may be in the form of a note in the employee’s health record, a facsimile cover sheet, log books, routine routing or documents, or cc’s identified on the document, as long as the sender is able to identify what personal health information was disclosed, and to whom, if the need should arise, along with a copy of the consent.
- 4.5.5. The OHN can disclose the following health information to an employee’s manager/supervisor without written consent:
- Fitness to work
 - Notice that a medical condition exists and that the employee is under medical care
 - Time that the employee has been and is expected to be off work
 - Medical restrictions on the type or amount of work or specific tasks to ensure employee safety and effectiveness.
- 4.5.6. The OHN may receive requests for disclosure of personal health information without the employee’s consent (ie. legal, regulatory body requests). In all such cases the request must be co-ordinated by the Site Privacy Officer or WRHA In-House Legal Counsel (see WRHA Policy No. 10.40.142 and 10.40.140). The information disclosed should be limited to the extent the recipient needs to know the information.

4.6. Access to Personal Health Information:

- 4.6.1. The employee may request to examine and receive a copy of his or her employee health information maintained by OESH. This is done by completion of the WRHA Request to Access Personal Health Information Form (#W-00330 04/10) (see Appendix 3 – see also : http://home.wrha.mb.ca/privacy/phia_forms.php).

- 4.6.2. The OHN should determine if there is any reason to refuse access to personal health information (see WRHA Policy No. 10.40.040 Section 3.7)
- 4.6.3. The OHN must respond to a request as promptly as possible, but no later than 30 days after receiving it. The OHN shall make every reasonable effort to assist an individual making a request by responding without delay, openly, accurately and completely.
- 4.6.4. The OHN should arrange a time to be present with the employee when viewing their occupational health record and/or provide a copy if requested.
- 4.6.5. Every effort should be made to provide an explanation about any term, code or abbreviation used in the occupational health records.
- 4.6.6. The OHN should retain a copy of the WRHA Request to Access Personal Health Information form on the employee's occupational health record.

4.7. Breaches of Confidentiality

- 4.7.1. Breach Response Steps: When an information security breach or violation has been discovered, identify the level of the incident.

General steps that should be taken by the OHN include:

- Confirm the breach or violation and the level of gravity
- Take all necessary steps to prevent further breach of the information including retrieval of breached records from any unauthorized recipients.
- Report the information security incident to the site Privacy Officer.

- 4.7.2. Breach Response Considerations: A response to the breach may be based upon the following considerations:

- If it is evident that the breach presents a danger to the subject.
- If the quantity of information and subjects involved in the breach is significant
- If the recipient of the breach has, or is, likely to contact the subject.
- If the recipient will not destroy or return the information.

Generally, if it is a significant breach, it is appropriate to inform the employee that their information has been breached. Do not inform the subject if it is determined that disclosure of the breach would likely harm the subject. The site Privacy Officer will provide guidance on responding to breaches.

5.0 References

- 5.1. *Alberta Occupational Health Nurse's Association* (2007). *Privacy and Confidentiality Guidelines*. Edmonton: Author
- 5.2. Canadian Nurses Association. (2002). *Code of Ethics*. Ottawa: Author.
- 5.3. Clearwater, K.L., Frost, A.B., Kersey, R.M., LaBossiere, K.D., Olson, R.W., Rachlis, V.E. (2006). *Employment-Related Records in Manitoba*. Eau Claire, Wisconsin: Lorman Education Services.
- 5.4. College of Registered Nurses of Manitoba. (2004). *Standards of Practice for Registered Nurses*. Winnipeg: Author.
- 5.5. Government of Manitoba. (2010). *The Personal Health Information Act, C.C.S.C. c. P33.5*. Winnipeg: Queen's Printer.

- 5.6. Winnipeg Regional Health Authority. (2010). *Collection of Personal Health Information*, #10.40.070; *Use of Personal Health Information*, #10.40.100; *Security and Storage of Personal Health Information*, #10.40.120; *Confidentiality of Personal Health Information*, #10.40.020; *Consent to Use or Disclose Personal Health Information*, #10.40.105; *Access to Personal Health Information*, #10.40.040; *Disposal of Confidential Material, Including Personal Health Information*, #10.40.090; *Transmission of Personal Health Information Via Facsimile*, #10.40.130; *Reporting of Security Breaches Related to Personal Health Information and The Corrective Procedures to be followed*, #10.40.110; Winnipeg: Author.
-

6.0 Appendices

- 6.1. OESH Release of Medical Information – Confidential
- 6.2. Consent to Disclose Personal Health Information (form #W-00332 04/10)
http://home.wrha.mb.ca/privacy/phia_forms.php
- 6.3. Request to Access Personal Health Information (form #W-00330 04/10)
http://home.wrha.mb.ca/privacy/phia_forms.php



RELEASE OF MEDICAL INFORMATION – CONFIDENTIAL

Date:		Consent Valid Until:	
To:		Phone:	
		Fax:	
Re: Name:		Previous Name:	
DOB: (m/d/y)	MHSC# 6 digit:	9 digit:	

THE ABOVE NAMED INDIVIDUAL:

- Has recently been employed by the WRHA. The checked tests/immunizations are a condition of employment requirement. Please forward the dates/results of the checked areas. If you have no records on the individual, please return form to OESH. Thank you for your cooperation.
- Requires further medical information for adequate assessment.
- Has given permission to release the following information to your institution.

<input type="checkbox"/> Measles (Red measles / Rubeola):	Vaccine Date: _____	Titre date: _____	Result: _____
<input type="checkbox"/> Mumps:	Vaccine Date: _____	Titre date: _____	Result: _____
<input type="checkbox"/> Rubella (German measles):	Vaccine Date: _____	Titre date: _____	Result: _____
<input type="checkbox"/> OR MMRII:	Vaccine given: Dose #1 Date: _____	Dose #2 Date: _____	
<input type="checkbox"/> Chickenpox:	Titre date: _____	Result: _____	
<input type="checkbox"/> Vaccine date:	Dose #1: _____	Dose # 2: _____	Titre date/result: _____
<input type="checkbox"/> Hepatitis B Vaccine Dates:			
Dose #1:	_____	Dose #2: _____	Dose #3: _____
Dose #4:	_____	Dose #5: _____	Dose #6: _____
<input type="checkbox"/> Titre date:	_____	Result:	_____
<input type="checkbox"/> BCG Vaccine:	<input type="checkbox"/> No <input type="checkbox"/> Yes	Date: _____	Scar Present: <input type="checkbox"/> No <input type="checkbox"/> Yes
<input type="checkbox"/> Tuberculin Skin Test (TST):	Most recent: Date: _____	Result: _____	mm
<input type="checkbox"/> 2-Step TST test:	#1) Date: _____	Result: _____	mm
	#2) Date: _____	Result: _____	mm
<input type="checkbox"/> CXR: PLEASE FAX COPY OF ACTUAL REPORT WITH THIS FORM			
Date:	_____	Result:	_____
<input type="checkbox"/> Polio Vaccine: Primary series given?	Yes ____ No ____	Date of last booster dose:	_____
<input type="checkbox"/> Tetanus & Diphtheria:	Date last booster dose given:	_____	
Other and/or Comments:	_____		

Employee Signature: _____ **OESH Physician/OHN Signature:** _____