

	NIGHTINGALE Nursing Registry Ltd.		POLICIES & PROCEDURES	
	Issued: January 2004		Policy #	
	Revised: New		Section: Administration	
	Approved: SH/AG		Subject: Personal Information Release	
Reviewed by: AG	Date: January 2005 Initial: AG	Date: January 2006 Initial: AG	Date: January 2007 Initial: AG	
Date: January 2008 Initial: AG	Date: January 2009 Initial: AG	Date: March 19, 2010 Initial: AG	Date: Initial:	
Date: Initial:	Date: Initial:	Date: Initial:	Date: Initial:	

1 POLICY

- 1.01 Nightingale Nursing Registry Ltd. is committed to protecting the privacy of its employees, clients/customers and confidential business information.
- 1.02 Employees are obligated to ensure that personal information, to which they may have access remains confidential, is only used for the purposes for which it was collected, is not disclosed without authorization or used for personal gain.
- 1.03 Employees are required to follow all procedures regarding collection, use, and disclosure of personal information as set out in this policy.
- 1.04 Employees who disclose personal information, contrary to this policy will be subject to disciplinary measures, up to and including discharge for cause.
- 1.05 The Privacy Officer/s are accountable for the implementation of this policy. Any issues or questions regarding this policy should be directed to The Privacy Officer/s.

2 PURPOSE

All employees at one time or another may receive personal, privileged and/or confidential information which may concern other employees, company operations or clients/customers. The purpose of this policy is to preserve the privacy of employees, clients and Nightingale Nursing Registry Ltd., by outlining employee obligations and procedures for dealing with personal, privileged and/or confidential information.

3 SCOPE

This policy applies to all employees, contractors, subcontractors of Nightingale Nursing Registry Ltd. or anyone else who is granted access to personal, privileged and/or confidential information.

4 RESPONSIBILITY

- 4.01 Employees are responsible for:
- keeping their own employee files current regarding name, address, phone number, dependants, etc.
 - being familiar with and following policies and procedures regarding personal information;
 - obtaining the proper consents and authorizations prior to disclosure of personal, privileged and/or confidential information;
 - immediately reporting any breaches of confidentiality to their Supervisor;
 - keeping private passwords and access to personal, privileged and/or confidential data;
 - explaining this policy to clients and referring them to The Privacy Officers if necessary;
 - relinquishing any personal, privileged, confidential or client information in their possession before or immediately upon termination of employment.
- 4.02 Supervisors are responsible for:
- obtaining consent to the collection and use of personal information from employees;
 - ensuring policies and procedures regarding collection, use and disclosure of information of personal information are consistently adhered to;
 - responding to requests for disclosure after the proper release is obtained;
 - co-operating with The Privacy Officer/s to investigate complaints or breaches of policy;
 - obtaining from terminating employees prior to their termination any personal, privileged, confidential or client information in their possession.
 - ensuring that disclosure of personal information or personal health information to a Third Party is done with the approval of the Privacy Officer/s in order to minimize risk of non-compliance with applicable legislative or regulatory regimes.
- 4.03 Human Resources and/or Payroll personnel are responsible for:
- ensuring that appropriate consents have been obtained from employees with respect to the collection and use of personal information;
 - maintaining systems and procedures to ensure employee records are kept private;
 - obtaining the proper consents and authorizations prior to disclosure of information contained in employee records;
 - responding to employees' requests for access to their files;
 - ensuring proper disposal of unnecessary files/information.
 - maintaining separate files to ensure that personal health information is protected.
 - ensuring that disclosure of personal information or personal health information to a Third Party is done with the approval of the Privacy Officer/s in order to minimize risk of non-compliance with applicable legislative or regulatory

regimes.

- 4.04 The Privacy Officer/s is responsible for:
- internal compliance with applicable policies or legislation;
 - co-operating with supervisors, human resources and/or payroll personnel in developing internal policies for the collection, use and disclosure of personal information and personal health information of employees and clients;
 - monitoring and responding to Third Party requests for personal information or personal health information;
 - ensuring appropriate consents are obtained for the collection, use and disclosure of personal information and personal health information;
 - where collection, use or disclosure is permitted without prior consent, notifying individuals of the collection, use and disclosure of personal information and/or personal health information after such occurrence.

5 DEFINITIONS

- 5.01 **Personal information** is any factual or subjective information, recorded or not about an identifiable individual and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number. Personal information also includes information that may relate to the work performance of the individual, any allegations, investigations or findings of wrongdoing, misconduct or discipline. Personal information does not include job title, business contact information or job description.
- 5.02 **“Personal health information”** is information about an identifiable individual that relates to the physical or mental health of the individual, the provision of health care to the individual, the individual's entitlement to payment for health care, the individual's health card number, the identity of providers of health care to the individual or the identity of substitute decision-makers on behalf of the individual.
- 5.03 **Third parties** are individuals or organizations other than the subject of the records or representatives of Nightingale Nursing Registry Ltd. Note that in certain circumstances, the company may be entitled to provide personal information to an external party acting as an agent of Nightingale Nursing Registry Ltd.
- 5.04 **Consent** Consent means voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual. An individual's consent to the collection and use of his or her personal information must be given with knowledge, not only of the information being collected, but also for the purpose or use to which the information will be put.
- 5.05 **Collection** means the act of gathering, acquiring, or obtaining personal information from any source, including third parties, by any means.

- 5.06 **"Disclosure"** means making personal information available to others inside and/or outside the organization.
- 5.07 **"Use"** means the treatment and handling of personal information by, and within the company.

6 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE
Personal Information Protection and Electronic Documents Act (PIPEDA)
 Third Party Reference Requests
 E-Mail and Internet Use
 First Reference, Implementing Privacy Legislation in the Workplace

7 PROCEDURE

7.01 Employee Records

- (a) An employee's supervisor, higher level managers, human resources and payroll personnel shall have access to employee records containing personal information. An employee's supervisor, higher level managers, human resources and payroll personnel will have access to an employee's personal health information if the Privacy Officer/s determines that such access is permissible and necessary. Personal information and personal health information will not be disclosed outside of the organization without the knowledge and/or approval of the employee. Notwithstanding the foregoing, Nightingale Nursing Registry Ltd. will co-operate with law enforcement agencies and will comply with any court order or law requiring disclosure of personal information without the employee's consent.
- (b) Employees may request access to review their own file by making arrangements with the Accounting & Payroll department. Employees shall provide at least twenty-four (24) hours notice to the Accounting & Payroll department. Employees may obtain a copy of any document in their file which they have signed previously. No material contained in an employee file may be removed from the file. A representative of the Accounting & Payroll department will be present during viewing of the file.
- (c) An employee may provide a written notice of correction related to any data contained in the employee's file. The notice of correction shall be provided to the Accounting & Payroll department.
- (d) Employee requests for disclosure of their own personal information to Third Parties must be accompanied by a completed, signed and dated Authorization to Release Information form. Attachment A to this policy is used for this purpose. This form should also be used in dealings with insurance companies with respect to employee benefits and to provide confirmation of earnings to financial institutions for lending purposes.
- (e) Unless retention of personal information is specified by law for certain time periods, personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within twelve (12) months after its use.

7.02 Client Information

- (a) Personal, privileged and/or confidential information about customers and clients may only be collected, used, disclosed and retained for the purposes identified by Nightingale Nursing Registry Ltd. as necessary.

- (b) Employees must ensure that no personal, privileged and/or confidential client information is disclosed without the client's consent and then only if security procedures are satisfied.
 - (c) Client information is only to be accessed by employees with appropriate authorization.
 - (d) Unless retention of personal information is specified by law for certain time periods, personal information that is no longer required to fulfil the identified purpose shall be destroyed, erased or made anonymous within twelve (12) months after its use.
- 7.03 Notwithstanding Paragraphs 7.01(e) and 7.02(d) personal information that is the subject of a request by an individual or a Privacy Commission shall be retained as long as necessary to allow individuals to exhaust any recourse they may have under PIPEDA.
- 7.04 Concerns or complaints related to privacy issues must be made, in writing, to the Privacy Officer/s setting out the details of the concern or complaint. The Privacy Officer/s shall investigate the matter forthwith and make a determination related the resolution of the concern(s) or complaint(s).
- 7.05 No employee shall be disadvantaged or denied any benefit of employment by reason that Nightingale Nursing Registry Ltd. believes that an employee will do anything referred to paragraphs (a), (b), or (c) below or by reason that an employee, acting in good faith and on the basis of reasonable belief,
- (a) has disclosed to the Privacy Commissioner of Canada that Nightingale Nursing Registry Ltd. or any other person has contravened or intends to contravene a provision of PIPEDA related to the protection of personal information;
 - (b) has refused or stated the intention of refusing to do anything that it is in contravention of a provision of PIPEDA related to the protection of personal information;
 - (c) has done or stated an intention of doing anything that is required to be done in order that a provision of PIPEDA related to the protection of personal information not be contravened.
- 7.06 An employee who is found to be in breach of this policy will be subject to discipline up to an including discharge for cause.

Attachment A

AUTHORIZATION TO RELEASE PERSONAL INFORMATION

I, _____ [Employee's Name], hereby authorize Nightingale Nursing Registry Ltd. to release personal information listed below to _____ [Third Party].

Choose whichever apply:

Confirmation of employment and salary information (usually used for banking/lending purposes).

All employment information in company's possession, including dates of hire, positions held, information relating to performance and attendance (both objective and subjective), salary information and all related matters (usually used for reference checking purposes).

Any medical information in the company's possession (including absences, medical notes or reports (usually used for sick leave, disability benefits or health insurance).

Other (specify information to be released):

I hereby release and discharge Nightingale Nursing Registry Ltd. from any claim whatsoever relating to the Company acting in accordance with this Authorization.

Employee's Signature

Date