Plain Language Statement
Integrated Decision Support (IDS)

Under its obligations as a Health Information Network Provider ("HINP), under the *Personal Health Information Protection Act*, 2004 and O.Reg 329/04, the Integrated Decision Support Solution ("IDS") has prepared the following plain language description of the services and security safeguards used by IDS and the Ontario Hospital Association ("OHA"), as it's steward.

IDS is an information technology solution that aggregates and otherwise processes clinical, financial, and operational information received from health care providers to present the information in a form that is more readily actionable for quality of care activities (the "Purpose"). More specifically, the information produced through use of the IDS Solution assists health information custodian ("HIC") participants in making informed, evidence-based decisions that improve or maintain the quality of the health care they provide.

IDS is stewarded by the OHA, an association that provides services including data and analytics support. Under the OHA's operation of the IDS Solution they are acting as a HINP, integrating data on behalf of HICs for the purposes of quality of care, managing operations, research, and education & training, pursuant to signed Data Sharing Agreements ("DSA") amongst participants. The OHA is not a commercial provider of information technology services and provides the IDS Solution and related services as a service to participating HICs, their agents and patients, pursuant to a Master Services Agreement ("MSA").

IDS has safeguards in place to ensure the security of personal health information ("PHI"). A Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA) were conducted by an external auditor, ensuring that the integrity of PHI is maintained, under the provision of services as a HINP for the Participating HICs. Access to IDS is controlled and monitored, through a secure portal for approved users. Data is stored securely and made available at levels only to those for whom, under the IDS DSA, it is permitted. Strict password policies (role based and unique) exist and access is only given to those individuals for whom their organizational contact (local registration authority, "LRA") has given IDS the approval to set up. IDS is not available via the public internet.

Any questions or concerns can be directed to Alice Betancourt, the OHA's Director of Legal, Regulatory, and Governance Issues at abetancourt@oha.com or to IDS at IDSInfo@oha.com.