"PEOPLE" MANUAL - CORPORATE CULTURE & HUMAN RESOURCES	
POLICY NO:	**SECTION TITLE: Corporate Culture**
CCHR-A-10	**SUBJECT TITLE: Privacy and Confidentiality**
EFFECTIVE DATE:	**AUTHORIZED BY: Corporate Policy Committee**
January 1, 2014	**REVISION DATES: September 1, 2018** *This policy replaces and supersedes CCHR-A-03, CCHR-A-05, CCHR-A-10, CCHR-A-11 and CCHR-A-12*[i]

PURPOSE

The purpose of the Chartwell Retirement Residences ("Chartwell", "us" or "we") Privacy and Confidentiality Policy is to promote responsible practices in the handling and management of Personal Information and to ensure compliance with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and / or the privacy statutes of each Canadian jurisdiction where Chartwell operates, as applicable.

DEFINITION or TERMS OF REFERENCE

"Circle of Care" means those directly involved in the provision of health care to an individual.

"Chartwell" means Chartwell Retirement Residences and its affiliates and subsidiaries.

"Confidential Information" is private information about Chartwell and its business, its staff, its finances, its Residents and Residents' representatives or families. Non-public financial information relating to Chartwell, proprietary corporate information, information relating to Chartwell's operations that is not in the public domain, Employee Records, Health Records, Personal Information and Personal Health Information are all considered Confidential Information.

"Confidentiality" is the obligation of Employees to keep Personal Information and information that is not made available or disclosed to unauthorized individuals, entities, or processes secret. The privacy of the resident's and employee information will depend on maintaining the confidentiality of their Personal Information.

"Employee" for the purpose of this policy means every individual working or volunteering at a Chartwell corporate office or at a retirement home or long term care home owned, operated, and/or managed by Chartwell.

"Employee Records" means all data, information, documentation and reports prepared by Chartwell relating to Chartwell Employees whether stored in hard copy or electronically. Employee Records contain Personal Information.

"Health Records" means all data, information, documentation and reports prepared by Chartwell relating to the care provided to Residents whether stored in hard copy or electronically. Health Records include progress notes, charting notes, Medication Administration Records (MARs), assessments and plans of care. Health Records contain Personal Information.

"Personal Information" means information about an identifiable individual, but does not include the name, title, or business address or telephone number of an employee of an organization or information that is publically available about an individual. For example, Personal Information includes, but is not limited to, home address, birthdate, disciplinary history and financial information. Personal Information includes Personal Health Information, Health Records and Employee Records.

"Personal Health Information" means identifying information about an individual in oral or recorded form, if the information relates to the physical or mental health of the individual. For

example, personal health information includes family health history, information about visits to a doctor, identity of a substitute decision maker and a health card number.

"PIPEDA" means Canada's *Personal Information Protection and Electronic Documents Act*.

"Privacy" means the right of the individual to control the collection, use and disclosure of information about themselves and the right to determine when, how and to what extent they share information about themselves with others.

"Privacy Officer" means the person appointed by the Executive Vice President and General Counsel to oversee Chartwell's compliance with its Privacy and Confidentiality Policy and the principles set out in it.

"Resident" for the purpose of this Policy means a current or former resident and prospects of a retirement home, long term care home or apartment owned, operated and/or managed by Chartwell or a participant in a program or service offered by Chartwell.

"Third Party" means any individual or organization outside of Chartwell.

SCOPE

This policy applies to Personal Information and Confidential Information that is collected, used, retained or disclosed by all entities owned, operated and/or managed by Chartwell in Canada. This policy applies to Employees at those entities. This policy also applies to any service providers collecting, using or disclosing Personal Information on behalf of Chartwell.

POLICY

Chartwell respects the privacy rights of our Residents and Employees and is committed to protecting the Personal Information and Confidential Information in our possession or control. Chartwell adopts the Ten Principles of Personal Information Protection as set out in Schedule 1 of PIPEDA as the basis of its privacy compliance program. Chartwell also meets the standards set in each applicable privacy statute in each Canadian jurisdiction in which it operates. The Ten Principles of Personal Information Protection apply to all of Chartwell's undertakings and business, including its Residents' Personal Information and its Employees' Personal Information (subject to any requirements set out in specific collective agreements).

Individuals who violate this Policy and Procedures are subject to appropriate disciplinary action by Chartwell, up to and including possible termination of employment.

Principle 1 – We Are Accountable For The Personal Information In Our Possession.

Chartwell is responsible for Personal Information in its possession or control. Chartwell shall use appropriate means to provide a comparable level of protection while information is being processed by a Third Party. Chartwell has established policies and procedures aimed at protecting Personal Information. Chartwell has appointed a Privacy Officer to oversee privacy issues for Chartwell. We have also educated our employees about our Privacy and Confidentiality Policy and their role in protecting Personal Information. If you have questions about Chartwell's privacy practices, you can contact our Privacy Officer at 1-888-663-6448 or by email at privacyoffice@chartwell.com.

Principle 2 – Chartwell will inform you why it is collecting Personal Information when the information is collected.

When Chartwell collects Personal Information, we will inform you orally, electronically or in writing of the reasons why we require such information, what use will be made of it and with whom it may be shared. Collection may occur without knowledge or consent as permitted by law, including collection in the course of an investigation.

Except where required or permitted by law, Chartwell will not use or disclose information for a purpose other than the purpose for which it was collected without consent. Personal Information is shared with only those who need to know the information.

Resident Information

Chartwell will collect, use, retain and disclose information about Residents for the following purposes:

- To establish and maintain responsible business relations with Residents
- To understand Resident needs and preferences
- To provide Residents with health care and other related services
- To communicate with other service providers regarding a Resident's care, including but not limited to, Provincial and Local Health Authorities.
- To provide Third Party providers of health services with information about a Resident's health
- To develop, enhance, market or provide Chartwell services
- For administration, management, strategic planning, and decision-making within the organization
- To meet legal, regulatory, insurance, audit and security requirements
- To obtain accreditation with provincial or national associations and agencies applicable to Chartwell's business

The Personal Information collected about Residents by Chartwell includes:

- Resident name, personal statistics and contact information
- Payment/financial information
- Recreational interests
- Provincial Health Card number and facts about a Resident's past and present health issues
- Where applicable information about a Resident's Substitute Decision Maker or Power of Attorney

Employee Information

Chartwell collects Personal Information from Employees in order to pay them, comply with laws, provide them with benefits, administer performance management tools, to improve on and manage programs, policies and employee relations, for emergency preparedness and generally to establish, manage or terminate the employment relationship. In certain cases, Chartwell may also aggregate Employee Personal Information to provide business metrics and evaluate the effectiveness of our HR programs, but this aggregated information will not allow the identification of any individual. Chartwell also collects Personal Information from individuals seeking employment with Chartwell in order to screen applicants and ensure capable candidates are hired for appropriate positions.

Chartwell may also use or disclose Employee Personal Information in the course of investigating, negotiating or completing a sale, financing or other business transaction involving all or any part of Chartwell's business.

When appropriate, the Personal Information that Chartwell collects may be transferred to a subsidiary or affiliated company; our insurers and bankers; benefit insurance carriers; administrators or managers of our pension/retirement plans; and other companies engaged in contractual activities on our behalf for the purposes for which the Personal Information is to be used.

Principle 3 – Chartwell will collect, use or disclose Personal Information about you only with your consent.

Chartwell will generally seek consent to collect, use, retain and disclose Personal Information at the time of collection. Chartwell may seek consent to use and disclose Personal Information after it has been collected, but before it is used or disclosed for a new reason. Chartwell will take into account the sensitivity of the Personal Information when determining the appropriate form and method of obtaining consent.

The acceptance of employment or benefits by an employee generally constitutes deemed consent for Chartwell to collect, use and disclose Personal Information for all identified purposes.

In certain circumstances, Personal Information may be collected, used, retained or disclosed without knowledge and consent of the individual, including the following:

- when required by law (such as in response to a court order or subpoena) or to comply with regulatory requirements, including but not limited to, requirements from local or Provincial Medical Officer of Health
- where we are involved in a corporate re-organization or we sell or merge all or part of our business to a third party
- where medical reasons make it impossible or impractical to seek consent
- where there is an emergency where the life, health or security of an individual is threatened
- where the information is collected, used or disclosed for the purpose of an investigation
- when requested by a regulatory college or agency who licenses Employees or service providers

What happens if you choose not to give us your consent? What if you withdraw your consent at a later date?

Residents always have the option not to provide their consent to the collection, use and disclosure of their Personal Information, or to withdraw their consent at a later stage. Where a Resident chooses not to provide us with permission to collect, use or disclose Personal Information, we may not have sufficient information to continue providing the Resident with our services.

Where an Employee or candidate for employment chooses not to provide us with permission to collect, use or disclose Personal Information, we may not be able to employ them, continue to employ them and / or to provide them with benefits.

Residents and Employees may contact the General Manager / Administrator of their home or the Privacy Officer for more information regarding the implications of withdrawing consent.

Principle 4 – Chartwell limits the amount and type of Personal Information we collect.

Chartwell will limit the collection of Personal Information from Residents and Employees to that which is reasonably required to provide our services or operate our business. Chartwell may collect Personal Information from other sources such as credit bureaus, previous employers, other health care providers such as hospitals, or other Third Parties that have the right to disclose the information. If Chartwell receives information from a third party that has not been requested and is not linked to any purpose, we will return it to the individual or destroy it.

Principle 5 – Chartwell will use and disclose Personal Information only for the purposes for which we have your consent. We will keep Personal Information only as long as necessary to accomplish these purposes.

Use of Personal Information

If Chartwell intends to use or disclose Personal Information for any purpose not previously identified to the individual, we will obtain their prior consent. Chartwell may disclose Personal Information:

- to credit grantors and reporting agencies
- where disclosure is required by law or necessary to protect Chartwell's interests
- where disclosure is for servicing purposes to a supplier or agent who provides services to Chartwell
- where Chartwell is involved in a corporate reorganization or sells or otherwise disposes of all or part of its business
- where the individual consents to the disclosure

Retention of Personal Information

Chartwell shall keep Personal Information only as long as it remains relevant for the identified purpose, or as required or permitted by law. If Personal Information has been used to make a decision about a Resident or Employee, Chartwell shall retain the information, or the reason for making the decision, for a period of time that is reasonably sufficient to all for access by the Resident or Employee.

Principle 6 – Chartwell will endeavor to keep accurate the Personal Information in our possession or control.

Chartwell will take all reasonable steps to ensure that Personal Information used by it is sufficiently accurate, complete, and up to date to minimize the possibility that incorrect information may be used to make a decision about a Resident or Employee. From time to time, Residents and Employees may be asked to update their Personal Information. Individuals are encouraged to advise us of any changes to their Personal Information that may be relevant to the services we are providing.

Residents are encouraged to contact the General Manger or Administrator of their home to update Personal Information.

Employees and candidates should contact the General Manager / Administrator or their Human Resources representative should they need to update their Personal Information.

Principle 7 – Chartwell will protect Personal Information with safeguards appropriate to the sensitivity of the information.

Chartwell will protect Personal Information by using appropriate security measures to protect Personal Information against such risks as loss or theft, unauthorized access, disclosure,

copying, use, modification or destruction regardless of the format in which it is held. We will consider the sensitivity of the information in determining the level of protection required. Chartwell will use care in disposing of or destroying Personnel Information to prevent unauthorized parties from gaining access to the information. All Employees with access to Personal Information will be required to respect the Confidentiality and Privacy of Personal Information.

Chartwell will protect Personal Information transferred to Third Parties by contractual agreements that stipulate that the Third Party shall respect the Confidentiality of Personal Information and comply with all legal requirements under applicable Canadian federal and provincial privacy legislation.

In some circumstances, Personal Information may be processed and stored outside of Canada by Chartwell or a Third Party processor, and such Personal Information may be subject to disclosure in accordance with the laws applicable in the jurisdiction in which the information is processed or stored.

Principle 8 – Chartwell will be open about the procedures used to manage your Personal Information.

Chartwell will make information about its policies and practices with respect to the management of Personal Information easy to understand and reasonably accessible, including:

- the name or title and address of the person or persons accountable for Chartwell's compliance with the Privacy and Confidentiality Policy;
- a description of the type of Personal Information held by Chartwell, including a general account of its use;
- the procedure to gain access to Personal Information held by Chartwell;
- copies of brochures or other information that explains Chartwell's privacy policies, standards and codes; and
- what types of Personal Information are made available to related organizations.

Principle 9 – At their request, Chartwell will advise individuals of what Personal Information we have in our possession or control about them, what it is being used for, and to whom and why it has been disclosed. An individual shall also be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Upon request, Chartwell will permit Residents or Employees to review Personal Information held by Chartwell regarding them. The information will be provided at no cost unless the individual is advised in advance of the cost for retrieval and photocopying. Any charges to the requestor of such information will be reasonable.

In certain circumstances, Chartwell may not be able to provide access to all of the Personal Information it holds about an Employee or Resident. For example, Chartwell will not provide access where doing so would likely reveal Personal Information about a third party unless such information could be severed from the record or the third party consents to the disclosure. Other reasons for denying access include, but are not limited to situations where disclosure could reasonably be expected to threaten the life, safety or security of another individual, information covered by solicitor-client privileged, where disclosure would reveal confidential commercial information, information collected in relation to an investigation of a breach of an agreement or contravention of a law, or where it is prohibitively costly to provide the requested

information. Where an individual is denied access to information, Chartwell will provide reasons for why access was denied.

Residents may ask Chartwell to correct their Personal Information if this information is out of date, inaccurate or incomplete. Chartwell will promptly modify any Personal Information found to be inaccurate or incomplete. Any unresolved differences regarding the accuracy of Personal Information will be noted in the individuals file. Residents seeking access to their health or business file or seeking correction of information should ask the General Manager or Administrator verbally or in writing.

Corporate office Employees seeking access to their file should submit a written request to their designated human resources representative. Employees working in a Chartwell Residence seeking access to their file should submit a written request to their General Manager/Administrator. Residents seeking access to their file should submit a written request to their General Manager/Administrator.

In most instances, individuals will receive a response to their access request within 30 days. If an individual has any concerns about the access that is provided, they are encouraged to contact our Privacy Officer at 1-888-663-6448 or by email at privacyoffice@chartwell.com.

Principle 10 – Individuals may challenge Chartwell's compliance with this Privacy Policy.

Chartwell will respond to individual complaints and questions relating to privacy. We will investigate and attempt to resolve all complaints. To challenge compliance with this Policy, individuals should forward their concerns in writing to Chartwell's Privacy Officer at:

Chartwell Retirement Residences

100 Milverton Drive, Suite 700

Mississauga, ON, L5R 4H1

or

privacyoffice@chartwell.com

The Privacy Officer will ensure that a complete investigation of all complaints has been undertaken and will report their findings to the individual in most instances within 30 days.

Confidential Information

One of Chartwell's most valuable assets is information. Employees are to maintain the confidentiality of Confidential Information entrusted to them by Chartwell and its Residents, suppliers and others related to our business. Employees are to take steps to safeguard Confidential Information by keeping such information secure, limiting access to such information to those Employees who have a "need to know" in order to do their job and avoiding discussion of Confidential Information in public areas such as elevators, on planes and on mobile phones.

Confidential Information may be disclosed to others when disclosure is authorized by Chartwell or must be made pursuant to laws or regulations. The obligation to preserve Confidential Information is on-going even after termination of employment. Employees who have any doubt about whether information is confidential are to discuss with their manager.

CROSS REFERENCE

Act Respecting the Protection of Personal Information in the Private Sector (Québec)
Civil Code of Québec

Freedom of Information and Protection of Privacy Act (B.C.)
Personal Health Information Protection Act, 2004 (Ontario)
Personal Information Protection & Electronic Documents Act (Canada)
Personal Information Protection Act (Alberta)
Personal Information Protection Act (B.C.)

LTC – Admission Consent

LTC – Resident Immunization Program

LTC – Resident Photographs

RRCS – Privacy of Personal Information – Notice and Consent

Website Privacy Statement

Record Management and Retention

Disclosure Policy

SDM Matrix

PROCEDURES

1. Access to Confidential Information

a) Employees are only to access information required to perform their duties. An Employee who for any reason deliberately accesses Confidential Information or Personal Information that is not required in the performance of their normal duties is considered to have breached confidentiality, whether or not the information is disclosed to another person.

b) All Employees will be informed of this Privacy and Confidentiality Policy as part of their new employee orientation and will be required to sign a Confidentiality Agreement.

c) Employees are not to transmit Confidential Information to another person either during or after work hours without authorization unless the recipient of the Confidential Information is a Chartwell Employee who requires the information to perform their job duties. Employees at a corporate office are to obtain authorization from their manager or human resources representative. Employees in retirement home or long term care home are to obtain authorization from the General Manager or Administrator.

d) An employee who is requested to provide Confidential Information is to advise that they are not authorized to disclose such information and should refer the inquiring party to the General Manager / Administrator or Human Resources representative as applicable.

2. Disclosure of Employee Information

a) Employee Records may only be released by the General Manager / Administrator of a facility or an authorize human resources representative. Employee Information is only released with the proper written authorization by the employee concerned or, when required or permitted by law.

b) All requests for release of Employee Records are to be referred to the General Manager, Administrator or Human Resources representative.

c) Employees requesting the release of their Employee Records or other Personal Information must provide written authorization specifying what information is to be released and to whom.

3. Access and Disclosure of Resident Information

a) Personal Health Information regarding a Resident is only to be disclosed:

i. to the Resident or to an incapable Resident's substitute decision maker;

ii. to a person identified by the Resident or an incapable Resident's substitute decision maker where written authorization from the Resident or substitute decision maker is obtained;

iii. to individuals within the Circle of Care when required and consent has not been specifically withdrawn; or

iv. when required or permitted by law.

b) Only registered staff (i.e. RNs, LPNs, RPNs, etc.) or the General Manager/Administrator are authorized to share information regarding a Resident's clinical status, well-being or other Personal Health Information.

c) Residents or their substitute decision makers requesting the release of or access to their Health Records or other Personal Information must provide written authorization specifying what information is to be accessed or released and to whom.

d) Requests for access or disclosure are to be provided to the General Manager/Administrator.

e) Direct the requestor to relevant program office (eg. E-Health Ontario, Health Authority) where the request is for records involves records belonging to another program or agency.

f) Where the request is being made by a substitute decision maker, the General Manager /Administrator or their designate must confirm the person is indeed the substitute decision maker for the resident. Refer to the SDM matrix or contact privacyoffice@chartwell if you are unsure about whether a person is the resident's SDM.

g) The General Manager/Administrator or designate is to identify what records are available and advise the requestor of any charges for copies of the records.

h) If the records can be disclosed, provide a copy of the records within 30 days.

i) Where some or all of the records cannot be disclosed for reasons outlined in Principle 9, ***contact the privacy office who will review and provide a response letter***. The response letter is to be sent within 30 days of the receipt of the request.

4. Correcting Personal Information

a) Residents or their substitute decision makers requesting a correction to their Health Records or other Personal Information must provide written request specifying what information is to be corrected.

b) Requests for correction are to be provided to the General Manager/Administrator.

c) Direct the requestor to relevant program office (eg. E-Health Ontario, Health Authority) where the request to correct personal information involves records belonging to another program or agency.

d) The General Manager/Administrator is to discuss the correction with the appropriate clinician(s) to determine whether to change the information. Where the correction is granted, strike out the previous information from the medical record (leaving it readable) and record the new information.

e) Where the request is being made by a substitute decision maker, the General Manager/Administrator or their designate must confirm the person is indeed the substitute decision maker for the resident. Refer to the SDM matrix or contact privacyoffice@chartwell if you are unsure about whether a person is the resident's SDM.

f) The General Manager / Administrator or their delegate (i.e. DOC/HWM) is to provide a response in writing within 30 days advising if the correction was granted and if not the reason the request has been refused.

5. Safeguarding Information

a) Employee and Resident files are to be stored securely (eg. in a locked filing cabinet located in a locked room).

b) Access to Employee and Resident files should be restricted to authorized staff that may need access to carry out their duties.

c) Do not store Personal Information on mobile devices such as laptops, PDA's and USB keys unless absolutely necessary. If Personal Information must be stored on a mobile device, the device must be encrypted.

d) Clear your desk of any documents containing Personal Information or other confidential information when you are not in your office.

e) Protect your passwords. Do not write your password down or share with anyone.

f) Do not leave devices containing Personal Information or any other confidential information in your vehicle. If it absolutely cannot be avoided, lock them in the trunk before you start the trip, not in the parking lot of your destination.

6. Privacy Breach Protocol

a) An Employee who becomes aware of a privacy breach or suspected privacy breach involving personal or health information in the custody or control of Chartwell must immediately notify their supervisor, the General Manager/ Administrator or Chartwell's Privacy Officer.

b) The General Manager, Administrator or Privacy Officer will assess the situation and determine if a breach has occurred and take immediate steps to contain the breach. ***Refer to the National Privacy Tool Kit – How to Respond to a Privacy Breach at https://sites.google.com/a/chartwellreit.ca/ppf-legal/privacy-privee***

c) If a breach has occurred, the General Manager or Administrator must:

   i. Notify their DRO and Chartwell's Privacy Officer

   ii. Complete an Information Security or Privacy Incident Report and submit to the Privacy Officer

d) The Privacy Officer will determine whether the Privacy Office or the General Manager/Administrator take the lead in conducting the investigation based on the nature of the breach and potential risk to the organization. The investigation will include the following:

   a. Identification and analysis of the events that led to the privacy breach

   b. Evaluate what was done to contain the privacy breach

   c. Recommend remedial action to help prevent future breaches

e) The Privacy Officer will contact the following individuals as necessary:

   a. applicable platform Vice President
   b. Senior Vice President Information Technology
   c. Vice President Marketing & Communications
   d. Senior Executive Committee
   e. Insurer

f) After assessing the situation, the Privacy Officer will determine if notification to individuals or institutions (i.e. College of Nurses, Privacy Commission) is required. Direction will be given by the Privacy Officer regarding the form of notice and who is to provide the notice.

g) All suspected privacy breaches involving Ontario e-Connect must be reported by the Privacy Officer or delegate to e-Health Ontario Service Desk by the end of the next business day, after becoming aware of the incident.

7. Annual Privacy Breach Reporting – Ontario

   a. All privacy breaches must be reported to the Privacy Office
   b. The Privacy Office will track privacy breach statistics and will provide the Ontario Privacy Commissioner with the required annual report starting March 2019
   c. maintain a log of all reported privacy breaches and will identify what incidents are required to be reported to the Ontario

8. Disposal

a) Paper documents containing Personal Information are to be placed in secure shred bins for shredding and not placed in regular garbage or recycle bins.

b) Paper documents containing Personal Information must be shredded in a manner which prevents the Personal Information being obtained from the shreds.

c) Electronic documents containing Personal Information are to be erased or destroyed.

d) Electronic devices no longer in use are to be returned to Chartwell's IT department for secure disposal.

e) Medication pack/strip must have the name and numbers removed from the packaging before disposal.

FORMS

Information Security or Privacy Incident Report

Confidentiality Agreement

Authorization for Release of Employee Information

Consent to Disclose or Access Personal Health Information Form

Request to Correct Personal Health Information Form

Schedule to Lease – Privacy Notice

AUDIT INDICATORS

Employee Files

Resident Files

Incident Reports

Written Authorization / Consent

Progress Notes

Privacy Commissioner's Investigation, Audit or Inquiry

[i] CCHR-A-03 Confidentiality of Resident Information, - CCHR-A-05 Employee Privacy, CCHR-A-10 Privacy & Confidentiality, CCHR-A-11 Release of Employee Information, CCHR-A-12 Resident Privacy