Plain Language Statement
Integrated Decision Support (IDS)

The following is a plain language description of the services and security safeguards used by Integrated Decision Support ("IDS") and the Ontario Hospital Associations ("OHA"), as it's steward. In accordance with the requirements of s. 10(4) of the *Personal Health Information Protection Act, 2004* ("PHIPA") and ss. 6(3) of O. Reg. 329/04 made under PHIPA, this description provides an explanation to the health information custodians ("HICs") who utilize these solutions and to the public of which health information network provider ("HINP") services are being provided. The document explains how the security processes in place will ensure the confidentiality of the personal health information ("PHI") used in the provision of such services.

IDS is an information technology solution that aggregates and otherwise processes clinical, financial, and operational information complied or created by health information custodians (the "Participants") 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, system improvement, managing operations, program planning, 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").

Since its creation in 2009, IDS has worked to create a network of health providers, exchanging data about shared-care patients to enable improvements in the quality of care delivery. IDS operationalizes the following features in the delivery of its solution:

- Pre-linked patient data across the continuum of care
- Timely, refreshed weekly, data for decision-making
- A 'by providers, for providers' mission as it is governed by its user community
- Value added features and data solutions that continually adapt to provider priorities and needs in response to an everchanging healthcare system
- A minimal PHI policy helps with risk management whereby IDS does not allow any direct* PHI to be available to users; only indirect PHI that is necessary to enable the 'purpose' of IDS

Understanding the importance of ensuring the privacy and security of PHI, 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 and made available at levels only to those for whom, under the IDS DSA, it is permitted. Data is stored in a secure environment with effective administrative, physical, technical and information security safeguards in compliance with industry best practices. 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. These are individuals whose roles and responsibilities in their organization permit access to data to fulfill the requirements of their job. IDS is not available via the public internet.

*No patient names, addresses, DOB, HCN, contact information, test results