



Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

All rights reserved.

The contents of this publication may be reproduced unaltered, in whole or in part and by any means, solely for non-commercial purposes, provided that the Canadian Institute for Health Information is properly and fully acknowledged as the copyright owner. Any reproduction or use of this publication or its contents for any commercial purpose requires the prior written authorization of the Canadian Institute for Health Information. Reproduction or use that suggests endorsement by, or affiliation with, the Canadian Institute for Health Information is prohibited.

For permission or information, please contact CIHI:

Canadian Institute for Health Information

495 Richmond Road, Suite 600

Ottawa, Ontario K2A 4H6

Phone: 613-241-7860

Fax: 613-241-8120

cihi.ca

copyright@cihi.ca

© 2020 Canadian Institute for Health Information

How to cite this document:

Canadian Institute for Health Information. *CIHI's Health Data and Information Governance and Capability Framework: Supplementary Toolkit*. Ottawa, ON: CIHI; 2020.

Cette publication est aussi disponible en français sous le titre *Cadre de renforcement des compétences et de la gouvernance en matière de données et d'information sur la santé de l'ICIS : trousse d'outils complémentaire*.

Table of contents

- Capability descriptions 4
 - Core 4
 - Foundational 4
 - Supplemental 5
 - Enabling 6
- Core capabilities 7
- Foundational capabilities 17
- Supplemental capabilities 31
- Enabling capabilities 55

Capability descriptions

The following tables contain descriptions of each capability, organized by classification: core, foundational, supplemental and enabling. The associated ID (in column 1) relates to the subject area: strategy and governance (SG), policies and processes (PP), assets and standards (AS),

—	Data change management policies and processes	Principles, frameworks, policies and processes for managing and

Core capabilities

In the following tables, the ID columns refer to the subject areas: strategy and governance (SG), policies and processes (PP), assets and standards (AS) and people and knowledge (PK).

PP1: HDI privacy policies and processes

Capability description — PP1

	HDI privacy policies and processes	<ul style="list-style-type: none"> Principles, frameworks, policies and processes for compliance with legal and statutory privacy rules. Includes clear understanding of legislative authority and intent, governance and accountability structures, consent management, compliance, training and incident management (identification, notification and remediation). Also aligns with social licence to collect, store, distribute and use HDI. Note that HDI privacy policies and processes, HDI security policies and processes and data risk management (DRM) are key elements of HDI capability framework. 	<ul style="list-style-type: none"> HDI privacy framework and guidelines Privacy impact assessment guidelines Privacy incident management guidelines 	<ul style="list-style-type: none"> HDI privacy policy Consent management policy Data commercialization policy Privacy impact assessment Privacy incident log

Strategic and operational questions to ask — PP1

<ul style="list-style-type: none"> • How are risks managed to achieve both protection (privacy/security) of sensitive health data and enabling access to create impactful insights? 	<ul style="list-style-type: none"> • How are HDI privacy issues identified, communicated, escalated and resolved? • What continuous learning cycles are in place to improve our program?
--	--

Capability level descriptions — PP1

<ul style="list-style-type: none"> • HDI privacy policy is formally in place. • Although policy is in place, non-existent or inconsistent processes often require heroic efforts to comply with the policy. 	<ul style="list-style-type: none"> • Key HDI privacy policy supporting processes are defined and used for organizational data repositories and data flows. • Privacy incidents/breaches are investigated, but inconsistently. • Privacy impact assessments are performed, but inconsistently. 	<ul style="list-style-type: none"> • HDI privacy framework has been defined and provides overall direction and guidance on implementing the policy. • Formal processes for the management of personal health information data incidents/breaches are in place. • Privacy-related processes cover the full life cycle from data sources to data users, sharing, use and archiving. • Data sharing agreements contain provisions for privacy. • HDI privacy audit process is in place. 	<ul style="list-style-type: none"> • HDI privacy policy and processes are coordinated and implemented consistently in accordance with the HDI privacy framework. • A proactive approach to privacy is a core component of the HDI privacy framework (e.g., privacy by design). • Efforts have been started to coordinate/harmonize HDI privacy framework with key partner organizations associated with the related data sets and data flows. • Compliance to HDI privacy policy and processes is monitored continuously and automated to a large extent.
	<ul style="list-style-type: none"> • Direct users of sensitive data are familiar with the HDI privacy policy and processes. 	<ul style="list-style-type: none"> • All those who must know about HDI privacy policy and processes are properly informed. 	<ul style="list-style-type: none"> • Data sharing agreements are monitored for compliance with privacy policy. • HDI privacy audit repository and analytics are in place.
	<ul style="list-style-type: none"> • HDI privacy fluency is limited to those directly involved (e.g., privacy impact assessment, privacy review). 	<ul style="list-style-type: none"> • HDI privacy framework training is in place and available across the organization. 	<ul style="list-style-type: none"> • HDI privacy framework training is in place across the organization attuned to management and staff needs.

PP2: HDI security policies and processes

Capability description — PP2

	HDI security policies and processes	<ul style="list-style-type: none">• Principles, frameworks, policies and processes for security of technology platforms and data flows, including accountability and requirements. Includes data vulnerability (e.g., hackability) and threat risk assessments.• May include security patch management, change of default passwords, periodic penetration tests, audits and remediation.• May span physical and technical		

Capability level descriptions — PP2

<ul style="list-style-type: none"> ● HDI security policy is formally in place. ● Although policy is in place, non-existent or inconsistent processes often require heroic efforts to comply with the policy. 	<ul style="list-style-type: none"> ● Key HDI security policy supporting processes are defined and used to secure organizational data repositories and associated data flows. ● Data security violations are investigated, but inconsistently. ● Threat risk assessments are performed, but inconsistently. 	<ul style="list-style-type: none"> ● HDI security framework has been defined and provides overall direction and guidance on implementing the policy. ● HDI security processes cover the full life cycle from data sources to data users, sharing, use and archiving. ● Formal data security breach/incident management processes are in place. ● HDI security audit and periodic penetration testing processes are in place. 	<ul style="list-style-type: none"> ● HDI security policy and processes are coordinated and implemented consistently in accordance with the HDI security framework. ● A proactive approach to security is a core component of the HDI security framework. ● Compliance to HDI security policy and processes is monitored continuously and automated to a large extent. ● Efforts have been started to coordinate/harmonize HDI security framework with key partner organizations associated with the related data sets and data flows. ● HDI security audit repository and associated analytics are in place.
	<ul style="list-style-type: none"> ● Direct users of sensitive data are familiar with the HDI security policy and processes. ● HDI security policy and processes fluency is limited to those directly involved (e.g., threat risk assessment, security review). 	<ul style="list-style-type: none"> ● All those who must know about HDI security policy and processes are properly informed. ● HDI security framework training is in place and available across the organization. 	<ul style="list-style-type: none"> ● HDI security framework training is in place across the organization attuned to management and staff needs.

PP3: HDI access and sharing policies and processes

Strategic and operational questions to ask — PP3

<ul style="list-style-type: none"> • How are risks managed to achieve both protection (privacy/security) of sensitive health data and enabling access to create impactful insights? • How well are we meeting our information sharing commitments (timeliness, quality)? How can we meet these commitments without inappropriately impacting privacy and security? 	<ul style="list-style-type: none"> • How do we consistently ensure that the appropriate authorities, consent and social licence are in place for the collection, use and disclosure of the data for intended purposes? • What continuous learning cycles are in place to improve our program?
--	---

Capability level descriptions — PP3

<ul style="list-style-type: none"> • DAS policy is formally in place. • Although policy is in place, non-existent or inconsistent processes often require heroic efforts to comply with the policy. 	<ul style="list-style-type: none"> • Key DAS processes are defined and used for organizational data repositories and associated data flows. • Data access varies with data sets and is implemented inconsistently. • Data sharing agreements, when used, are implemented inconsistently. 	<ul style="list-style-type: none"> • DAS framework has been defined to implement the policy and provides overall direction and guidance on managing DAS holistically. • A comprehensive set of DAS processes and associated templates and guidelines is in place based on the framework. 	<ul style="list-style-type: none"> • DAS policy and processes are coordinated and implemented consistently in accordance with the DAS framework. • Efforts have been started to coordinate/harmonize DAS processes, technology and standards with key partner organizations.
	<ul style="list-style-type: none"> • Internal custodians of organizational data sets are familiar with the DAS policies and processes. 	<ul style="list-style-type: none"> • Formal data access violation management process is in place. • Data access audit processes are in place. • DAS framework is used on all organizational/sensitive data sets and data flows. 	<ul style="list-style-type: none"> • Compliance to DAS policy and processes is monitored continuously and automated to a large extent. • DAS audit repository and analytics are in place.
	<ul style="list-style-type: none"> • DAS fluency is limited to those directly involved (e.g., organizational data sets' internal custodians). 	<ul style="list-style-type: none"> • Internal custodians of organizational data assets are familiar with the DAS framework. 	<ul style="list-style-type: none"> • DAS framework training is in place across the organization attuned to management and staff needs.

AS1: Enterprise HDI assets catalogue and content

Capability description — AS1

	<p>Enterprise HDI assets catalogue and content</p>	<ul style="list-style-type: none"> ● HDI assets under the custodianship of the organization including the inventory and data lineage of these data assets, as well as records of incoming/outgoing data flows. ● Covers both structured and unstructured data assets such as databases, records and documents, as well as reference, master and transactional data. ● Explicit classification of these data sets (or elements thereof) for confidentiality and other controls, may also be included. ● Note that the definition of the data elements in these data assets, as well as the data/record classification framework are provided in the enterprise data model capability (AS3). 	<ul style="list-style-type: none"> ● Enterprise data assets (EDA) management guidelines 	<ul style="list-style-type: none"> ● EDA operations guide ● Data assets inventory ● Linked data assets inventory ● Reference data catalogue ● Data lineage documentation (asset level) ● Data lineage documentation (critical element level)
--	--	--	--	--

Strategic and operational questions to ask — AS1

PK1: HDI stakeholder engagement plan

Capability description — PK1

	HDI stakeholder engagement plan	<ul style="list-style-type: none">•		

Strategic and operational questions to ask — PK1

<ul style="list-style-type: none"> • Are we trusted by key stakeholders (e.g., patients) to collect, use and disclose personal health information? Do we have corresponding communication and engagement in place? 	<ul style="list-style-type: none"> • What are stakeholder communication and engagement approaches that address key operational and strategic risks (to build trust) and increase alignment to key organizational, business, IT and HDI objectives? • How do we engage with key stakeholders (based on influence, impact and interest) consistently and effectively?
---	---

Capability level descriptions — PK1

<ul style="list-style-type: none"> • The organization recognizes that a stakeholder engagement plan on HDI resources and capabilities is required. 	<ul style="list-style-type: none"> • HDI stakeholder engagement plan is in place related to core HDI resources and capabilities core and foundational to the organization. 	<ul style="list-style-type: none"> • HDI stakeholder engagement plan is in place related to most HDI resources and capabilities core, foundational and supplemental to the organization. 	<ul style="list-style-type: none"> • HDI stakeholder engagement plan is in place with key partner organizations on all relevant HDI resources and HDI core, foundational, supplemental and enabling capabilities.
<ul style="list-style-type: none"> • HDI-related stakeholder engagement plan is non-existent or inconsistent, often requiring heroic efforts to get it done. 	<ul style="list-style-type: none"> • HDI stakeholder engagement is limited to organization units directly involved in the core HDI resources and capabilities. 	<ul style="list-style-type: none"> • HDI stakeholder engagement is also used for introducing enabling HDI capabilities to stakeholders. 	<ul style="list-style-type: none"> • Stakeholders are involved, where appropriate, in decisions related to HDI activities.



SG2: Strategic HDI governance model

Capability description — SG2

	Strategic HDI governance model	<ul style="list-style-type: none"> • Structure of HDI governance, including internal and external stakeholders for strategic direction, oversight, escalation and decision-making to 		
--	--------------------------------	---	--	--

Strategic and operational questions to ask — SG2

- | <ul style="list-style-type: none">• How is the corporate strategy aligned to the business, IT, HDI and other strategies and roadmaps? | |
|---|--|

SG3: Operational HDI governance model

Capability description — SG3

Capability level descriptions — SG3

<ul style="list-style-type: none"> ● HDI operational governance, including accountabilities, roles and responsibilities, is articulated, but not as a separate governance structure. 	<ul style="list-style-type: none"> ● HDI operational governance is partially in place, with organization units responsible for specific HDI assets (e.g., operational databases) and HDI capabilities (e.g., privacy policy, data sharing agreements, data standards). 	<ul style="list-style-type: none"> ● HDI operational organization units are in place, each with a well-defined mandate, and responsible for a number of HDI assets and/or capabilities. ● HDI operational units also have specific responsibilities for addressing HDI aspects of core business/IT operational initiatives, as well as HDI-specific initiatives aimed at enabling an insight-driven organization. 	<ul style="list-style-type: none"> ● HDI operational organization units receive guidance from and periodically report back to the HDI strategic governance body on progress against the HDI roadmap, including deliverables, realization of benefits, tracking of timelines and costs, and compliance with agreed-upon decisions. ● HDI operational organization units have responsibilities that reach beyond the organization to include key partner organizations (e.g., responsibility for health data standards across ministries and agencies).
<ul style="list-style-type: none"> ● HDI operational governance is subsumed within the existing business and/or IT operational governance model. 	<ul style="list-style-type: none"> ● Focus of HDI operational governance is limited to key HDI assets and capabilities critical to the core business/IT operational initiatives. 	<ul style="list-style-type: none"> ● These HDI operational organization units are collectively accountable for the implementation of the approved HDI roadmap and associated strategic initiatives. 	<ul style="list-style-type: none"> ● HDI operational organization units are also responsible for the HDI workforce capability and capacity required to meet the strategic and operational needs of the organization.

SG4: HDI risk management

Capability description — SG4

	HDI risk management			

Strategic and operational questions to ask — SG4

<ul style="list-style-type: none"> • How can using data and information allow us to prevent “fres” (versus fighting them)? • What is the risk to our long-term outcomes of not better using our data and information? 	<ul style="list-style-type: none"> • What is our current exposure to negative risks (e.g., harms resulting from breaches) and what mitigation strategy do we have in place? • What is our exposure to positive risks (e.g., failure to realize benefits from sharing data in a timely manner)? Could we minimize those without increasing the negative risks beyond our risk tolerance?
---	---

Capability level descriptions — SG4

<ul style="list-style-type: none"> • An overarching framework for DRM covering data privacy, security, 			

AS3: Enterprise data model

Capability description — AS3

Enterprise data model (EDM)		<ul style="list-style-type: none"> • Enterprise-level conceptual, logical and physical models of the health data assets managed by the enterprise, providing a common, consistent view of data across the enterprise and of their interrelationships. • Includes diagrams (e.g., entity/relationship diagrams, class diagrams), business data glossary and technical data dictionaries, as well as classification frameworks for data sets and electronic records (e.g., related to confidentiality). 	<ul style="list-style-type: none"> • Enterprise information architecture framework and guidelines • Enterprise data modelling guidelines • Master data management framework and guidelines • Reference data management framework and guidelines • Electronic record classification framework and guidelines 	<ul style="list-style-type: none"> • Enterprise information architecture • Conceptual data model • Logical data model • Physical data models • Business data glossary • Technical data dictionaries • Metadata and reference data dictionaries
-----------------------------	--	---	--	---

Strategic and operational questions to ask — AS3

Capability level descriptions — AS3

<ul style="list-style-type: none"> • Data modelling is emerging as a practice with a program or project perspective. • Data models (conceptual, logical and/or physical) may be generated within the context of specific information system or data analytics 			

AS4: Enterprise HDI insights practices

Capability description — AS4

	<p>Enterprise HDI insights practices</p>	<ul style="list-style-type: none"> • Health data analytics assets of the organization (e.g., analytics platforms, data warehouses), as well as the suite of analytics practices in place to provide trustworthy decision support, business intelligence (including data visualization). • Also includes the generation of indicators, metrics, algorithms and reports as required by the organization. • Incorporates considerations for ethics in the interpretability, bias and impact of generated insights. • Note that enterprise HDI insights must comply with privacy, security and DRM policies. 	<ul style="list-style-type: none"> • Enterprise data analytics framework and guidelines • Analytics preparation guidelines • Data visualization guidelines • Analytics release guidelines 	<ul style="list-style-type: none"> • Indicator inventory • Algorithms inventory
--	--	--	---	---

Strategic and operational questions to ask — AS4

<ul style="list-style-type: none"> • How do we adopt and adapt to emerging trends in insights in alignment with our scope, strategy and mandate? 	<ul style="list-style-type: none"> • How do we manage the total cost/benefit of maintaining and developing insights? • What are gaps in our analytic capability to achieve our mandate? How do we gain access to close those gaps (virtually or physically)? • How do we facilitate creation of insights for our organization through improved self-service based on EDA? How do we extend this appropriately to partners seeking access?
---	--

Capability level descriptions — AS4

<ul style="list-style-type: none"> • The organization recognizes that insights from data analytics are essential to the organization and should be managed at the enterprise level. 	<ul style="list-style-type: none"> • Key data analytics practices are in place. 	<ul style="list-style-type: none"> • An enterprise data insights (EDI) framework is in place integrating enterprise-level data analytics methods and covering the full analytics life cycle (requirements, collection, preparation, integration, analysis, visualization/reporting, insights). 	<ul style="list-style-type: none"> • Enterprise data analytics activities are coordinated and implemented consistently across the organization in accordance with the EDI framework.
<ul style="list-style-type: none"> • Data analytics practices are non-existent or performed inconsistently, often requiring heroic efforts to get it done. 	<ul style="list-style-type: none"> • Data analytics activities are mostly limited to data from core corporate data sets. 	<ul style="list-style-type: none"> • EDI artefacts (e.g., study frameworks, linked analytics data sets, algorithms, data visualization, reports, indicators) are being generated and cover a material portion of the organization data, and are used on all associated programs and projects. 	<ul style="list-style-type: none"> • Efforts have been started to coordinate/harmonize EDI with key partner organizations associated with and/or impacted by the enterprise data analytics activities.
	<ul style="list-style-type: none"> • Data analytics fluency is limited to organization units directly involved in these activities. 	<ul style="list-style-type: none"> • EDI training is in place across the organization attuned to staff needs. 	<ul style="list-style-type: none"> • EDI training is in place across the organization attuned to management and staff needs.

Supplemental capabilities

SG6: HDI program management

Capability description — SG6

	HDI program management			

Strategic and operational questions to ask — SG6

<ul style="list-style-type: none">• Not applicable	<ul style="list-style-type: none">• How do we adopt a culture of continuous improvement in our data and information operations? What (core and foundational) capabilities need to be improved to realize sustained trust, timeliness and value from our investments and achieve our objectives?

Capability level descriptions — SG6

SG7: HDI policies compliance and audit

Capability description — SG7

	<p>HDI policies compliance and audit</p>	<ul style="list-style-type: none"> ● Framework for the review of compliance with legislation, organization policies, strategic and operational decisions, including data standards, and quality and privacy policy ● May include practices for spot checks, remediation, communication and active learning from data policy compliance issues encountered ● May also include interaction with regulatory or international bodies for periodic or mandatory reporting (e.g., privacy commissioners, OECD) 	<ul style="list-style-type: none"> ● Data policies compliance and audit (DPCA) framework and guidelines 	<ul style="list-style-type: none"> ● Data policy catalogue ● DPCA reports
--	--	---	--	---

Strategic and operational questions to ask — SG7

<ul style="list-style-type: none"> ● How are HDI policies incorporated into the board's audit and compliance program? 	<ul style="list-style-type: none"> ● How are HDI issues of audit or compliance identified, communicated, escalated and resolved?
--	---

PP4: Data life cycle policies and processes

Capability description — PP4

	Data life cycle policies and processes	<ul style="list-style-type: none">• Principles, frameworks, policies and processes for managing the full life cycle of data and records for their use locally and with trusted partners for further value generation• Includes data collection and preparation to support the collection, parsing, cleansing, remediation and storage of data to enable it to be		

Strategic and operational questions to ask — PP4

<ul style="list-style-type: none"> • Not applicable 	<ul style="list-style-type: none"> • How are business, data and IT policies defined and aligned across the data life cycle: creation, flow, collection, storage, use and destruction? • How do we manage/minimize data duplication to maintain its integrity to the authoritative data sources?

Capability level descriptions — PP4

<ul style="list-style-type: none"> • Policy framework for electronic records and data assets is formally in place. 	<ul style="list-style-type: none"> • Some key DLCM policies and 		

PP5: Data standards policies and processes

Capability description — PP5

	Data standards policies and processes	<ul style="list-style-type: none">Principles, frameworks, policies and processes for the adoption and deployment of data content standards (e.g., ICD-10, SNOMED-CT), data exchange standards (e.g., HL7 FHIR), master data (e.g., person, facility, provider) and associated		

Capability level descriptions — PP5

<ul style="list-style-type: none"> • DSM policy is formally in place to guide the data standards life cycle within the organization, including the selection, customization, implementation and eventual deprecation and/or replacement of data standards and associated specifications. • Although policy is in place, nonexistent or inconsistent processes often require heroic efforts to comply with the policy. 	<ul style="list-style-type: none"> • Key DSM processes (e.g., data standard/specification selection, customization and implementation processes) are defined to implement the policy and are used for organizational data repositories and associated data flows. 	<ul style="list-style-type: none"> • A DSM framework has been defined to provide overall direction and guidance for managing data standards and associated specifications, and their impacts across data sets, data flows, data sources and data users, all in alignment with the data standards policy, HDI strategic plan and enterprise architecture. 	<ul style="list-style-type: none"> • DSM policy and processes are coordinated and implemented consistently in accordance with the DSM framework.
	<ul style="list-style-type: none"> • DSM processes are applied to various degrees, mostly for those related to data in large, organizational data sets. • Most custodians of organizational data assets are familiar with the DSM policy and processes. 	<ul style="list-style-type: none"> • A comprehensive set of DSM processes and associated templates and guidelines is in place based on the framework. • DSM is used on all organizational/sensitive data sets and data flows affected by the data standards and associated specifications. • Internal custodians of organizational data assets and data flows are familiar with the DSM framework. 	<ul style="list-style-type: none"> • Efforts have been started to coordinate/harmonize the DSM framework with key partner organizations associated with the affected data sets and data flows. • Compliance to DSM policy and processes is monitored and reported.
	<ul style="list-style-type: none"> • DSM fluency is limited to those who most benefit from its use. 	<ul style="list-style-type: none"> • DSM framework training is in place across the organization attuned to staff needs. 	<ul style="list-style-type: none"> • DSM framework training is in place across the organization attuned to management and staff needs.

PP6: HDI quality policies and processes

Capability description — PP6

	HDI quality policies and processes	<ul style="list-style-type: none">Principles, frameworks, policies and processes for asserting the relevance		

Capability level descriptions — PP6

PP7: Data anonymization policies and processes

Capability description — PP7

<p>Data anonymization policies and processes</p>		<ul style="list-style-type: none"> Principles, frameworks, policies and processes for the anonymization and de-identification of data to appropriate levels, including open data Considers risks associated with granular data for insights and risk likelihood/impact of privacy breaches, includes practices for re-identification in appropriate scenarios 	<ul style="list-style-type: none"> HDI anonymization, de-identification and re-identification framework and guidelines Open data framework 	<ul style="list-style-type: none"> HDI anonymization, de-identification and re-identification policy Open data policy Open data catalogue
--	--	---	--	--

Strategic and operational questions to ask — PP7

<ul style="list-style-type: none"> Not applicable 	<ul style="list-style-type: none"> What practices, policies and culture do we have in place to minimize the risk of unauthorized re-identification within our organization and with partners?
--	--

PP9: Data change management policies and processes

Capability description — PP9

	<p>Data change management (DCM) policies and processes</p>	<ul style="list-style-type: none"> • Principles, frameworks, policies and processes for managing and coordinating changes in data and data flows within and across systems and organizations • Includes interaction across decision-making authorities and updates to core artefacts to retain knowledge 	<ul style="list-style-type: none"> • DCM framework and guidelines • Data change planning guidelines • Data change impact assessment guidelines 	<ul style="list-style-type: none"> • DCM policy • Data change impact assessments
--	--	--	---	--

Strategic and operational questions to ask — PP9

<ul style="list-style-type: none"> • Not applicable 	<ul style="list-style-type: none"> • How do we get a thorough understanding of the direct and indirect impacts and costs associated with proposed changes (to the current data infrastructure)? Have we considered various/other options for how the changes may be made?
--	--

Capability level descriptions — PP9

<ul style="list-style-type: none"> • DCM policy is formally in place to guide the changes to the data life cycle, including the creation, revision, replacement and/or deprecation of data sets and/or data flows. 	<ul style="list-style-type: none"> • Key DCM processes (e.g., data lineage analysis, data life cycle impact analysis [intake, preparation, linking, etc.], data sharing agreements impact analysis) are defined and used for organizational data repositories and associated data flows. 	<ul style="list-style-type: none"> • A DCM framework has been defined to provide overall direction and guidance for managing data changes and their impacts across data sets, data flows, data sources and data users, all in alignment with the DCM policy, HDI strategic plan and enterprise architecture. 	<ul style="list-style-type: none"> • DCM policy and processes are coordinated and implemented consistently in accordance with the DCM framework.
<ul style="list-style-type: none"> • Although policy is in place, nonexistent or inconsistent processes often require heroic efforts to comply with the policy. 			

PP11: Indigenous populations data policies and processes

Capability description — PP11

	Indigenous populations data policies and processes	<ul style="list-style-type: none">• Principles, frameworks, policies and processes for the treatment of Indigenous populations data (First Nations, Inuit and Métis) aligned with their principles for data acquisition, storage, access and use	<ul style="list-style-type: none">• Indigenous populations data management (IPDM) framework and guidelines	<ul style="list-style-type: none">• IPDM policy

Capability level descriptions — PP11

•			

PK3: HDI workforce plan

Capability description — PK3

	HDI workforce plan	<ul style="list-style-type: none">• Approach, effort and timetable for meeting the organization's requirements for HDI capacity to achieve its mandate with regard to HDI management, analytics, security, privacy, etc.• Considers assessment of supply and demand		

Capability level descriptions — PK3

<ul style="list-style-type: none">• The organization recognizes that advancing its HDI workforce capacity is required.• HDI workforce planning is nonexistent or inconsistent,			

PK4: HDI fluency program

Capability description — PK4

	HDI fluency program	<ul style="list-style-type: none">• Education curriculum, approach and modules to align target audience (e.g., employees, management, board) on key topics related to data and information		

Capability level descriptions — PK4

<ul style="list-style-type: none"> ● HDI-related training is nonexistent or inconsistent, often requiring heroic efforts to get it done. 	<ul style="list-style-type: none"> ● The organization recognizes that advancing its HDI fluency is required. ● HDI fluency program is in place to address the core and foundational HDI capability training needs of the organization. 	<ul style="list-style-type: none"> ● HDI fluency program is in place to address the core, foundational and supplemental HDI capability training needs of the organization to support the HDI roadmap. ● Expansion of HDI fluency program is being considered for introducing enabling HDI capabilities. 	<ul style="list-style-type: none"> ● HDI fluency program is in place not only to support the HDI capabilities core, foundational and supplemental to the organization but also the enabling HDI capabilities that have tremendous value potential to the organization in support of the HDI roadmap. ● Efforts have been started to share and harmonize HDI fluency program modules with key partners.
	<ul style="list-style-type: none"> ● HDI fluency training is limited to organization units directly involved with HDI resources and analytics. 	<ul style="list-style-type: none"> ● HDI fluency training is in place across the organization attuned to staff needs. 	<ul style="list-style-type: none"> ● HDI fluency training is in place across the organization attuned to management and staff needs.

Enabling capabilities

SG5: HDI project life cycle

Capability description — SG5

	<p>HDI project life cycle</p>	<ul style="list-style-type: none"> • Extension of the standard project life cycle (e.g., software development, vendor software implementation) to integrate with strategic and operational accountability models for HDI • Includes project roles for HDI accountabilities and artefacts, covering HDI requirements, data models, specifications, configuration and conversion, as well as accountability for transition to post-project HDI management and governance 	<ul style="list-style-type: none"> • Business intelligence/data warehouse project life cycle methodology • Data analytics project life cycle methodology • Information management impact assessment methodology 	<ul style="list-style-type: none"> • Data project artefacts (e.g., requirements) • Updated operational data artefacts (e.g., glossary) • Information management impact assessments
--	-------------------------------	--	--	---

Strategic and operational questions to ask — SG5

Capability level descriptions — SG5

<ul style="list-style-type: none"> • The need for a data project life cycle (DPLC) for data-centric projects has been recognized. 	<ul style="list-style-type: none"> • A formal DPLC has been developed with extensive participation from business and IT for complex data-centric projects. 	<ul style="list-style-type: none"> • Variants of the DPLC, such as data analytics project life cycle and business intelligence project life cycle, are being drafted and piloted. 	<ul style="list-style-type: none"> • Variants of the DPLC, such as the data analytics project life cycle and the business intelligence project life cycle, are companion methodologies to the organization's standard project life cycle methodology.
<ul style="list-style-type: none"> • Initial steps have been taken to embody elements of the DPLC within the standard project life cycle. 	<ul style="list-style-type: none"> • DPLC is used mostly on large, organizational data-centric/ analytics-focused projects. 	<ul style="list-style-type: none"> • DPLC is used on a growing number of data-centric/ analytics-focused projects. 	<ul style="list-style-type: none"> • DPLC is used on most data-centric/ analytics-focused projects.
	<ul style="list-style-type: none"> • DPLC fluency is limited to those directly involved in these projects. 	<ul style="list-style-type: none"> • DPLC fluency level is growing in the data-oriented parts of business programs and IT organization. • All those who must know about the DPLC are properly informed. 	<ul style="list-style-type: none"> • DPLC training is in place across the organization attuned to management and staff needs. • Where relevant, efforts have been started to coordinate/harmonize the DPLC and its variants with key partner organizations.

PP8: HDI-related intellectual property policies and processes

Capability description — PP8

	HDI-related intellectual property policies and processes	<ul style="list-style-type: none"> Principles, frameworks, policies and processes for management and recognition of intellectual property (IP) of HDI-related products, including publication rights and sharing of value 	<ul style="list-style-type: none"> HDI-related IP management guidelines (including infringement guidelines) 	<ul style="list-style-type: none"> HDI-related IP policy Organization patents, copyrights and trademarks

Strategic and operational questions to ask — PP8

<ul style="list-style-type: none"> Not applicable 	<ul style="list-style-type: none"> How well protected is our IP related to our data and information assets (including insights and algorithms)? How could we generate a revenue stream from some of our IP? What IP should be generally available and open?

Capability level descriptions — PP8

• HDI-related IP policy is formally in place to guide the management of the organization's IP as well as			

AS5: Enterprise advanced analytics practices

Capability description — AS5

	Enterprise advanced analytics practices	<ul style="list-style-type: none">● Application of advanced analytics practices such as machine learning, artificial intelligence and predictive analytics, as well as testing for the generation of valuable insights to the organization● Incorporates considerations for ethics in the interpretability, bias and impact of generated insights	<ul style="list-style-type: none">● Advanced analytics ethical code of	

Capability level descriptions — AS5

<ul style="list-style-type: none"> • The organization recognizes that advanced analytics practices have tremendous value potential for the organization and warrant formal review and assessment. 	<ul style="list-style-type: none"> • Specific advanced analytics practices with value potential to the organization (e.g., natural language processing, machine learning, predictive analytics, advanced statistics) have been formally reviewed and assessed. 	<ul style="list-style-type: none"> • Enterprise data insights (EDI) framework has been augmented with selected advanced analytics practices (e.g., natural language processing, machine learning, predictive analytics, advanced statistics). 	<ul style="list-style-type: none"> • Advanced analytics practices are coordinated and implemented consistently across the organization in accordance with the EDI framework.
<ul style="list-style-type: none"> • Advanced analytics practices are nonexistent or inconsistent and, if used, often require heroic efforts to get value from them. 	<ul style="list-style-type: none"> • Specific advanced analytics practices are at the proof-of-concept stage. • Advanced analytics fluency is limited to organization units directly involved in the advanced analytics practices reviews, assessments and proof-of-concept activities. 	<ul style="list-style-type: none"> • Advanced analytics artefacts are captured and catalogued in the EDI artefacts repository and deliver tangible value to the organization. 	<ul style="list-style-type: none"> • Efforts have been started to coordinate/harmonize the use of advanced analytics practices and share advanced analytics artefacts (e.g., algorithms) with key partner organizations. • Advanced analytics training is in place across the organization attuned to management and staff needs.

PK5: HDI capability improvement program

Capability description — PK5

	HDI capability improvement program	<ul style="list-style-type: none"> Establishment and ongoing operation of an HDI capability improvement program that includes periodic current capability assessment, target capability requirements to meet business needs, capability gap analysis and capability gap closure plan 	<ul style="list-style-type: none"> HDI capability framework and guidelines 	<ul style="list-style-type: none"> HDI capability assessment HDI target capability roadmap HDI network capability assessment

Strategic and operational questions to ask — PK5

<ul style="list-style-type: none"> Not applicable 	<ul style="list-style-type: none"> What (foundational) capabilities need investment to support our organizational strategy? What are opportunities to harmonize with partners to reduce costs and increase timeliness of insights?

Capability level descriptions — PK5

<ul style="list-style-type: none"> • The organization recognizes that advancing its HDI capabilities has tremendous value potential and warrants formal assessment. • HDI capability improvement is nonexistent or inconsistent, often requiring heroic efforts to get it done. 	<ul style="list-style-type: none"> • Specific HDI capabilities of high value potential to the organization have been selected and a capability improvement plan has been designed for them. • HDI capability assessment and improvement frequency is limited to organization units directly involved in the HDI capability assessment and improvement planning activities. 	<ul style="list-style-type: none"> • HDI capabilities core, foundational and supplemental to the organization are being implemented as per the HDI capability improvement plan. • Enabling HDI capabilities are being investigated for their value potential to the organization. 	<ul style="list-style-type: none"> • Enabling HDI capabilities are being implemented as per the HDI capability improvement plan. • Efforts have been started to coordinate/harmonize HDI capabilities with key partner organizations. • HDI capability assessment and improvement training is in place across the organization attuned to management needs.
---	--	---	--



CIHI Ottawa

495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto

4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria

880 Douglas Street
Suite 600