

APPENDIX "A"

INFORMATION SECURITY CLASSIFICATION AND STANDARDS CHART

A significant amount of Region Information does not fall into any of the classes identified below because these documents are either public or are not sensitive. **Inquiries regarding information classification should be directed to the Information and Privacy (I&P) Office.**

Classification A: Sensitive *(No identifiable information)*

Potential Harm (examples)	<ul style="list-style-type: none"> erosion of Region credibility and reputation; or inappropriate release or communication of sensitive Region Information.
Information Type (examples)	<ul style="list-style-type: none"> general internal assessments or documents not meant for general Disclosure; or unapproved or incomplete policies or proposals.
Access Privileges	<ul style="list-style-type: none"> granted on a need-to-know basis to deliver services or carry out job functions.
Storage	All locations: <ol style="list-style-type: none"> any area under direct surveillance during business hours; on a Region server; on directories accessible only to staff member; and in designated secure off-site records storage areas.
Transport/ Transmission	<ul style="list-style-type: none"> standard mail, courier or transport; or faxing or internet transmission using approved Region procedures.
Reproduction	No restrictions, but Region copies destroyed immediately after use.
Disposal	Confidential shredding or secure disposal in accordance with IT Security standards.

Classification B: High-Sensitive *(Confidential: important business documents, identifiable information)*

Potential Harm (examples)	<ul style="list-style-type: none"> threat or potential breach of individual privacy, or release of identifiable individual information without permission; economic harm to the Region or third parties; risk to Region disaster preparedness and recovery; or erosion of Region credibility as service provider;
Information Type (examples)	<ul style="list-style-type: none"> personal patient registration, diagnostic, and treatment Information, including identifiable photographs; employment records including salary and benefit Information, minutes of evaluation; third-party business confidences; Region vital records, blue cards; or quality assurance committee minutes or documents.
Access	<ul style="list-style-type: none"> granted on a need-to-know basis to deliver services or carry out job functions; or as authorized by Executive Director (or designate), or positional equivalent.
Storage	Region Locations: <ol style="list-style-type: none"> in locked areas under surveillance during business hours, restricted to authorized personnel; in unlocked Region administrative/clinical area with non-public access under constant direct surveillance; and on a secure Region network server.

APPENDIX “A” cont’d

Storage (cont’d)	<p>Off-site Locations Off-site storage requires the approval of the Executive Director (or designate), or positional equivalent, and is based on program needs.</p> <ol style="list-style-type: none"> 1. in locked areas or vehicles during daytime transport; 2. under surveillance of staff member in homes (for Home Care only); 3. on directories accessible only to staff member; 4. in designated secure off-site records storage areas, and 5. in Information Systems approved by I&P Office.
Transport/ Transmission	<ul style="list-style-type: none"> • mail, courier, or transport in properly labeled secure packaging or lockable chart transport bags, using reputable companies that employ secure conditions; and • faxing and internet transmission shall be minimized in accordance with the Transmission of Information by Facsimile or Electronic Mail policy (#1420);
Reproduction	<ul style="list-style-type: none"> • copy only when necessary and when access to original is highly impractical or for vital records backup; • Region copies destroyed immediately after use.
Disposal	Confidential shredding or secure disposal in accordance with IT Security standards.

Classification C: Extreme-Sensitive (*Restricted Access*)

Potential Harm (examples)	<ul style="list-style-type: none"> • immediate threat to health and safety of patients, staff, or other individuals; • threat to security systems protecting medical facilities and equipment; • interference with civil or criminal justice administration.
Information Type (examples)	<ul style="list-style-type: none"> • names of staff and patients in areas identified as a target of criminal offences; • plans of high-risk area facilities; • Information describing security systems; • backup of vital records; or • forensic records under the <i>Young Offenders Act</i> or for high-risk adults.
Access	After successful security screening and authorization from the Executive Director (or designate), or positional equivalent.
Storage	<p>Only stored in Region locations:</p> <ol style="list-style-type: none"> 1. in locked areas under 24 hour surveillance, accessible only by authorized personnel; 2. only on a dedicated high secure Region network server; and 3. records shall be marked as “extreme-sensitive.”
Transport/ Transmission	<ul style="list-style-type: none"> • mail or transport only under high-secure conditions; • no unsecured internet transmission; or • no faxing except in emergencies.
Reproduction	<ul style="list-style-type: none"> • copy only when necessary and as approved by the Executive Director (or designate), or positional equivalent; • distribution and destruction log for each reproduction; or • Region copies destroyed immediately after use.
Disposal	Confidential and supervised on-site shredding or secure disposal in accordance with IT Security standards.