

HEALTHCARE INFORMATION GOVERNANCE





INTRODUCTION

AS CANADIAN HEALTHCARE ORGANIZATIONS WORK TO IMPROVE PATIENT CARE, GAIN VALUABLE INSIGHT INTO PATIENT DATA, REMAIN COMPLIANT WITH APPLICABLE REGULATIONS AND MAINTAIN DATA SECURITY, IMPLEMENTING TRUE DIGITAL HEALTH IS TOP OF MIND FOR MANY. HOWEVER, IN ORDER TO ACHIEVE THIS, CANADIAN HEALTHCARE ORGANIZATIONS MUST FIRST OVERCOME SOME SIGNIFICANT AND COMPLEX CHALLENGES.

According to a report by the Fraser Institute¹, while Canada is among the most expensive universal-access health-care systems in the OECD countries, its performance, in terms of availability and access to resources, is modest to poor in comparison to other OECD countries.

While approximately 85% of primary care physicians are now leveraging EMR's in their practice, fully integrated patient health data from other sources is often not integrated into that EMR due to lack of interoperability with labs, hospital and pharmacy systems.

One of the key impacts of COVID 19 was the challenge clinicians and administrators dealt with to provide care during the pandemic. The changes that were forced upon primary care physicians, hospitals, labs, etc. escalated long overdue change. Virtual care is now a core part of our publicly-funded health delivery system. Recognition that key health information components – diagnostic test results, prescriptions, consults, and referrals – should always be created in a usable digital format. And technology infrastructure needs to be supported by expanded IT with equitable access a priority. Underlying all of those changes is still the requirement for privacy and security of that patient data.²

¹ Barua, Bacchus, et al. "Comparing Performance of Universal Health Care Countries, 2021". Fraser Institute, <https://www.fraserinstitute.org/studies/comparing-performance-of-universal-health-care-countries-2021>

² https://www.canada.ca/content/dam/hc-sc/documents/corporate/transparency_229055456/health-agreements/bilateral-agreement-pan-canadian-virtual-care-priorities-covid-19/template-wf-report-eng.pdf

COVID 19 has exacerbated the revenue loss and budgetary issues hospitals have experienced for the past several years. Prior to the pandemic, Canadian healthcare organizations had been dealing with shrinking budgets yet, they needed to invest in costly EHRs and the required digital technology, while trying to move away from an over dependence on paper and physical records. In addition, the increasing focus on data science, analytics and artificial intelligence in healthcare continues to add further pressure for Canadian healthcare organizations to ensure data quality and integrity. In order to overcome these challenges and successfully adopt digital health, Canadian healthcare organizations need Information Governance.

Information Governance (IG) establishes a framework that manages information in all forms throughout its lifecycle. This is important as healthcare organizations work to achieve goals such as value-based care and population health management. However, these initiatives are only possible if organizations can securely and consistently share trusted information in a usable and actionable format. In order to achieve this, Canadian healthcare organizations need to apply strategies in the following areas:

- **Information Governance:** the “rules of the road” for how the organization intends to manage its information assets.
- **Information interoperability:** the ability of two or more systems to exchange and use information.
- **Enterprise lifecycle management:** management of the range of information assets, physical and electronic, across the enterprise including design, acquisition, processing use and disposition.
- **Information and data quality:** methods for assessing and improving the quality of data and information with quality defined as validity, accuracy, completeness and timeliness.





Information Governance (IG) is an approach to managing information through processes, roles, controls and metrics to collect, organize, utilize and secure data. This includes managing information throughout its lifecycle and supporting the healthcare organization's strategy, operations, regulatory, legal, risk and environmental requirements.

Having reliable and trusted information is more important in healthcare than ever before. This is not only because reliable, trusted information is needed to provide quality patient care but also because it is necessary to keep up with evolving delivery models, changing security risks, and regulatory demands.


IG helps Canadian healthcare organizations achieve:

- > safe, quality patient care
- > population health management
- > operational effectiveness
- > regulatory compliance
- > cybersecurity
- > cost efficiency



**AN IG PROGRAM SHOULD
ESTABLISH ENTERPRISE-WIDE
POLICIES, PROVIDE STANDARD
PROCESSES, AND PROTECT
INFORMATION WITH APPROPRIATE
CONTROLS.**

Before any healthcare organization begins their IG journey, an assessment must first be conducted to determine the present state of IG maturity and to then strategically plan for what steps would be needed to advance towards a mature IG adoption model. *[Iron Mountain's Healthcare Information Governance \(HCIG\) framework](#)* can not only help you with this self-assessment but also help your healthcare organization reach IG maturity.



WHAT IS HCIG AND HOW DOES IT WORK?

Iron Mountain's Healthcare Information Governance (HCIG) is a framework that offers a comprehensive and flexible approach to IG and helps healthcare organizations cost-effectively:

- > **govern all types of information, independent of format/location, in a consistent and coordinated manner**
- > **secure information across its lifecycle and the organization's ecosystem, including data and IT governance**
- > **address data privacy and integrity, mitigating risks of breach, to extract the most value from the information**

This organization-wide framework manages and leverages information as a strategic asset throughout its lifecycle in order to support strategy, regulatory, legal, risk and environmental requirements. It is comprised of 10 organizational competencies and 85+ indicators critical in understanding and advancing IG maturity across your healthcare organization's ecosystem.

HCIG uses [™], the industry's only purpose-built assessment and measurement platform for IG adoption and maturity, which enables you to map your current IG practices, processes and polices against the HCIG framework to assess and evaluate how information is created, used, managed and secured across your healthcare organization using a five index rating scale. You'll gain greater insight into your current capabilities and establish a baseline for pursuing and measuring meaningful improvement.

With the help of IGHealthRate[™], you'll take a crucial first step in understanding and advancing your IG maturity so you can leverage information as a strategic asset to:

- > **improve patient outcomes**
- > **deliver data-driven decision-making**
- > **mitigate compliance and security risks**
- > **leverage clinical, financial and administrative information for analytics and insights**
- > **streamline business processes, improve productivity and reduce operating costs**
- > **deliver value-based care and population health readiness**

Completing the assessment will help you not only identify your organization's state of IG maturity, it will also help you prioritize your IG agenda, and identify gaps in your IG practices so that you can determine high risk areas and prioritize to strategically ensure risk avoidance.

THE 10 COMPETENCIES OF IGHEALTHRATE™

The 10 competencies are an important part of the IGHealthRate™ assessment process and crucial in helping you not only gauge your healthcare organization's IG maturity but also identify gaps and areas of vulnerability that need to be addressed.

The 10 competencies the IGHealthRate™ assessment will measure your organization against include:

- 1 IG Structure**
- 2 Strategic Alignment**
- 3 Enterprise Information Management**
- 4 Privacy and Security**
- 5 Legal and Regulatory**
- 6 Data Governance**
- 7 IT Governance**
- 8 Analytics**
- 9 IG Performance**
- 10 Awareness and Adherence**

These competencies address a healthcare organization's programmatic structures for the adoption, implementation, and development of IG. Canadian healthcare organizations of all types and sizes will find utility and applicability in this model. Furthermore, the flexibility and scalability promotes a natural progression of improvement and maturity.



COMPETENCY #1: IG STRUCTURE

In order to achieve any of the benefits IG can provide to a healthcare organization – including improving patient outcomes, mitigating security and privacy risks, and achieving integrated system of care objectives, for example – a structured approach to IG is needed.

This competency addresses the organizational and programmatic structures for the adoption, implementation and development of IG and ties together the areas of enterprise information management (EIM), data governance (DG) and IT governance (ITG).

Key components to establishing this structure for IG include an executive sponsor, an IG leader (for example, a chief information governance officer or chief data science officer), as well as some kind of an oversight committee such as an IG executive committee. The successful implementation of IG requires accountability and decision-making as well as obtaining support from leadership.

Furthermore, maintaining a successful IG program also requires oversight and mechanisms for decision-making as well as accountable leaders who will ensure the development and stewardship of the organization's information assets.

The maturity markers for the IG structure competency include:

Executive sponsorship for IG is formally established and communicated throughout the organization.

A qualified IG leader is leading the IG program.

Trained staff, a team of professionals, are dedicated to IG.

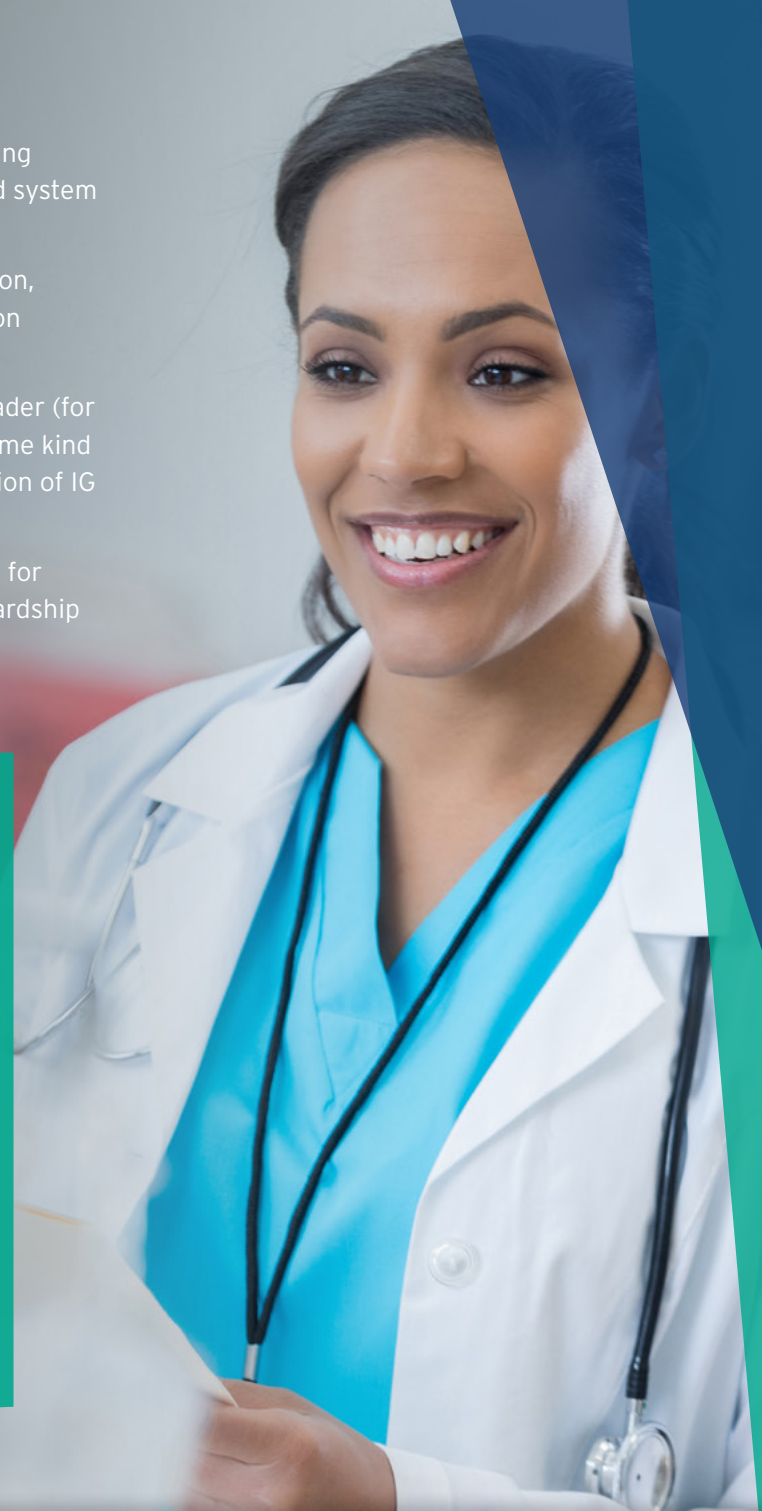
An **IG oversight committee** is the organization's source of guidance for strategic direction for the enterprise-wide IG program.

IG policies, program and purpose are aligned with goals for the organization's strategic use of information.

Integration of key program structures including EIM, DG and ITG to facilitate the optimal use and management of information for patient care and business purposes.

IG roles and responsibilities are formally documented and operationalized at all levels of the organization.

Funding, both operational and capital funds, are allocated to support the IG program.





COMPETENCY #2: STRATEGIC ALIGNMENT

Strategic alignment takes stock of information at every stage of the lifecycle and addresses both internal and external use. Since information is an organizational asset, strategic alignment is necessary in order to realize the information's full value. This means ensuring information is used in a way that is aligned with an organization's mission, vision, values, and strategies; whether that information is being used internally or externally.

This competency addresses the planning and coordination of all information-related activities and the planning for information management. Strategic alignment will also support a data-driven culture and ensures employees at all levels have access to the information needed to make decisions.

The maturity markers for the strategic alignment competency include:

IG is aligned with organizational strategy including the organization's mission, vision and goals.

Information use is a strategic asset that supports informed, timely decision-making to the benefit of the organization, its patients and stakeholders.

Information activation and interoperability practices are developed with internal and external community partners and has a measurable impact on quality of patient care, cost of care, and patient satisfaction.

Consumer-centric information enablement and engagement is done through clear, accessible and trustworthy information.

Social media policies and management protects confidential health information from use on social media.

COMPETENCY #3: ENTERPRISE INFORMATION MANAGEMENT

Enterprise information management (EIM) is one of the core competencies of IG. EIM encompasses policies and processes for managing information across the organization as well as managing information throughout all phases of its lifecycle.

This competency focuses on the tactical implementation of key functions such as information access, security, confidentiality, information integrity and quality, information design and capture, content and records management, and information analysis. This applies to the use of information throughout and within all the departments of the organization as well as the organization's partners.

Furthermore, EIM has an impact on legal and evidentiary needs, regulatory compliance, business and contractual use of information, and coordination of care.

For these reasons, EIM is the backbone for trustworthy, usable, relevant, timely and accurate information as well as for interoperability and trusted information exchange.

The maturity markers for the EIM competency include:

EIM must be established and applied to all types of information, whether physical or digital, on all media formats.

Records and information classification in all forms and formats are organized across the organization.

Information asset inventory is needed of the organization's records and information should be documented and kept up-to-date.

Organization-wide storage management policies and protocols are in place and being implemented.

Electronic clinical systems and EHR governance program are formalized and the workforce is educated on how to advance safe use of health information technology.

Retention and disposition management practices are implemented organization-wide.

Long-term digital preservation program or strategy is fully defined and implemented by the organization to ensure digital information of value remains accessible and usable.

Identity management practices are in place and extend to external partners. These practices include a master patient index, provider index, employee records and other key identities across the organization.

Information exchange and sharing are established as formalized practices to ensure information is shared and exchanged with appropriate and authorized parties.

Information sharing with patients, clients, residents and their representatives are established as formalized practices to ensure authentic, reliable, timely and accurate information is being shared.

Patient information request automation is implemented so that self-service technologies are available to patients to allow them access to the broadest set of personal health information at all times and in the form or format preferred by the individual.



COMPETENCY #4: DATA GOVERNANCE

Data governance (DG) is also one of the core programmatic structures of IG. With data volume, velocity and variety rapidly increasing across all industries data is also becoming increasingly recognized as a strategic asset. However, in order to capitalize on data as a strategic asset, people need to be able to access accurate, complete data in order to deliver quality and safe care, reliable analytics, population health improvements, and care delivery cost reductions.

DG provides the design and execution of data planning for data needs and data quality assurance in concert with the strategic information needs of the organization.

DG supports a data-driven decision-making culture and, ultimately, healthcare organizations will benefit from a structured approach to governing enterprise data throughout its lifecycle to ultimately enable trust in their data and information.

The maturity markers for the DG competency include:

Establishment of a DG program with accountabilities, policies and practices to ensure the availability and quality of the organization's data on all types of media.

Business process data ownership is established and practiced throughout the organization and in each business unit.

Effective use of data stewards for appropriate management of data assets.

Master data management is implemented enterprise-wide in order to define and manage critical data and provide a single point of reference for master data across the organization and in all systems.

Data classification should be established and implemented across the entire organization in order to create a formalized structure for grouping, documenting and tracking data.

Data quality management accountabilities and practices are established to ensure that data meets required quality characteristics and the needs of the organization.

Metadata management practices should be established, continuously monitored and evaluated to ensure alignment with business needs and regulatory requirements.

DG policies and procedures should be clear and well-defined throughout the organization. This will help ensure data quality, metadata management, master data management and data classifications.

COMPETENCY #5: INFORMATION TECHNOLOGY GOVERNANCE

Information technology (IT) governance provides a formal structure for measuring the connection between IT investment and expected results from implemented technologies. It also helps the organization, and stakeholders, understand measurable results produced by using certain technologies. For example, how technology has affected efficiency, workflows, etc.

IT governance will help healthcare organizations promote alignment, use best practices when it comes to selection and deployment of technologies, ensure and measure the benefits of IT investments, mitigate risk, and more.

The maturity markers for the IT governance competency include:

An **IT governance** program is established and aligned with the organization's strategy.

An **IT governance framework** is in place to guide IT strategy, execution, risk mitigation and value creation.

The **IT governance scope** is fully institutionalized and measures the program's effectiveness in innovation of information use, care coordination and advances in population health.

A **change management** process is in place and is monitored.

A **business continuity plan** is in place, is based on industry standards, and is integrated into emergency management plans.

A **disaster recovery** plan is in place to enable information recovery and continuity as quickly as possible in the event of a disaster.

A **mobile device management** program is developed, implemented, followed, communicated and monitored.

E-mail policies and management must be developed, implemented, followed, communicated and monitored.



COMPETENCY #6: ANALYTICS

Analytics is essential to a mature IG program. Data needs to be processed in a meaningful way so that the appropriate information is provided in a relevant situation. The importance of this can't be stressed enough as analytics supports successful clinical and business decision making.

The goal of an IG program is to ensure that all information resources support business goals and this can't be done without the ability to acquire, manage, analyze, interpret and transform data. Analytics is essential to the success of the IG program because it ensures that data is transformed into accurate, consistent and timely information.

The maturity markers for the analytics competency include:

Analytics aligned with organization strategy.

Analytics scope and fit for an organization should align with the organization's role and mission.

Access to analytics tools and resources ensures information is available for use in support of patient care and business decisions across the organization.

Reliability of data for analytics is key to trusting processes and results.

Analytics tools appropriate for organization's scope are in place, available, and utilized.

On demand internal and external reporting are provided to enable compliant self-service and on-demand analytics reporting capabilities.





COMPETENCY #7: PRIVACY AND SECURITY

Privacy and security are crucial for any healthcare organization as well as for a mature IG program. Effective privacy and security helps ensure data and information across the healthcare organization are protected from breaches, corruption and loss as well as ensures information is kept private and confidential.

An important part of governing information is providing secure and appropriate access to information while remaining compliant with laws and regulations as well as industry best practices. This is essential to providing safe, cost-effective care as well as mitigating risk in healthcare organizations.

The maturity markers for the privacy and security competency include:

Administration safeguards are a must for a healthcare organization especially when working collaboratively with external partners.

Technical security safeguards must also be in place to protect information across the organization. Technologies must be routinely audited and monitored on an ongoing basis.

Physical safeguards and a physical security plan specific to information protection must be in place.

Information access management policies and technologies must be in place to ensure users access only the information that is appropriate for their authority and job function.

Information sharing and protections should be supported by policies, processes and technologies as well as fully implemented across the healthcare organization.

Information sharing with business associates should be governed by a set of policies, rules, contracts and enabling technologies to ensure information that is accessed, used, maintained, stored and shared is appropriate and secure.

Incident and breach management should be implemented across the healthcare organizations. A trained incident response team and a proactive monitoring system to prevent privacy and security incidents and breaches should be in place.

Security risk assessment and risk management plans should be up-to-date and include all information assets and outlines the plans for risk remediation.

An **employee sanction process** should be in place and documented to sanction workforce members for violations of policy regarding access, use, disclosure and destruction of all information in any form or format.

Maturity of a privacy and security program is based on an external model or framework that encompasses a set of certified or accredited best practices.

COMPETENCY #8: REGULATORY AND LEGAL

Compliance with legal and regulatory requirements is an important aspect of any healthcare organization's IG program. This means healthcare organizations need to have a deep understanding of laws and regulations. Part of being compliant also means being able to respond to regulatory audit requests, electronic discovery (e-discovery), legal holds, mandatory reporting and releases to patients upon request. All of this should be coupled with effective IG processes to provide for auditing and monitoring in addition to ensuring compliance.

The maturity markers for the regulatory and legal competency include:

Legal and e-discovery response should be done in an accurate and timely manner.

Legal hold response should also be done in an accurate and timely manner.

Chain of custody practices and protocols should be well defined, communicated and established.

Regulatory audit response needs to be consistent and done in an accurate and timely manner.

Mandatory reporting should be consistently responded to in an accurate and timely manner.





COMPETENCY #9: AWARENESS AND ADHERENCE

This competency focuses on ensuring a healthcare organization's workforce are aware of, and adhering to, IG program principles, processes, practices and procedures. The success of a healthcare organization's IG program stems from organization-wide recognition and awareness of the value of IG as well as how it will help the organization accomplish its mission, execute its strategies and achieve its goals.

Guidance should be provided to the workforce about compliant behaviors with respect to the creation, use, handling, access, sharing, storage, retention and disposition of information. This also includes compliance with any required policies, practices, laws and regulations. Formal documentation, training and strategy should be used to help shift workforce behaviors.

The maturity markers for the awareness and adherence competency include:

Awareness and education program scope should not only be enterprise-wide but also reach business partners.

Awareness and education program practices should be role-based and delivered via multiple methods. This includes business partners.

Workforce awareness and adherence with IG practices should be implemented across the organization. This includes ensuring there is adequate training related to IG policies, processes and practices to ensure the workforce understand their responsibilities as they relate to the IG program and compliance.

Trained IG staff should be part of your healthcare organization. Adequate training should be provided to staff working on IG initiatives. This includes data stewards, data owners, organization's leaders and IG analysts.

Consumer and patient awareness of the organization's IG and protection practices that support population health and well-being initiatives.



COMPETENCY #10: INFORMATION GOVERNANCE PERFORMANCE

Monitoring the performance of implemented policies and practices related to IG is key to ensuring healthcare organizations reap the benefits. This competency enables the development of methodology for measuring the performance and impact of an IG program. If IG policies and procedures are not being followed or practiced, then the benefits and return on investment of IG will not be fully realized.

The maturity markers for the Information Governance performance competency include:

Performance of IG goals and objectives should support the healthcare organization's strategic direction.

Measuring IG program effectiveness should include a continuous process for auditing and monitoring the program to gauge the impact and effectiveness.

IG program audit should be a formal process and should be comprehensive, risk-based, closed-loop and conducted annually.

IG program compliance management should include clearly defined policies, procedures and measurements. They should be followed consistently to ensure a standardized, consistent approach to internal and external compliance.

Continuous improvement of IG should be an organization-wide, comprehensive process to ensure continuous quality improvement of the IG program and should include active remediation and reporting.

Personnel performance metrics and measurements should be in place to define responsibilities and accountabilities for IG. This should be incorporated in the healthcare organization's human resources performance management process for all members of the workforce.



HCIG CASE STUDY

ACHIEVING COST SAVINGS WITH IG

In 2018, a healthcare organization in the United States invested in HCIG in order to help them improve efficiencies as well as save money. As many in the healthcare industry know, this is a challenging task.

However, this US healthcare organization witnessed the power of IG at work with HCIG.

They focused their IG project on four areas of the healthcare organization:

- **patient identification**
- **retention management**
- **electronic archival**
- **protected health information storage**

The results they got with HCIG were significant.

RESULTS

- **Reduction of master patient index (MPI):** The healthcare organization was able to reduce duplicates in their MPI from 8% to 0.2% and save over **\$7 MILLION**.
- **Reduction of storage costs:** They reduced their storage costs and saved **\$100,000 IN ANNUAL COSTS**.
- **Reduction of email archival:** The organization reduced their email archival to 69 days and therefore decreased support costs.
- **Risk mitigation of MPI:** Lastly, with new policies and technologies in place, they were able to mitigate the risk of PHI storage on public drives, mitigating risks of a potential breach.



HCIG CASE STUDY

USING IG TO IMPROVE EFFICIENCY, REPORTING AND PATIENT OUTCOMES

The Northern Health Authority, a Canadian healthcare provider, needed a unified, consistent approach to information governance (IG), to enhance overall efficiency, improve data quality, and facilitate regulatory compliance.

TACKLING COMPLEXITY AT THE ROOT

“How you deliver healthcare, and how you create information and data, are closely linked. By helping clinical staff make that connection, IGHealthRate supports our move from paper records towards digital.”

– Andrea Lorette, Lead, Information Governance and Information and Data Hub, Northern Health Authority

RESULTS

The **IGHEALTHRATE** self assessment tool helped establish a baseline for IG performance and develop a roadmap for a centralized, standardized approach across all clinical and business areas.

- An IG maturity assessment baseline was used to set goals and measure future progress
- Establishing data owners and data stewards has increased IG awareness
- IG principles optimized COVID 19 response and ensured a coordinated approach to COVID-19-related analytics
- Looking ahead, data quality will continue to improve as IG best practice becomes embedded and a new information and data quality framework is completed

Read the full case study [here](#)

INFORMATION LIFECYCLE MANAGEMENT AND IG

Information Governance (IG) is essential to secure data management and healthcare compliance. Without IG, managing information throughout its lifecycle and using that information to support the healthcare organization's strategy and operations – as well as meeting regulatory, risk and environmental requirements – is not possible. When it comes to effective information management, a holistic approach is key.

Information lifecycle management (ILM) means more than the creation and, when the time is right, the destruction of information. Effective ILM will enable organizations to not only remain compliant with any applicable laws and regulations, but will also help organizations improve efficiency, ensure security, and get the most out of their data. ILM includes:

- **content creation**
- **application of retention, privacy and classification**
- **digitizing, converting, migrating**
- **integrating workflows**

- **leveraging intelligence and insights**
- **securely storing and accessing information**
- **enabling restoration and disaster recovery**
- **disposing and/or recycling with the help of a secure chain of custody**

Underlying all of this is policy and governance. In order to effectively manage your information, healthcare organizations need regulatory compliance, technologies and policies in place to address internal and external cybersecurity threats as well as recover from them. Organizations also need technologies and policies in place to securely manage personal data throughout its lifecycle.



Click for larger view

GETTING STARTED

To gauge how mature your healthcare organization's IG program is you will need to conduct a self-assessment or leverage an industry assessment tool, such as IGHealthRate™, that engages the wider organization.

To address these challenges and benefit from the outcomes, you could try to undertake your own assessment and define your own path forward. Typically, this would be a major undertaking as you and your organization develop the expertise, set benchmarks, do the assessment and create a plan for better governance. Achievable? Of course. Easy and timely? Probably not.

Alternatively, consider working with Iron Mountain, the industry leader in IG. Our Healthcare Information Governance (HCIG) Advisory Services team can deliver a one day facilitated workshop that provides your executive committee with a baseline IGHealthRate™ assessment. IGHealthRate™ has been developed to quickly deliver a common understanding of the IG challenges while providing clear recommendations on how to improve upon the current practices.

The IG consultant will work with you and your team to develop recommendations to address your gaps and risks, including a tactical roadmap and implementation plan that focuses on maturing your IG program and aligns to strategic priorities. This is all done within the constraints of your budget and resource limitations.

Step 1: You'll need to create an engaged cross-functional committee. The key stakeholders that should be included are the executive leaders in the core functional areas of risk, health information management, privacy, medical services delivery, finance, IT and legal.

Step 2: Set preliminary goals, objectives and timelines. Make sure you're realistic. This isn't a short-term project. Goals and objectives may change once the assessment is complete.

Step 3: Establish a budget framework for a phased approach. An assessment plan should work within your budget and resource limitations.

Step 4: Decide if you're going to work with an industry leader to facilitate your assessment. If you're going it alone, assign a project manager to oversee the assessment.

Let Iron Mountain's Healthcare Information Governance (HCIG) Advisory Services and Solutions support you on your journey to achieving strategic digital health initiatives as well as critical metrics and targets.

Call 1.800.899.4766 to inquire about taking the IGHealthRate™ Assessment

For more information visit





800.899.IRON | IRONMOUNTAIN.CA

© 2022 Iron Mountain Canada Operations ULC. All rights reserved. This document was created by Iron Mountain Canada Operations ULC and its affiliates ("Iron Mountain"), and information provided herein is the proprietary and confidential material of Iron Mountain and/or its licensors which may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the prior written permission of Iron Mountain. Current product or service plans, strategy, release dates, or capabilities are subject to change without notice, and do not represent or imply an invitation or offer, or availability in all countries, and are not intended to be a commitment to future product or feature availability. This document is not sponsored by, endorsed by, or affiliated with any other party, and any customer examples described herein are presented as illustrations of how customers have used Iron Mountain products and services, and do not constitute a further endorsement, affiliation or other association with such customers or other entities referenced herein. Iron Mountain shall not be liable for any direct, indirect, consequential, punitive, special, or incidental damages arising out of the use or inability to use the information. Iron Mountain provides this information AS-IS and makes no representations or warranties with respect to the accuracy or completeness of the information provided or fitness for a particular purpose. "Iron Mountain" is a registered trademark of Iron Mountain, Incorporated in the United States and other countries, and Iron Mountain, the Iron Mountain logo, and combinations thereof, and other marks marked by TM are trademarks of Iron Mountain Incorporated, all licensed for use by Iron Mountain Canada Operations ULC. All other trademarks and other identifiers remain the property of their respective owners.

