

<p>Privacy Policy Health Information in Electronic Environments</p>
--

Policy Purpose:

The purpose of this policy is to identify the safeguards used by managers within the NWT healthcare system to plan, implement, operate and maintain IT healthcare systems responsibly.

Application:

This policy covers information that is in electronic formats that may be used in the delivery of medical care services.

Policy Statement:


IT and program managers within the NWT healthcare system use appropriate standards and practises to safeguard and respect the privacy of individual's personal information.

Policy Requirements:

Activity	Consideration
NWT system-wide approach	The NWT e-Health Committee leads the decision-making related to IT system acquisition. Individuals regional Authorities, Divisions within the Department and other groups within the NWT healthcare systems do not acquire IT systems.
Risk assessments	Risk Assessments should be conducted on a pre-determined regular basis on all systems that maintain personal information. This includes performing assessments on new systems that will maintain personal information and on systems that have undergone significant upgrades or changes. Personal information should be categorised as low, medium or high sensitivity.
Security implementation	Physical and technological safeguards should be implemented to secure personal information maintained by the healthcare organization. These safeguards should be implemented in accordance with the sensitivity of the information. The higher the sensitivity, the more rigorous safeguards should be in place. Safeguards should be implemented in accordance with appropriate security policies.
Accuracy and Integrity Assurance	Accuracy and integrity of personal information maintained on IT systems should be checked on a regular basis though the use of auditing procedures.
Compliance Audits	Compliance audits should be used on a regular basis to determine that personal information is being accessed, collected, used and disclosed in compliance with appropriate privacy legislation and policies. Results of compliance audits should be used to determine staff awareness and training.

Activity	Consideration
Unauthorised access	If it is determined that unauthorised access (internal or external) to personal information has occurred, an individual designated with the responsibility for ensuring the protection of the personal information should be notified and the security policy should be consulted.
Personal Information Retention	The retention of personal information should be based on an established records retention schedule. Disposal of records in accordance with this schedule must be conducted in a secure manner.
Collection practices	Management should regularly review practices, including intake forms and procedures for the collection of personal information to ensure only information that is required to perform the task is being collected and that the collection practices comply with appropriate policies, procedures and legislation.
Staff awareness	Management should provide staff with a regular review of their obligations in regards to the appropriate use of personal information and provided with contact information of an individual within the healthcare organization if they are unaware of how to respond to a particular issue regarding the collection, use or disclosure of personal information

Approval and Effective Date:



Chad Fehr, CEO

Jan. 22, 2009

Date